13+

Identifying and Avoiding Online Risks: Phishing, Malware, and Scams

SUBJECT: Safe Online Navigation

LESSON TOPIC: Cybersecurity Awareness

DURATION: 45 minutes (1 Lesson); 1-1.5 hours (Preparation)

LEARNING OBJECTIVES:

Main objective of the lesson

To educate students about the various online risks, specifically phishing, malware, and scams, and to equip them with the knowledge and skills necessary to identify and avoid these threats to ensure their online safety.

Competences that students will acquire

Students will acquire critical thinking and analytical skills to identify and mitigate online threats, technical proficiency in using cybersecurity tools, and improved digital literacy. They will also develop personal responsibility for online safety, effective communication skills for reporting incidents, and a proactive approach to maintaining cybersecurity.

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.

MATERIALS/RESOURCES NEEDED:

- Module 2 (https://www.digi-civis.eu/e-learning)
- Canva Presentation (https://www.canva.com/design/DAGJ_oaybA/k6GVY6Ox8nnuBkwjCJaO8w/edit)
- 10 question Quiz on Cybersecurity Practices.
- Preparation of sets of printed emails, including both phishing and legitimate ones (these emails can be sourced from Google or created by teacher for educational purposes).
- Caulfield, M., & Wineburg, S. (2024). Verified: How to Think Straight, Get Duped Less, and Make Better Decisions about What to Believe Online.
- Kallen, S. A. (2023). Spotting Online Scams and Fraud.

METHODS/TECHNIQUES:

- **Presentation:** The teacher will deliver a presentation to introduce the topic, explain key concepts, and provide real-life examples of phishing, malware, and online scams.
- **Group Work:** Students will participate in a group activity where they analyze and identify phishing emails. This collaborative exercise will encourage discussion, critical thinking, and teamwork as they determine which emails are phishing attempts.
- **Individual Work:** Students will complete a quiz to assess their understanding of cybersecurity practices covered in the lesson. This activity allows students to individually apply what they've learned and reinforce their knowledge on identifying and avoiding online risks.

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 PLAN OVERVIEW

PREPARATION:

The teacher must:

- Thoroughly go through the Digi-civis Module 2 to understand the fundamental concepts of online risks, including phishing, malware, and scams.
- Examine the recommended books and videos to gather detailed information and real-life examples that will enhance the lesson's content.
- Teachers must prepare sets of printed emails, including both phishing and legitimate ones. These emails can be real examples collected (with sensitive information removed) or fake ones created for educational purposes. Ensure the emails are in the local language or English, depending on the students' proficiency and the language of instruction
- Review the provided Canva presentation to ensure all key points are covered and the visuals are engaging and informative.
- Print the provided quiz or, if feasible, provide the quiz as a digital file for students to complete using devices and digital pens.

IMPLEMENTATION:

1. Introduction (10 minutes)

Overview of the Topic:

- Briefly explain what phishing, malware, and online scams are.
- Discuss why it is important to understand and avoid these online risks.
- Show a short video clip that illustrates real-life examples of phishing attempts and others.

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 PLAN OVERVIEW

IMPLEMENTATION:

2. Group Activity (15 minutes)

Phishing Simulation:

- Divide students into small groups.
- Provide each group with a set of printed phishing emails and legitimate emails.
- Ask them to identify which emails are phishing attempts and explain their reasoning.
- Each group presents their findings and reasoning to the class.

3. Class Discussion (10 minutes)

- Engage students with questions about their own experiences with suspicious emails or online activities. For example, discuss common characteristics of phishing emails (e.g., generic greetings, urgent language, suspicious links).
- Highlight common online scams (lottery scams, tech support scams, online shopping scams).

4. Individual Activity (10 minutes)

- 10 question Quiz on Cybersecurity Practices.
- Provide students with a quiz to assess their understanding of the lesson content.

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.

ADDITIONAL INFORMATION TO LEARN MORE:

- Phishing Explained In 6 Minutes https://www.youtube.com/watch?v=XBkzBrXlle0
- Ransomware In Cybersecurity https://www.youtube.com/watch?v=-KL9APUjj3E
- More New Clever Email Scams to Watch Out For https://www.youtube.com/watch?v=xEKY7lZStE4

ANNEXES:

- Canva Presentation (https://www.canva.com/design/DAGJ__oaybA/k6GVY6Ox8nnuBkwjCJaO8w/edit)

HOMEWORK:

No formal homework is required for this lesson. However, you can encourage students to talk with their family members about any experiences they’ve had with scam messages or emails. Ask students to learn how their family members spotted these scams and what advice they can offer to help students avoid similar risks.

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.

ASSESSMENT:

Use these 10 quiz questions for assessment or draw inspiration from them to create your own quiz on cybersecurity practices.

Quiz on Cybersecurity Practices

Answer the following multiple-choice questions to assess your understanding of cybersecurity practices.

1. What is phishing?

- A) A type of malware
- **B) A method to trick people into giving personal information**
- C) A legitimate way to secure your account

2. Which of the following is a common sign of a phishing email?

- **A) Generic greetings like "Dear Customer"**
- B) Personalized information
- C) Proper spelling and grammar

3. What is malware?

- A) A secure software program
- **B) Harmful software that can damage your computer**
- C) A type of email scam

4. Which of the following is a type of malware?

- A) Phishing email
- **B) Virus**
- C) Strong password

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.

ASSESSMENT:

5. How can you protect your computer from malware?

- **A) Keep your antivirus software up to date**
- B) Click on all email links
- C) Share your passwords

6. What should you do if you receive an email from an unknown sender asking for personal information?

- A) Reply with your information
- **B) Ignore and delete the email**
- C) Forward it to your friends

7. Which of the following is a common online scam?

- A) Genuine tech support help
- **B) Fake lottery wins**
- C) Secure online shopping

8. Why is it important to use strong, unique passwords for different accounts?

- **A) To protect each account separately and prevent multiple accounts from being compromised**
- B) To make it easier to remember all passwords
- C) To share them easily with friends

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.

ASSESSMENT:

9. What steps should you take if you think your device is infected with malware?

- A) Ignore it
- **B) Run a virus scan with up-to-date antivirus software**
- C) Keep using the device normally

10. How can you help your friends and family stay safe online?

- A) By sharing your passwords with them
- **B) By teaching them how to recognize and avoid online threats**
- C) By ignoring online safety tips

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.