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 5.6

Practical Tools for Online Safety

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 5.6

Practical Tools for Online Safety

Objectives:

- To equip participants with practical tools and techniques for identifying and mitigating common online threats, including phishing, malware, and scams.
- To build proficiency in utilizing cybersecurity resources, such as password managers, VPNs, and secure browsers, while fostering an understanding of online privacy management.
- To promote safe and responsible online practices through critical evaluation of digital platforms, recognizing warning signs of cyber threats, and adopting protective habits like reporting suspicious activities.

Key Message(s):

- Awareness and preparation are your first line of defense. Understanding online threats and having the right tools empowers you to navigate the digital world securely.
- Your safety is in your hands. Leveraging practical tools like VPNs, secure browsers, and privacy settings allows you to protect your personal data and maintain control over your online presence.

TYPE OF LESSON:

Lesson Overview

Online safety hinges heavily on the ability to effectively use tools designed to protect personal information and prevent digital threats. This lesson emphasizes practical, hands-on engagement with key cybersecurity tools, such as password managers, VPNs, and privacy settings. Participants will actively explore how these tools work, test their features, and learn strategies to incorporate them into daily digital routines. Through guided activities, they will build confidence in applying these tools to safeguard their online presence and respond to risks with practical solutions.

The workshop is organized into 4 steps:

1: Introduction to online safety tools (10 min)

2: Hands-on tool exploration (15 min)

3: Scenario-based risk management (10 min)

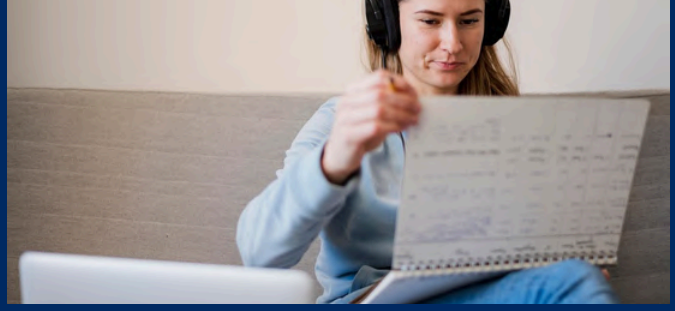
4: Final reflections (5 min)

Step 1

Introduction to online safety tools

Have you ever come across something online that seemed suspicious? Maybe a strange email asking you to reset your password, a pop-up offering a free prize, or a website asking for too much personal information? These situations can feel risky - and they often are.

The good news is that there are **practical tools** you can use to protect yourself in moments like these. By the end of this activity, you'll know how to recognize these risks and use tools like password managers, VPNs, and privacy settings to stay safe online. Let's dive in and see how these tools can help you!



Step 1

Introduction to online safety tools

Here are three simple tools that can make your online life much safer:

- **Password managers**: These help you create and store strong, unique passwords so you don't have to remember them all.
- **VPNs (Virtual Private Networks)**: These protect your online activity, especially on public Wi-Fi, by keeping your connection secure.
- **Browser privacy settings**: These let you control what information websites can collect about you, like your location or browsing habits.

We'll focus on these tools today because they can make a huge difference in staying safe online.

Think about the last time you came across something online that felt off -maybe a a website that didn't seem trustworthy. How did you handle it? Did you ignore it, investigate further, or maybe even click on it?

Let's brainstorm together:

- What kinds of online threats or risks have you noticed before?
- What tools or strategies do you already use to stay safe online?

We'll take a few minutes to share ideas as a group. Don't worry if you haven't experienced this firsthand - your peers' stories might spark new thoughts.

Step 2

Hands-on tool exploration

Now it's time to dive in and explore how simple tools can make your online presence safer. In this activity, you'll try out browser privacy settings and test your password creation skills using *The Password Meter*. Let's get started!

Part 1: Browser privacy settings

Your browser can control how much information websites collect about you. Let's check and adjust your privacy settings:

1. Open your browser's privacy settings (look for "Settings" or "Preferences," then navigate to "Privacy" or "Security").
2. Review these key areas:

- **Tracking prevention**: Is it turned on?
- **Cookies**: Are third-party cookies blocked?
- **Permissions**: Which websites can access your location, camera, or microphone?

Step 2

Hands-on tool exploration

3. Make adjustments: Turn on any privacy settings you think will help protect your data.

For example:

- Block tracking cookies.
- Disable location sharing for websites you don't trust.

Quick reflection: What surprised you about your current settings? Did you make any changes?

Part 2: Testing password strength with *The Password Meter*

Creating a strong password is one of the easiest ways to protect your accounts. Now, let's see how secure your passwords are:

1. Go to The Password Meter.
2. Think of a new password (don't use one you already have!).

Step 2 Hands-on tool exploration

3. Enter it into *The Password Meter* and look at the feedback:
   - How strong is your password?
   - What suggestions does it give to make it stronger?

4. Experiment by changing your password based on the feedback (e.g., add symbols, make it longer, or mix lowercase and uppercase letters). See how the score improves!

Quick reflection: How easy or hard was it to create a strong password? What's one thing you'll do differently when setting passwords in the future?

By the end of this activity, you'll have improved your browser's privacy settings and learned to create stronger passwords!

Step 3

Scenario-based risk management

After we have looked at some practical tools, let's see how they can be applied to real-life situations. You will work in small groups to analyse scenarios, identify risks and decide how to deal with them using the tools discussed.

Read the scenario your group is given. Here are some examples:

1. *You get an email saying you've won a prize, but the link looks suspicious. What do you do?*
2. *A social media app asks to access your location, camera, and microphone when you install it. Should you allow it?*
3. *You're using public Wi-Fi at a café and are prompted to log in to an unfamiliar website. How do you stay safe?*

Talk with your group about the risks in your scenario. Ask yourselves:

- *What could go wrong if you don't act carefully?*
- *Why does this situation feel unsafe?*

Decide how you could use practical tools to handle the risk. For example:

- *Use browser privacy settings to block unnecessary permissions.*
- *Avoid clicking suspicious links and check emails for phishing signs.*
- *Turn on a VPN to secure your connection on public Wi-Fi.*

Step 3

Scenario-based risk management

After several minutes, each group will share:

- *What risks you spotted in the scenario*
- *What tools or steps you used to stay safe*

Think about it: How could these tools help you in your own online activities?

Practical tools like browser privacy settings, VPNs, and phishing detection can turn risky situations into manageable ones. Using them regularly makes staying safe online much easier!

Step 4

Final reflections

Let’s reflect on what you’ve learned and how you’ll use it to stay safe online.

Step 1: Reflect

Think about these questions:

- Which tool (e.g., browser privacy settings, VPNs, password managers) was the most useful for you? Why?
- How has your view of online safety changed after using these tools?

Step 2: Plan your next step

Write down one action you’ll take to improve your online safety.

- What will you do? (e.g., “I’ll use a password manager to create strong passwords.”)
- When will you do it? (e.g., “By the end of the week.”).

Practical tools are your first step - stay consistent to keep your online safety strong!

Key Takeaway Summary

- **Browser privacy settings, password managers, and VPNs are simple but powerful tools to enhance your online safety.**
- **Actively manage what information you share online by adjusting privacy settings and limiting unnecessary permissions.**
- **Regularly update privacy settings, create secure passwords, and review app permissions to make online safety a routine part of your digital life.**
- **Stay proactive - combining tools with critical thinking and staying informed ensures you're prepared for evolving online threats.**
- **Try to also test other practical online tools to understand and improve your digital security - the more tools you know how to use, the more you will increase your security!**

Instructions for youth workers, educators, and teachers

Objective:
This lesson focuses on equipping participants with the practical skills to use basic online security tools. Through individual and group exercises and discussions, they will gain the ability to identify and deal with common online threats, strengthen their digital protection with resources such as password managers, VPNs and privacy settings, and integrate safer habits into their daily online activities.

Materials Needed:

- Internet access for testing tools (e.g., VPNs, password managers)
- Laptops, tablets, or smartphones for hands-on exercises
- Whiteboard or flip chart for brainstorming and summarizing discussions
- Blank sheets of paper for note-taking
- Pens, pencils or coloured markers

Step 1: Introduction to online safety tools (10 min)

1. Begin by engaging participants with a relatable question: “Have you ever come across something online that seemed suspicious, like a strange email, a pop-up offering a prize, or a website asking for too much personal information?” Briefly explain that these situations can feel risky and often are, but there are practical tools to address them.
2. Introduce the session's focus on three essential tools: password managers, VPNs, and browser privacy settings. Highlight their importance by explaining that password managers help create and store strong, unique passwords, VPNs secure online activity on public Wi-Fi, and browser privacy settings control what information websites can collect, such as location or browsing habits.
3. Encourage participants to reflect on their own experiences with online risks by asking, “Think about the last time you encountered something suspicious online. How did you handle it?”
4. Facilitate a brief discussion with questions like, “What kinds of online threats have you noticed?” and “What tools or strategies do you already use to stay safe?” Invite participants to share their stories or ideas, emphasizing that learning from each other can spark new insights.
5. Conclude by reinforcing the importance of these tools in managing online risks, stating, “By using tools like password managers, VPNs, and privacy settings, you can confidently navigate the digital world while protecting your personal information.” Keep the discussion interactive and supportive, ensuring participants feel encouraged to share their thoughts and learn from the group.

Step 2: Hands-on tool exploration (15 min)

1. Begin by explaining the goal of this activity: to explore practical tools that enhance online safety through browser privacy settings and password strength testing.
2. Divide the activity into two parts to ensure a structured approach.

Part 1: Browser privacy settings (8 minutes)

1.Guide participants to open their browser's privacy settings (navigate to "Settings" or "Preferences," then find "Privacy" or "Security"). Ask them to review key areas:

- Tracking prevention: Ensure it is enabled.
- Cookies: Check if third-party cookies are blocked.
- Permissions: Review which websites can access their location, camera, or microphone.

2. Encourage participants to make adjustments, such as blocking tracking cookies or disabling unnecessary location sharing.
3. Afterward, prompt a quick reflection: "What surprised you about your current settings? Did you make any changes?" This helps participants connect their discoveries with the value of these tools.

Part 2: Password strength testing (5 minutes)

1. Direct participants to access The Password Meter. Ask them to create a new password (not one they currently use) and test its strength.
2. Encourage them to analyze the feedback and experiment with changes, such as adding symbols, mixing cases, or increasing length, to see how the score improves.
3. Wrap up with a reflection: "How easy or hard was it to create a strong password? What's one thing you'll do differently when setting passwords in the future?"
4. Conclude the activity by reinforcing its practical value.
5. Keep the session hands-on and engaging, offering guidance as needed while participants explore and apply these tools.

Step 3: Scenario-based risk management (10 min)

1. This activity helps participants apply online safety tools to real-life scenarios. Divide participants into small groups and assign each group a scenario, such as:
   - A suspicious email with a prize link.
   - A social media app requesting excessive permissions.
   - Using public Wi-Fi and encountering an unfamiliar login prompt.
2. Instruct groups to discuss the risks, considering:
   - “What could go wrong if you don’t act carefully?”
   - “Why does this situation feel unsafe?”
3. Have them identify how to handle the risk using tools like browser privacy settings, avoiding phishing links, or enabling a VPN.
4. Afterward, each group shares the risks they identified and the tools they used to address them.
5. Conclude by highlighting: “Tools like privacy settings, VPNs, and phishing detection make managing online risks easier. Regular use of these tools strengthens online safety.” Keep the session focused and encourage practical, actionable insights.

Step 4: Final reflections (5 min)

1. Conclude the session by guiding participants through a reflective exercise to consolidate their learning. Begin by asking them to consider:
   - “Which tool (e.g., browser privacy settings, VPNs, password managers) was the most useful for you? Why?”
   - “How has your view of online safety changed after using these tools?”
2. Encourage participants to share their thoughts briefly, fostering a supportive environment for discussion.
3. Next, prompt them to plan a concrete action to enhance their online safety, such as:
   - “What will you do?” (e.g., “I’ll use a password manager to create strong passwords.”)
   - “When will you do it?” (e.g., “By the end of the week.”)
4. Wrap up by emphasizing the importance of consistency, reminding participants: “Practical tools are your first step - stay consistent to keep your online safety strong!” Keep the tone motivational and focused on applying lessons learned to everyday online practices.

Key Takeaways:

After completing the lesson, participants will gain a clear understanding of how to use basic tools such as password managers, VPNs and browser privacy settings to enhance their online security. They will learn to identify common threats, such as data tracking, and take proactive steps to protect their personal information. By integrating these tools and strategies into their daily routine, they will be able to navigate the digital world with confidence, minimizing potential threats. To effectively communicate these takeaways, you should use relatable scenarios and clear examples to demonstrate the real-world impact of these tools on everyday online safety.

Follow-Up and At-Home Activities:

Inspire participants to take a closer look at their current online practices by reviewing and adjusting browser privacy settings, testing the strength of their passwords with tools such as The Password Meter, and exploring VPN functionality. Assign them to evaluate the permissions of frequently used applications, noting potential risks and implementing safer alternatives. Finally, ask participants to share one newly learned security tip with a friend or family member, reinforcing their knowledge and spreading awareness about digital security.

Tips for Teachers:

You can use practical, real-world examples and other interactive exercises to demonstrate how tools like password managers, VPNs, and privacy settings can be effectively used to enhance online safety. Show participants step-by-step how to navigate and configure these tools, making the session hands-on and actionable. Create an open and supportive environment where participants feel comfortable discussing their experiences with online threats and asking questions. Highlight the importance of regularly using these tools and integrating them into everyday online routines to ensure consistent and proactive digital protection.

Tools

Get Safe Online

A comprehensive website offering free, straightforward advice on a wide range of online safety topics. It includes practical guides on protecting personal information, avoiding scams, and secure online communication. The content is user-friendly and designed for people with minimal technical knowledge.

www.getsafeonline.org

The Password Meter

A free tool that evaluates the strength of passwords and provides tips for improving them. Learners can experiment with creating passwords and receive instant feedback on their security level, making it an interactive way to understand the importance of strong passwords.

passwordmeter.com

References

- Alice. (2022, October 3). 5 Tools That Help Keep People Safe Online. Ryadel. Retrieved from https://www.ryadel.com/en/5-privacy-data-protection-security-tools
- Get Safe Online. (n.d.). Retrieved from https://www.getsafeonline.org
- Goodwall Team. (2022, March 24). 7 Best Online Safety Tools and Privacy Settings to Keep Yourself Protected. Retrieved from https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings
- 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
- The Password Meter. (n.d.). Retrieved from https://passwordmeter.com
- Vodafone. (n.d.). Using online safety and wellbeing tools. Retrieved from https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools

QUIZ

1. What is a primary function of a Virtual Private Network (VPN)?
A. Providing automatic antivirus protection
B. Increasing Internet speed
C. Preventing pop-up ads on all websites
D. Encrypting online activity, especially on public Wi-Fi

2. Which behavior could put your online safety at risk?
A. Using strong, unique passwords for each account
B. Adjusting privacy settings in your browser regularly
C. Using a password manager to store login credentials
D. Clicking on every link in unsolicited emails

3. What is a recommended step to enhance your browser privacy settings?
A. Using default settings without modifications
B. Blocking tracking cookies and disabling unnecessary permissions
C. Turning off cookies for all websites
D. Allowing all websites to access your location

QUIZ

4. What is the purpose of browser privacy settings?
A. To speed up user's browsing experience
B. To store user's passwords securely
C. To control what information websites can collect about user
D. To prevent pop-up ads on all websites

5. How can you improve your password strength?
A. By including symbols, mixing cases, and increasing length
B. By using common phrases that are easy to remember
C. By avoiding the use of numbers and special characters
D. By testing the same password repeatedly

Solutions

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

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

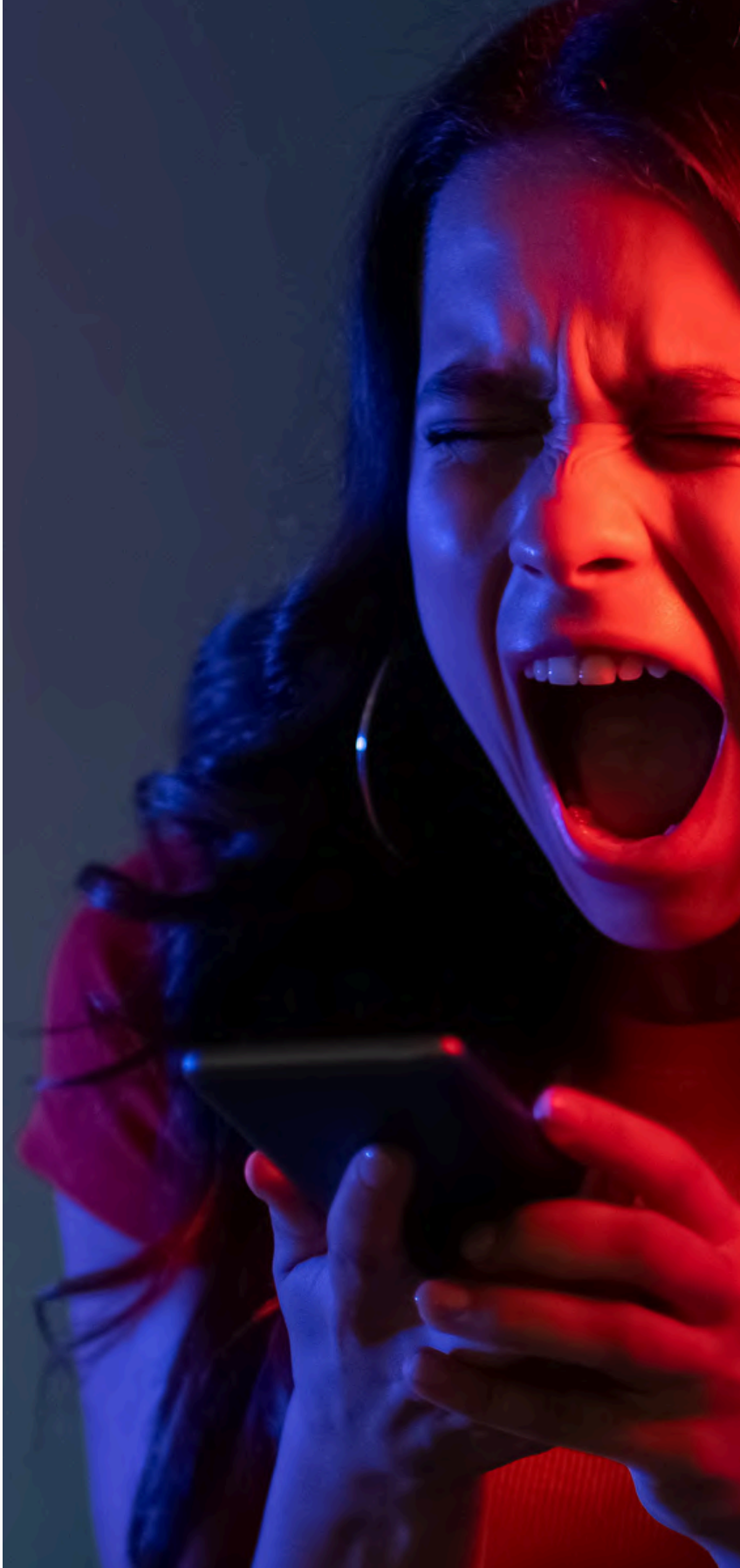
LABC

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.