Lesson Plan# 4

Grade 7 Primary School Level

Topic - Recognizing phishing, scams, and social engineering online

Integration into School Subjects – Computer Science, Safety Education

Target Group	Primary School Grade 7
Number of Students	Minimum number of students: 10 Maximum number of students: 30
Lesson Preparation	Prepare examples of phishing messages (e-mails, SMS messages, instant messengers). Prepare examples of safe and unsafe websites. Prepare technical resources, including a projector, laptops or tablets with Internet access.
Learning Objectives Based on the DataPro Curriculum	**A. How can I protect my data (and trust in information)?** **A.1 Identity Management:** Learning how to create strong and unique passwords. Developing awareness of protecting login credentials and personal data. Understanding the importance of two-factor authentication. **A.2 Self-Protection:** Recognizing dangerous e-mails, SMS messages, and links. Learning the basic principles of safe Internet use. Learning how to use security filters and system updates. **A.3 Against Disinformation:** Developing skills for critically evaluating information found online. Recognizing manipulation attempts and false messages. **A.4 Verifying Information:** Learning how to verify the credibility of sources. Developing the ability to compare information from multiple sources. **A.5 Protecting Others:**

	Understanding the consequences of sharing other people's data. Developing responsible online behavior. **A.7 Against Fraud:** Learning about methods used by cybercriminals. Recognizing phishing, fake contests, and data theft attempts. Learning how to react to suspicious online situations. **B. What makes data protection a human right?** **B.1 Privacy Means Freedom:** Understanding that privacy protection allows users to safely use the Internet. Developing awareness of risks resulting from losing control over personal data. **B.3 The Power of Privacy:** Learning about users' rights related to data protection. Developing the ability to consciously give consent for data processing. **C. What makes data valuable (economically)?** **Behavior as an Identifier:** Understanding that online activity can be used to profile users. Learning how to limit online activity tracking. **Against Behavioral Manipulation:** Recognizing manipulation techniques used in advertisements and social media. Developing critical thinking toward online content.
Other Learning Outcomes, if applicable	Development of digital competences. Development of teamwork skills. Improvement of analytical and critical thinking skills. Developing responsibility for one's own online actions.
Lesson Duration Including Homework Time	Lesson plan for 2 school lessons of 45 minutes each. Total: 90 minutes of lessons.

	Homework preparation will take approximately 30 minutes.
Technical Requirements / Materials	Laptops or tablets with Internet access. Projector. Materials with examples of phishing messages. Worksheets for students.
DataPro Resources That Can Be Used During the Lesson	Spot the Phish: InstaPik (Interacty activity) Spot the Phish: Czech Bank (Interacty activity)
Additional Educational Resources	Educational Videos: Your data – your business | How to protect your privacy online and offline | UODO (PL) Guidelines for safe internet use: Respect others online (PL) (Sieciaki.pl) Other: What is PHISHING and how can you avoid falling for suspicious emails and text messages? - gov.pl (PL)
Suggested Methodology or Lesson Delivery	Proposal 1 Introductory discussion: what threats can Internet users encounter? The teacher presents examples of phishing messages and fake websites. Students work in pairs to analyze the examples and identify elements indicating fraud. Discussion of results and creation of a shared list of safe online behavior rules. Proposal 2 Brief reminder of online safety rules. Practical exercise: students receive online situation scenarios and decide how they should react. Discussion: why do cybercriminals use manipulation and what emotions are they trying to trigger?

	The teacher presents methods for reporting online scams and responding to incidents. Proposal 3 Group project work: creating a poster or infographic titled “How Not to Be Scammed Online?”. Students present their projects. Summary of the most important safety rules. Homework Students prepare a short list of safe Internet use rules for younger students or family members.

Syllabi DataPro Poland/CWEP

Work Package 2

Contact	Joanna Bać
Institution	CWEP
E-Mail	joanna.bac@cwep.eu
Phone	+48 17 853 66 72

Project	DataPro
Dissemination level	Public
Date created	December 2024-February 2025
Author	Joanna Bać

Co-funded by the European Union

Disclaimer
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.