



Digital identity and safety

Relevant escape room scenario & project resource	• ER1 Understanding AI • ER11 Online exploitation and digital safety • Self-training worksheet: Ethical issues in digital entrepreneurship
Target group & needs	Age range: 15-25 Group size: 3-6 participants Previous knowledge or experience required: Basic everyday use of smartphones and social media
Duration	60–75 minutes
Target competence areas	• Protecting personal data and privacy • Understanding digital identity and footprint • Ethical decision-making and safe digital behaviours
Objectives	• Identify strong and weak password rules. • Recognise phishing and unsafe online behaviours. • Identify the meaning and impact of digital footprint. • Make ethical decisions in realistic digital dilemmas. • Apply basic privacy-protection strategies.
Materials & equipment	• Printed puzzle sheets (password logic grid, screenshots of messages/posts, scenario cards) • Pens and paper or whiteboard for notes • Timer or countdown clock



Useful resources	• Thales - ENISA Guidelines for Identity Protection and Phishing Resistant Multi-Factor Authentication • European Commission – Better Internet for Kids • Free phishing simulator game – Phish me if you can
Setup	• Prepare 4 challenge stations, with numbers to indicate the order they must be done. • Place one puzzle at each station. • Arrange tables so teams rotate between stations.
Step-by-step instructions	Step 1 – Story introduction (5 min) Participants are told that their account on a social media app has been compromised, hacked and altered. They must secure it and remove problematic content before irreversible damage occurs. Step 2 – Station 1: Password logic puzzle (15 min) Participants solve a logic grid to identify the strongest password, based on rules (length, symbols, uniqueness), and secure the account to access the next step. Step 3 – Station 2: Phishing or safe (15 min) Participants analyse messages and posts and decide if they're safe, unsafe or involve phishing, to identify risks and block potential threats before moving forward. Step 4 – Station 3: Digital footprint scenarios (10 min) Scenario cards describe typical online actions (oversharing, debates, email chains) and potential consequences. Participants must match each action to its long-term impact to unlock the next puzzle.



	Step 5 – Station 4: Ethical dilemmas (10 min) Participants must choose between options in complex situations (sharing data to “help” a friend, report or expose a cyberbully, post or censor a sensitive topic). Each choice leads to different outcomes that players must justify and navigate responsibly based on everything they have learned in the previous stations. Once they have proven their understanding, they can access their corrupted account and feel safe online.
Debriefing questions	• Which online behaviours felt “normal” and common but were actually risky? • How do small actions build a digital footprint over time? What does that entail? • Were ethical choices always obvious? Why or why not? What would be their consequences? • What would you change in your own online habits?
Assessment & evaluation	• Observation of group decisions and quality of reflection and justifications for station 5 and debrief • Self-assessment checklist (“I can recognise phishing”, “I know how to protect my data”)
Variations & adaptation	• Younger groups: Fewer scenarios, more visual cues, concrete and “black-and-white” dilemmas • Neurodiverse participants: Clear icons, reduced text, structured choices, additional hints, flexible timing • Advanced groups: More conflicting dilemmas with no perfect answer, encourage debate and nuance



Trainer tips	• Avoid moralising; focus on consequences and objective risks, not judgment. • Encourage discussion and mediation when participants disagree. • Keep scenarios realistic and close to participants' daily digital lives. • Emphasise that safety is a shared responsibility.
References & further readings	• European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity basics for citizens. • European Commission. (2025). DigComp 3.0: European Digital Competence Framework.



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.

Project code: 2023-2-LT02-KA220-YOU-000183156