Syllabus n.5 - Protecting Your Data

Browsing Safely - Protecting your Online Data

Target Group	Students from 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 • Access to data exposure verification tools (e.g. tools to check if an email has been compromised)
Learning Objectives from the 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 Data Security:** Adopt concrete strategies to protect your online information, such as limiting geolocation and using privacy settings wisely. **C.4 Information and Source Checking:** 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	Understand the importance of protecting personal data online. Identify your personal data and your online 'digital footprint'. Manage and configure privacy settings in apps and browsers. Create strong and secure passwords. Check whether your credentials have been compromised in a data breach.
Duration of the lesson	Around 60 minutes
Technical 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. A short presentation useful for a lesson on good practices and online safety, entitled "Protect yourself online: privacy, security and Digital Best Practices" Online True or False Quiz: "Cyber Trap: Who falls for them?", which tests you with realistic scenarios inspired by everyday digital life, helping you to better understand the risks to online privacy.
Additional specific teaching materials	Official website for checking personal data breaches: https://haveibeenpwned.com/?utm_source=chatgpt.com Infographic on good data protection practices: https://iapp.org/media/pdf/resource_center/fpf_student_privacy_compass_youth_privacy_data_protection_101_infographic.pdf
Tips for conducting a lesson	**1. Introduction and Brainstorming: Your Digital Footprint (10 minutes)**

	• **Activity:** Start with an open-ended question: 'What do you post online (photos, comments, videos, etc.) and who do you think can see it?' Encourage a brief discussion. • **Concept:** Introduce the concept of the online 'digital footprint' (everything we leave behind when we browse the internet) and its permanence. • **Discussion:** Ask students what they mean by 'personal data' and why it is essential to protect it. **2. Privacy Management: Settings and Apps (15 minutes)** • **Presentation:** Use the initial sections of the presentation 'Protect yourself online: privacy, security and good digital practices' (link above) to explain the importance of privacy settings in apps and on social media. • **Practical Guided Activity:** Ask students to open a popular app they use regularly (e.g. Instagram, TikTok, WhatsApp) or the web browser on their device. Guide them to find and review the privacy settings (e.g. who can see posts, profile information, geolocation). • **Tool:** Use the 'DataPro Assistant' chatbot (link above) for a practical exercise on analysing privacy settings in specific apps, or for checking generic digital interfaces. **3. Strong Passwords and Recognising Breaches (20 minutes)** • **Explanation:** Explain what makes a password 'strong' (length, complexity, uniqueness) and why it is dangerous to reuse the same passwords on multiple sites. Introduce the concept of 'data breach' (data violation or leak). • **Practical Activity 1 - Password verification:** Students can use an online tool (e.g. a password generator/evaluator or a password checker built into their browser) to assess the strength of a password they use (or a fictitious one they invent on the spot). Emphasise that they should never enter real passwords on unsecure websites. • **Practical Activity 2 - Violation Control:** Introduce an official website for checking personal data breaches (Have I Been Pwned - link above). Explain how it works. If students feel comfortable, they can check (under the guidance of the teacher and with the understanding that it is a personal choice) whether their email address has been involved in known breaches. **4. Interactive Quiz and Summary (10 minutes)** • **Activity:** Students complete the online quiz (link above) to better understand the risks to online privacy. • **Discussion:** At the end of the quiz, discuss the answers together, clarifying any doubts and reinforcing the concepts learned. • **Recap:** Summarise the key points of the lesson: the importance of protecting personal data, managing privacy settings, creating strong passwords and monitoring

	breaches (here you can use the infographic on good data protection practices - link above). **5. Questions and Closing (5 minutes)** ● **Q&A:** Open space for questions and final clarifications. ● **Conclusion:** Encourage students to continue exploring the privacy settings of their accounts and to stay informed about good online safety practices.

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