Syllabus n. 6 - Protecting Your Data

Digital Awareness - Recognizing the Risks and Reliable Online Sources

Target Group	Students of the first level of high school (14-15 years old)
Group Dimension	Minimum 15, maximum 25 students
Prerequisites and prior knowledge	**Prerequisites for students:** • Basic knowledge of how the Internet, search engines and social media work. • Personal experience in the daily use of apps, social networks and online services. • Basic awareness of the importance of personal data (e.g. name, photo, location) and the possible consequences of sharing it. **Materials and resources to be prepared:** • Access to individual digital devices with an Internet connection (tablets, smartphones or laptops). • Preparation of digital or printed forms for collecting and reflecting on one's digital behaviour. • Teaching sheets with concrete examples of “dark patterns” (deceptive digital interface models). • Interactive whiteboard or video projector with audio.
Learning Objectives from DataPro Curriculum	**C.1 Identity Management:** Recognise the data that constitutes digital identity; understand the concept of digital identity fragmented across multiple platforms. **C.2 Ensuring Data Security:** Adopt concrete strategies to protect your online information, such as limiting geolocation and using privacy settings wisely. **C.4 Information and Source Validation:** Analyse digital interfaces to identify misleading elements (e.g. disguised advertising, misleading buttons) and develop skills to avoid them. Consult multiple sources to verify information.

Further specific learning objectives	• Developing critical thinking skills to evaluate online information. • Recognising fake news and unreliable sources. • Identifying dark patterns and understanding how they influence online decisions. • Adopting strategies for more conscious and less manipulable browsing.
Duration	Around 60 minutes
Techinical requirements/ aids	Stable internet access Individual devices for each student (smartphone, tablet or laptop) Multimedia whiteboard or video projector with audio Access to digital tools (e.g. tools for managing privacy settings in browsers, password verification, data breach check websites – e.g. “Have I Been Pwned”)
Training materials and tools from DataPro	“DataPro Assistant” chatbot, for practical exercises on privacy analysis in the most widely used apps, and for checking digital interfaces, links and sources. “Unmask the News!” game (Interacty) to assess the validity of information and sources. MINI-WORKBOOK “News Detective - Mini Anti Fake News Guide” - to do at home with parents.
Additional specific teaching materials	Information on "dark patterns": https://better-internet-for-kids.europa.eu/en/dark-patterns https://www.storyboard18.com/how-it-works/dark-patterns-explained-the-digital-design-tactics-misleading-millions-68150.htm
Tips for conducting a lesson	**1. Introduction: The Online World between Truth and Deception (10 minutes)** • **Hook:** Show an example of ‘fake news’ or sensationalist news (selected in advance by the teacher) and ask students: ‘How can we tell if this news is true or false?’ • **Discussion:** Start a discussion about the importance of verifying online sources and the dangers of believing everything you read or see on the internet. **2. Evaluating Online Information and Sources (20 minutes)**

	• **Main Activity:** Students play ‘Unmask the News!’ (link above), which will help them practise their discernment skills. • **Post-game discussion:** After the game, discuss the strategies students used to evaluate sources and the red flags they identified. • **Tool (Optional):** The ‘DataPro Assistant’ chatbot (link above) can be used for a quick exercise on how to verify the credibility of a specific link or source by simulating scenarios. **3. "Dark Patterns": Hidden Web Tricks (20 minutes)** • **Explanation:** Introduce the concept of ‘dark patterns’ by reading the articles linked above together: these are user interface design techniques that trick users into doing things they would not normally do. Show common examples (e.g. ‘accept all’ buttons that are more prominent than ‘customise’ buttons, subscriptions that are difficult to cancel, misleading pop-ups, fake countdowns for offers, hidden costs). • **Discussion:** Ask students if they have ever encountered these ‘tricks’ online and how they felt about them. Discuss how ‘dark patterns’ influence our choices, our privacy, and our time online. • **Practical Activity:** Students can use their devices to browse websites or apps they are familiar with to look for examples of ‘dark patterns’. Alternatively, the teacher can project and analyse pre-selected examples together with the class. **4. Summary and Defence Strategies (5 minutes)** • **Summary:** Summarise the key concepts of the lesson: the importance of critical thinking, verifying sources, recognising “dark patterns” and awareness of online manipulation. • **Brainstorming:** Ask students what strategies they can adopt to defend themselves against disinformation and manipulation online. **5. Questions and Closure (5 minutes)** • **Q&A:** Open space for questions and final clarifications. • **Conclusion:** Encourage students to be aware, critical and attentive digital navigators, capable of distinguishing between truth and falsehood and protecting themselves from online traps. **Homework to do with parents:** MINI-WORKBOOK “News Detective - Mini Anti-Fake News Guide” (link above). Students can complete this activity by filling out the mini-workbook together with their parents, applying what they have learned at school and teaching them how to recognise fake news and navigate online more intelligently.

Syllabus DataPro <Italy>

Work Package 2

Contact Person	Sergio Pelliccioni
Organisation	ADM
Email	info@archiviodellamemoria.it
Phone	

Project	DataPro
Dissemination Level	public
Presentation Date	
Main author(s)	

Co-funded by the European Union

Disclaimer

Funded by the European Union. However, the views and opinions expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Education, Audiovisual and Culture Executive Agency (EACEA). Neither the European Union nor the EACEA can be held responsible for them.

DATAPRO