

DataPro · Syllabus Nothing to Hide

Cluster C – Data Protection Measures

What can I concretely do? | Grades 5–8 | approx. 90 min

Subject	Media and Informatics / Social Studies
Duration	2 lessons of 45 min each or 1 double period
Slides	Available at: https://www.datapro.education/datapro-webgames/ under “Class Material” → “Presentations: Data Protection Measures” → EN Available in English, Spanish, and other languages besides German (7 slides)
Additional Materials	- Phishing worksheet, DataPro Chatbot (for the quiz task), Kahoot: https://www.datapro.education/tools/ - before the lesson: Game Guide for teachers both available at https://www.datapro.education/datapro-webgames/
Prior Knowledge	After Cluster A + B – but can also be used independently
Game	https://dataprogames.ph-freiburg.de/nothing-to-hide/

Learning Objectives

- Create strong passwords using the mnemonic method (C.2)
- Explain 2FA factors and give examples of their use (C.2)
- Recognize phishing characteristics and social engineering tactics (C.4)
- Respond correctly to phishing attempts: don't click, report, check the sender (C.4)
- Independently research and create learning material with the DataPro Chatbot (C.5)

Lesson Sequence

Time	Phase / Goal	Lesson Sequence	Slide / Material
10 min	Introduction <i>Take Stock</i>	- Prompt question: what do you already do to protect yourselves online? - Cluster answers: what do many do / what is often forgotten - Set the tone: this is about conscious decisions, not perfection	No slides – open discussion
25 min	Input: Passwords & 2FA <i>Technical Security</i>	- Slide 2: passwords – carry out the task directly with students (mnemonic method) - Slide 3: 2FA – explain the three factors; collect everyday examples - Consolidation: why isn't a strong password alone enough?	→ Slide 2: passwords + task (integrated into the slide material) → Slide 3: 2FA
20 min	Input: Phishing & Social Engineering <i>Recognize Attacks</i>	- Slide 4: explain phishing types and social engineering tactics	→ Slide 4: phishing + social engineering

		- Slide 5: analyze examples – class discussion: what does this indicate? - Phishing worksheet: students identify characteristics in example messages	→ Slide 5: examples for discussion → Phishing worksheet https://www.datapro.education/tools/
25 min	Game: Nothing to Hide <i>Apply Protective Measures</i>	- Observation task: which protective measures help in the game? - Where would you have acted differently? - Note game points – comparison with earlier rounds possible	→ dataprogames.ph-freiburg.de → Slide 7: https://dataprogames.ph-freiburg.de/nothing-to-hide/
20 min	Transfer: Quiz Task <i>Apply & Share Knowledge</i>	- Slide 6: students choose a protective measure and create a quiz with the DataPro Chatbot - Prompting instructions are on slide 6 – read through with students - Exchange quizzes, compare solutions, capture results as a class	→ Slide 6: quiz task + prompting instructions → DataPro Chatbot (https://datapro.cyber-geiger.com)

Notes

The PDF has 7 slides; slide 2 contains a complete task with examples.

Slide 6 contains detailed prompting instructions for the DataPro Chatbot – read aloud.

The quiz task (slide 6) also works well as pair work.

Don't show the phishing examples on slide 5 beforehand – students should find the characteristics themselves.

Cluster C works well as a conclusion: comparing game points with Cluster A shows progress.

Assessment

- Quiz comparison from slide 6: who had more correct answers in the partner quiz?
- Kahoot quiz on protective measures at <https://www.datapro.education/tools/>
- Nothing to Hide game points – comparison Cluster A vs. Cluster C

Project	DataPro – Erasmus+
Institution	Pädagogische Hochschule Freiburg
Author	Renata Säuberli
Date	June 2026



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