



Co-funded by
the European Union



NON-FORMAL METHODS ON CYBERSECURITY



2025-1-ES02-KA220-YOU-000358192

**ESCAP(E+) - Educate Youth in Security through
Cyber Awareness Program and Engagement**

THIS WORK IS LICENSED
UNDER [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)





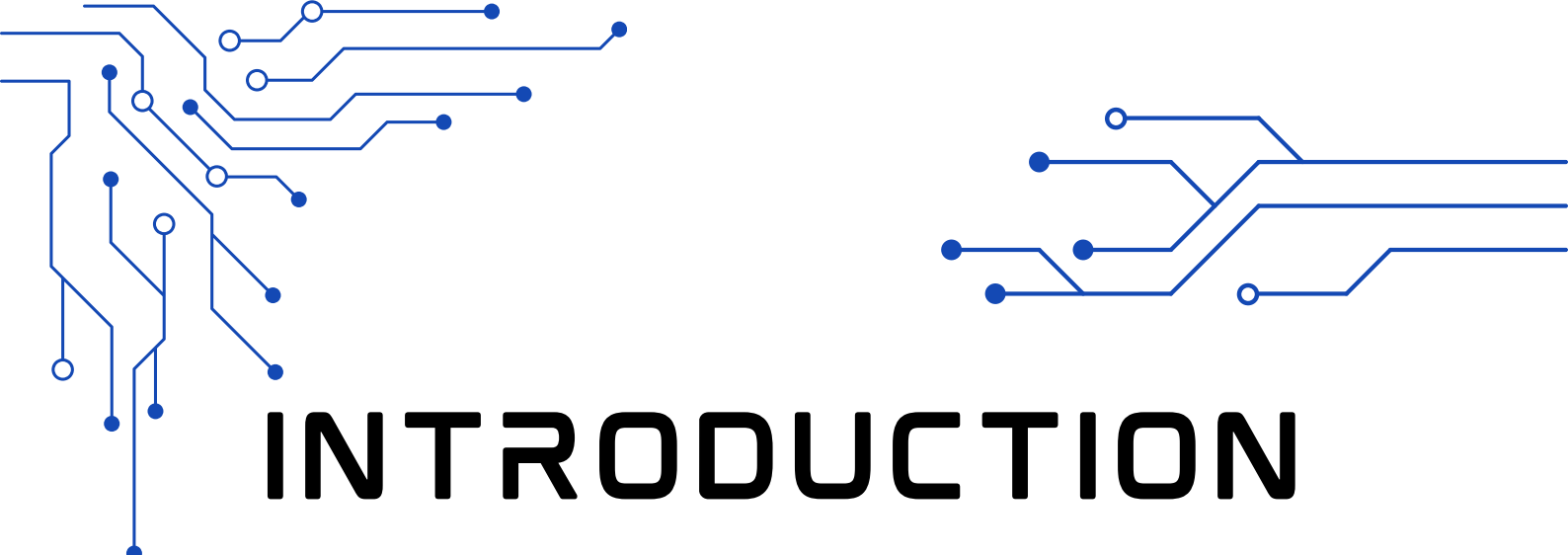
Co-funded by the European Union

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.

The materials developed are classified as 'Open Educational Resources' (OER) and can be freely (without permission of their creators): downloaded, used, reused, copied, adapted, and shared by users, with information about the source of their origin.

TABLE OF CONTENT

1. Introduction.....	4
2. Cybersecurity and Youth.....	8
3. Non-Formal Education Methodology.....	13
4. How to Use This Toolkit.....	18
5. Cybersecurity Learning Activities.....	23
6. Debriefing and Reflection Methods.....	71
7. Tips for Youth Workers.....	74
8. Resources and Tools.....	78



INTRODUCTION

PURPOSE OF THE TOOLKIT

The **ESCAP(E+) Cybersecurity Toolkit** has been developed as a practical and user-friendly resource to support youth workers, educators, and organisations in addressing cybersecurity topics with young people. In today's digital environment, youth are constantly interacting with online platforms, yet they often lack the knowledge and confidence to navigate risks safely. At the same time, many youth workers feel that cybersecurity is too technical or complex to integrate into their daily activities.

This toolkit responds directly to these challenges by offering concrete, ready-to-use approaches that simplify cybersecurity education and make it accessible in non-formal learning contexts. Instead of focusing on theoretical or highly technical explanations, the toolkit translates key concepts into interactive and engaging learning experiences that can be easily applied in workshops, youth exchanges, or local activities.

The main purpose of the toolkit is to empower youth workers to facilitate meaningful discussions and activities around online safety, digital behaviour, and cyber risks. It supports them in creating safe learning environments where young people can reflect on their own online practices, develop critical thinking, and build practical skills. By doing so, the toolkit contributes to strengthening digital resilience among youth and promotes a more responsible and informed use of digital technologies, in line with European priorities on digital transformation and education (European Commission, 2021).

PROJECT OVERVIEW – ESCAP(E+)

ESCAP(E+) – Educate Youth in Security through Cyber Awareness Program and Engagement – is a 24-month Erasmus+ Cooperation Partnership in the field of youth, implemented between December 2025 and November 2027. The project brings together six partner organisations from Spain, Portugal, Romania, Türkiye, Estonia, and Lithuania, combining expertise in youth work, digital education, gamification, and technological innovation.

The project was designed in response to the increasing exposure of young people to cyber threats and the lack of engaging, youth-friendly educational tools to address these risks. Its main aim is to enhance cybersecurity awareness and digital resilience among both young people and youth workers by using innovative, interactive, and non-formal learning methods.

Throughout its implementation, ESCAP(E+) develops a range of educational outputs that make cybersecurity learning more accessible and engaging. These include a virtual reality escape game application, a series of infographics and animated videos, and structured learning activities tested through youth labs and training sessions. By integrating gamification and experiential learning, the project ensures that participants are not only informed about cybersecurity but also actively involved in problem-solving and decision-making processes.

In addition, the project places strong emphasis on capacity building for youth workers, equipping them with practical tools and methodologies that can be directly transferred into their work. Through international cooperation and exchange of practices, ESCAP(E+) contributes to improving the quality and innovation of youth work across Europe, while aligning with Erasmus+ priorities related to digital readiness, resilience, and capacity building (European Commission, Erasmus+ Programme).

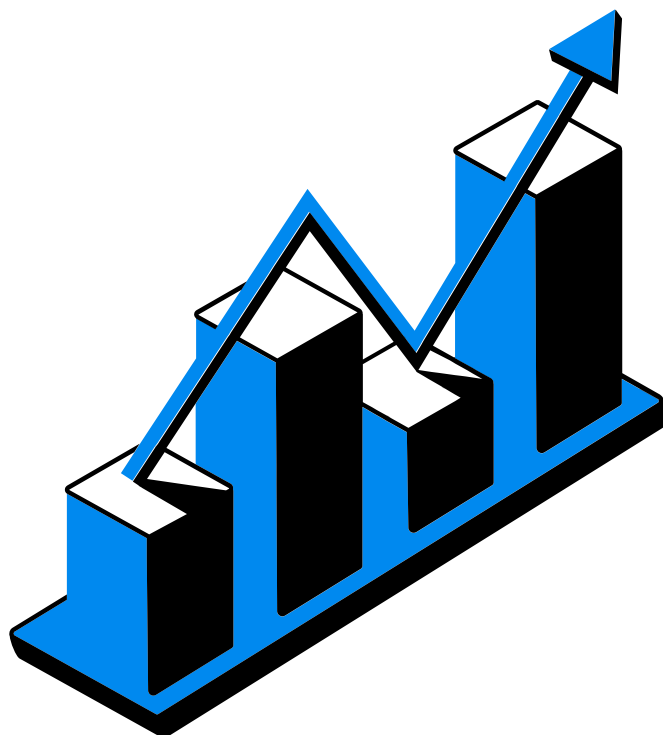
WHY CYBERSECURITY EDUCATION FOR YOUTH IS IMPORTANT



Young people today are among the most active users of digital technologies, spending a significant part of their daily lives online. Social media, messaging platforms, gaming environments, and digital tools are essential spaces for communication, learning, and self-expression. However, this high level of engagement also increases their exposure to a wide range of cybersecurity risks.

According to Eurostat, approximately 97% of young people in the European Union use the internet on a daily basis, highlighting the central role of digital environments in their lives (Eurostat, 2024). At the same time, European data and research indicate that many young people encounter online risks such as phishing scams, identity theft, cyberbullying, misinformation, and privacy breaches. Despite this, a significant proportion lack the skills needed to critically assess online content, protect their personal data, or respond effectively to digital threats.

This situation is further complicated by the fact that existing cybersecurity education is often designed for technical audiences and does not correspond to the needs or realities of young people. Youth workers also face difficulties in addressing these topics, as they may not have access to appropriate tools or training that fits within non-formal education approaches.



WHY CYBERSECURITY EDUCATION FOR YOUTH IS IMPORTANT

Cybersecurity education is therefore essential not only to increase awareness but also to develop practical competencies. It plays a key role in building digital literacy, strengthening critical thinking, and promoting responsible online behaviour. It also contributes to empowering young people to take control of their digital lives, make informed decisions, and protect themselves and others in online environments.

The importance of this topic is strongly reflected in European policy frameworks. The Digital Education Action Plan (2021–2027) emphasises the need to enhance digital skills and resilience across all sectors of education (European Commission, 2021), while the European Union Agency for Cybersecurity highlights education and awareness as fundamental pillars for building a safer digital society (ENISA, 2023).

ESCAP(E+) responds to these needs by offering an innovative approach that combines cybersecurity education with gamification, virtual reality, and non-formal learning. By making the learning process interactive, relatable, and engaging, the project ensures that young people are not passive recipients of information, but active participants in building their own digital safety skills.



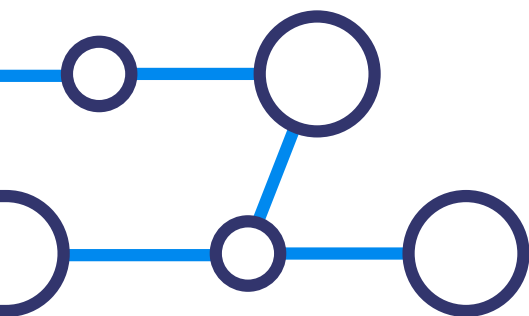


CYBERSECURITY & YOUTH

MAIN ONLINE THREATS FOR YOUNG PEOPLE

Desk research conducted across ESCAP(E+) partner countries reveals a threat landscape despite differences in national context. The threats most relevant to young people are the trust or behaviour-based manipulations that exploit the ordinary social dynamics of everyday platform use. Four platforms emerge as primary vectors (e-mail, Instagram, Facebook, and TikTok) each with a distinct threat profile but a shared underlying mechanism: To create a sense of urgency, to borrow institutional or social legitimacy, and to act before the user pauses to verify. Among the prevalent risks, **Phishing and credential theft via e-mail** represent the highest-severity threat documented. Fraudulent messages impersonate trusted institutions such as banks, universities, public authorities, delivery services, directing users to fake login pages where credentials are obtained. AI-assisted content generation has substantially raised the sophistication of these messages.

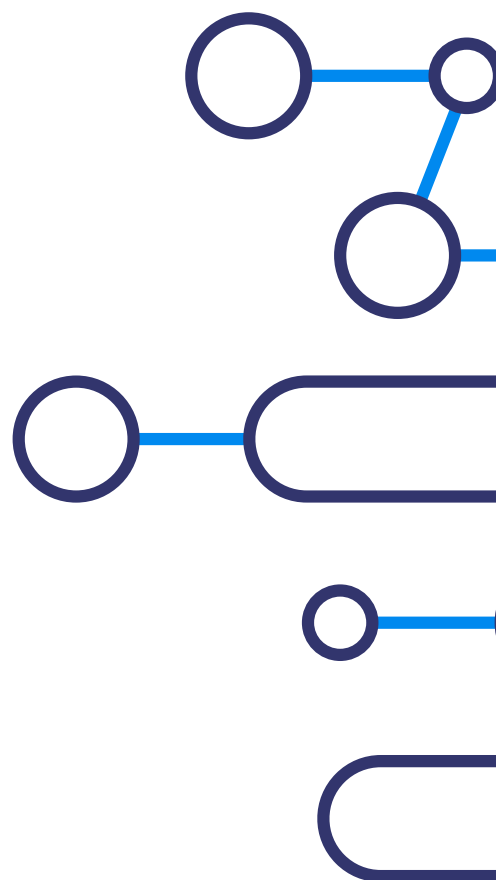
Professionally crafted fake job and internship scams may steer victims toward cheque fraud and identity data harvesting, with documented financial losses running into millions of euros annually. **Impersonation and account hijacking** on Instagram operate through direct messages engineered to provoke curiosity or trust. “Account verification” and “copyright warning” campaigns alarm page administrators into surrendering credentials; looped livestreams impersonating celebrities solicit “verification fees” from younger adolescents. A qualitatively more severe variant is sextortion: organised criminal networks build trust through romantic messaging, solicit intimate images, and then extort victims under threat of distribution.

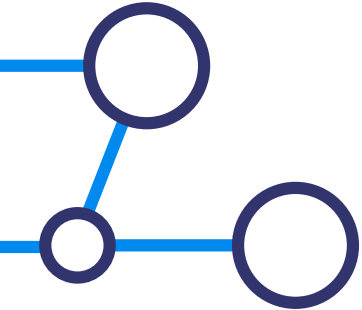


Marketplace fraud and disinformation on Facebook operate through two distinct but equally exploitative mechanisms. Fake listings for phones, tickets, and gaming products steer users to fraudulent payment pages, with scam funnels frequently redirecting victims across platforms, before reaching cloned payment forms. In parallel, coordinated disinformation campaigns exploit Facebook's engagement-driven algorithm to amplify false or emotionally charged content; corrections rarely reach the same audience as the original false claim, and the emotional impression persists long after a retraction.

Misinformation and scam redirects on TikTok

exploit the speed and emotional register of short-form video. Viral content falsely advertising scholarships, state payments, or rewards drives users toward malicious links. TikTok's For You Page algorithm amplifies content based on engagement rather than accuracy, meaning false but emotionally charged videos spread as effectively as verified information. In small, tightly connected societies already targeted by external information operations, this structural vulnerability carries risks that extend beyond individual harm. Beneath these threat profiles lies a fifth risk identified across every partner country report: **the unintended exposure of personal data through habitual oversharing**. Identity details, location patterns, and relationship information shared routinely across platforms provide the raw material for targeted social engineering without any technical intrusion being required.





DIGITAL BEHAVIOUR OF YOUTH

According to Eurostat (2025), 97% of EU citizens aged 16–29 use the internet daily. Partner country data reflects this intensity. Regular internet use among 16–24-year-olds reaches 99.6% in Spain, 99.2% in Lithuania, and approaches 100% in Estonia, where 96% connect several times a day. Romanian data shows 95.7% of high-school students online every day; Turkish data documents 95.3% of 16–24-year-olds as daily social media users. Crucially, high digital competence does not automatically translate into resilience. Estonia, where 62.6% of the population holds at least basic digital skills (above the EU average of 55.6%) nonetheless records some of the highest youth exposure rates to online harm in the EU. Several behavioural tendencies recur consistently across all partner country findings:

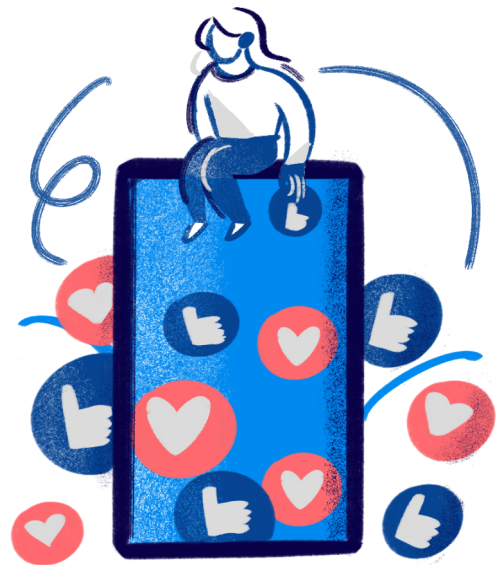
Platform-mediated socialisation as the default mode: Communication, peer validation, entertainment, and identity construction all happen through the same channels that carry threats. Applying a separate, sceptical mode of engagement to potentially risky content would require disrupting ordinary social participation.



Friction avoidance in security decisions: Accepting all permissions, reusing passwords, and skipping two-factor authentication are rational responses to systems designed to make compliance the path of least resistance. More than two thirds of young people aged 16–19 have engaged in some form of online risk-taking, frequently without awareness of having done so.

Low verification habits before sharing /

clicking: The speed and social reward structures of platform interaction normalise fast, high-frequency clicking and reposting. By the time fact-checkers flag false content, it has typically already reached millions of users; retractions rarely close this gap. Official digital safety guidance across partner countries consistently warns against reacting to “urgent” or “fear-based” content — the very categories that platforms’ own algorithms disproportionately surface.



Credential reuse and habitual oversharing:

Password reuse across accounts is common across all partner countries: a single breach creates cascading vulnerability wherever the same credentials are in use. Meanwhile, 49% of young Europeans aged 16–29 reported encountering hostile or abusive online messages in 2023, with exposure rates in the most digitally connected countries reaching as high as 69%, reflecting the personal data trails that routine platform use leaves behind.

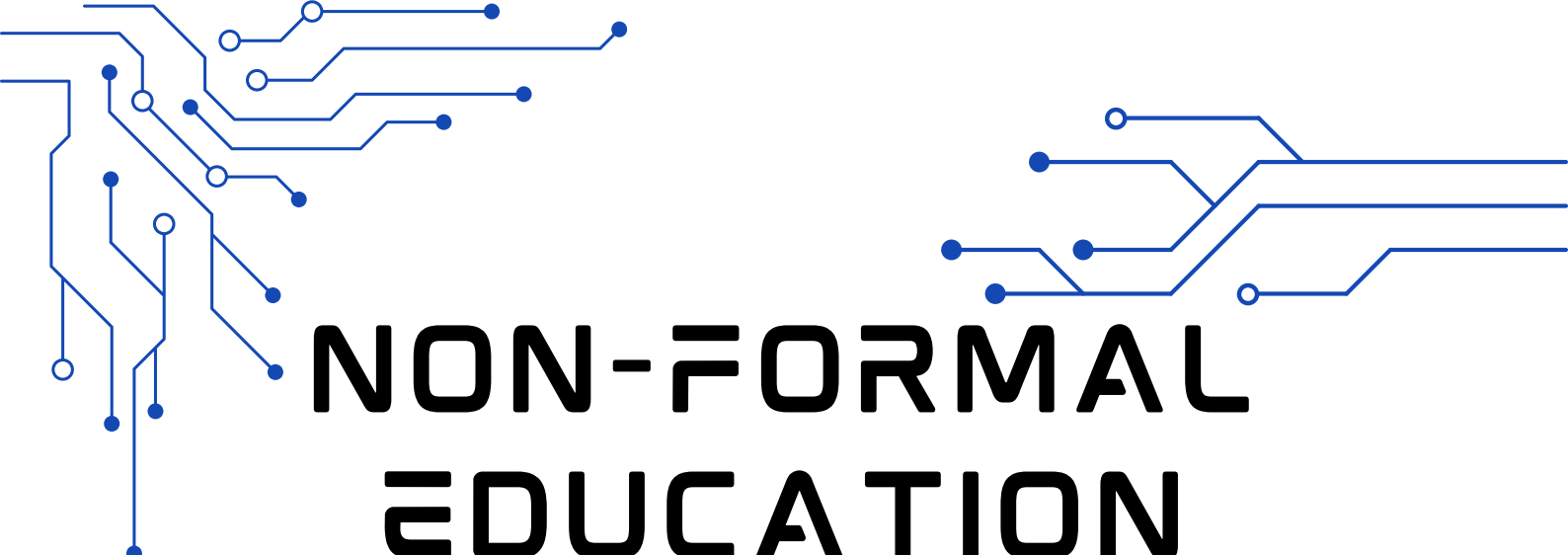
THE IMPORTANCE OF DIGITAL RESILIENCE

A conclusion across partner country reports is that awareness alone does not produce safe behaviour. Young people who broadly understand that phishing exists still click suspicious links; those who know that password reuse is risky still maintain the same credentials across multiple platforms. The gap between knowing and doing is not a deficit of information. It is a reflection of how decisions are made under conditions of speed, social pressure, habitual platform use, and persuasive design.

Closing that gap requires the active development of digital resilience. Digital resilience, as understood within ESCAP(E+), is the capacity to recognise a threat in context, make a considered decision under uncertainty, recover from a mistake, and act as a resource for others in one's network. It is both an individual and a social competence — and this distinction matters. The most effective vector for both risk and protection among young people is the peer network itself: behaviours, including safe behaviours, spread through the same social channels as threats do. Peer-to-peer corrections are more effective than institutional statements; discussing suspicious content with friends is among the most powerful defences against disinformation.

Resilience, is not only something that individuals build, it is something communities practice. All six partner country reports converge on the same pedagogical recommendation: Effective cybersecurity education for youth must be practical, scenario-based, and grounded in the platforms and behaviours that young people actually engage with. Scenario-based training equips learners with recognition skills rather than rules to memorize. “Rapid-response guidance” (knowing what to do in the first minutes after something goes wrong) is a discrete and teachable competence. Critical evaluation habits matter even among technically proficient users who may be overconfident in their ability to spot manipulation. And beyond skills, there is a cultural dimension: Young people need the confidence to seek help without shame, and a peer environment that normalises doing so. The psychological devastation documented in sextortion and disinformation cases, where the absence of that confidence proved decisive, makes this not merely a pedagogical preference but a safeguarding imperative. Experiential approaches may produce more durable and transferable change than passive information transfer. Embodied, tested knowledge, which holds together with clarity about where to turn when something goes wrong and a peer culture that normalises seeking help, is what digital resilience looks like in practice.





NON-FORMAL EDUCATION METHODOLOGY

WHAT IS NON-FORMAL LEARNING

The main characteristic of non-formal learning is that it refers to organised educational activities that take place outside the formal school system. They are designed to support personal, social and professional development. Non-formal learning is flexible, learner-centered and often voluntary. This is its main difference from formal education, which follows a structured curriculum, leads to certification and is delivered through institutions such as schools and universities.

Non-formal learning typically occurs in settings such as youth organisations, community groups, workshops, training programmes or initiatives like this ESCAP(E+) project which is co-funded under the Erasmus+. It lays a special focus on the needs, interests and active participation of learners. That is why it prioritises experiential learning, in contrast to the traditional formal learning that focuses primarily on theoretical knowledge.

Under the “learning by doing” framework, activities such as group discussions, role-playing, simulations, peer-to-peer exchanges and project-based tasks are promoted, because they engage participants actively in the learning process. This approach allows learners to connect new knowledge with their own experiences, making learning more meaningful and relevant to real-life situations.

Moving on, the role of the facilitator is of utmost importance. While in formal learning environments, traditional teachers simply transmit knowledge, in non-formal learning settings facilitators guide, support and create opportunities for learners to explore ideas, reflect and collaborate. The learning process is often horizontal, meaning that participants learn from each other, the so called: “peer learning”, as much as from the facilitator. This fosters a sense of ownership, empowerment and mutual respect within the group.

Furthermore, non-formal learning lays emphasis on developing transversal skills, often referred to as “soft skills.” These include communication, teamwork, critical thinking, problem-solving, creativity and digital competence. In the context of today’s rapidly changing world, such skills are essential for active citizenship, employability and lifelong learning. For example, in ESCAP(E+) project which deals with cyber awareness, non-formal learning involves analysing real-life online scenarios, discussing digital risks and collaboratively designing strategies for safer online behaviour. All these topics are being addressed throughout ESCAP(E+)’s toolkit.

In addition, non-formal learning programmes are characterised by their flexibility, because they can be adapted to different age groups, backgrounds and learning levels. They are particularly effective in reaching diverse audiences, including young people with fewer opportunities, as they can be tailored to be inclusive and accessible. There is usually no formal assessment or grading. Instead, reflection and constructive feedback are used to support both learning and personal growth.

What is worth mentioning is that non-formal learning complements both formal and informal learning. While formal education provides structured knowledge and qualifications and informal learning occurs naturally through daily experiences, non-formal learning bridges the gap by offering intentional yet flexible learning opportunities. In other words, it creates spaces where individuals can experiment, express themselves and build confidence in a supportive environment.

Concluding, non-formal learning is a dynamic and participatory approach that empowers individuals to actively engage in their own learning process. By focusing on experience, collaboration and real-life application, it plays a crucial role in fostering personal development, social inclusion and active participation in society.

WHY GAMIFICATION WORKS IN YOUTH WORK

To start with, let's clarify what gamification is. First of all, gamification refers to the use of game elements, such as points, challenges, storytelling, rewards and competition, in non-game contexts in order to enhance engagement and learning. Especially, in youth work, gamification has proven particularly effective because it aligns closely with how young people naturally learn, interact and stay motivated.

Undoubtedly, gamification works in youth work for many reasons. First of all, it increases motivation and engagement. Traditional learning approaches can sometimes feel passive or disconnected from young people's interests. By contrast, gamified activities introduce elements of fun, challenge and curiosity. When young people are presented with missions, levels or problem-solving tasks, they become active participants rather than passive recipients. This sense of involvement encourages sustained attention and deeper engagement.

Secondly, gamification supports experiential learning, a core principle of youth work and non-formal learning as we have analysed in the previous section. Instead of simply receiving information, participants learn by doing through simulations, role-playing or interactive challenges. This is closely linked to the ideas of David Kolb, who emphasised that knowledge is created through experience and reflection. In a gamified setting, young people can test decisions, make mistakes in a safe environment and immediately see the consequences of their actions. This makes learning more meaningful and easier to retain.

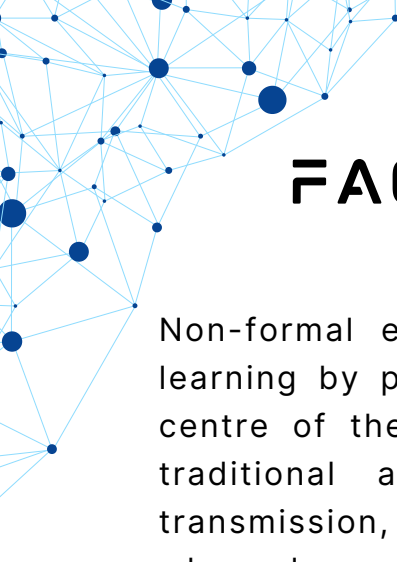
Third, gamification promotes intrinsic motivation, because it often includes rewards such as badges or points. However, its real strength lies in fostering internal satisfaction, such as the feeling of achievement, progress or mastery. Elements like clear goals, instant feedback and visible progress help learners understand how they are improving. This aligns with motivational theories suggesting that autonomy, competence and relatedness are essential for meaningful engagement.

Finally, gamification is highly effective in developing soft skills and transversal competences, as many gamified activities require teamwork, communication, problem-solving and critical thinking. For example, collaborative challenges or team-based missions encourage peer-to-peer learning and social interaction. These are essential skills in youth work, particularly in areas that deal with the ESCAP(E+) project; meaning digital literacy and cyber awareness, where young people must navigate complex, real-life situations.

Lastly, it is worth stating that gamification creates a safe space for experimentation, is flexible and inclusive and resonates with the digital culture of young people. Many are already familiar with game-based environments, whether through video games or mobile apps. Bringing similar dynamics into youth work creates a sense of familiarity and relevance, bridging the gap between learning and everyday life.

Summing up, gamification works in youth work because it transforms learning into an active, engaging and meaningful experience. By combining motivation, participation and real-life application, it supports not only knowledge acquisition but also personal development and social inclusion.





FACILITATING INTERACTIVE LEARNING

Non-formal education plays a crucial role in facilitating interactive learning by placing participation, experience and collaboration at the centre of the learning process. As we have examined in 3.1, unlike traditional approaches that often rely on one-way knowledge transmission, non-formal education creates dynamic environments where learners actively engage with content, facilitators and each other.

The learning process becomes a shared experience. It's not an individual task anymore. Through methods such as group discussions, simulations, role-playing and peer-to-peer activities, learners are encouraged to contribute their own perspectives and experiences. This interaction not only makes learning more engaging but also deepens understanding, as participants reflect, question and apply knowledge in real-life contexts.

Furthermore, non-formal education promotes a safe and inclusive space where learners feel comfortable expressing ideas, making mistakes and experimenting with new approaches. This sense of psychological safety is essential for meaningful interaction, because it fosters openness, trust and mutual respect within the group.

Last but not least, as we also mentioned in 3.1 the role of the facilitator, who guides the process rather than dominates it, is of utmost importance. By encouraging dialogue and collaboration, facilitators help learners take ownership of their learning journey. This empowers participants to become active contributors, strengthening both their confidence and their ability to learn from others.

All in all, non-formal education facilitates interactive learning by transforming learners from passive recipients into active participants. It encourages dialogue, reflection and cooperation, ultimately leading to more engaging, relevant and impactful learning experiences. This is what the ESCAP(E+) toolkit aims to achieve.



HOW TO USE THIS TOOLKIT

This toolkit is designed as a practical resource that helps users navigate, select, and apply non-formal cybersecurity activities in a structured and flexible way. It is intended mainly for youth workers, trainers, educators, facilitators, and organisations working with young people, especially in non-formal learning contexts. Its purpose is to make cybersecurity education more accessible, engaging, and usable by offering ready-to-use activities that can be implemented in workshops, youth labs, training courses, school-based sessions, and community activities.

Rather than being a document that must be followed from beginning to end, the toolkit should be used as a flexible learning resource. Users can choose individual activities, combine several activities into a thematic session, or use the toolkit as part of a longer educational process on digital literacy, cybersecurity, or online safety. The toolkit is meant to support practice, not impose a fixed method. This allows facilitators and organisations to use it in ways that fit their own learning contexts, priorities, and participants.

WHO IS THIS TOOLKIT FOR?

The toolkit is primarily designed for professionals and practitioners who work with young people in learning and participation settings. This includes youth workers, youth trainers, facilitators, teachers, youth leaders, volunteers, mentors, and organisations active in youth education or digital literacy.

The activities themselves are mainly intended for use with young people aged approximately 15–30. However, the toolkit can also be relevant in mixed learning environments where other groups are involved, such as students, peer educators, community volunteers, or adults supporting young people's digital wellbeing. Its strength lies in the fact that it can be used in a wide variety of settings while remaining practical and easy to apply.

HOW THE TOOLKIT IS STRUCTURED

The toolkit is organised to help users move from understanding the broader topic to applying concrete activities. It includes background sections that explain the topic and methodology, followed by practical activities, reflection elements, and additional support resources. This means users do not need to read it in a rigid order. They can begin with the introductory sections if they want conceptual understanding, or go directly to the activities if they need practical material for a session.

Each activity follows a consistent structure so that users can quickly understand how to apply it. In general, activities include a title, learning objectives, target group, duration, group size, materials needed, step-by-step instructions, reflection questions, and key learning messages. This makes it easier to compare activities and choose the one that best fits the available time, the learning objectives, and the profile of the group.

RECOMMENDED SESSION FORMAT

The toolkit works best when activities are used in an interactive format. Since the methods are based on non-formal learning, participants should be actively involved through discussion, teamwork, reflection, problem-solving, role-play, or scenario-based tasks. The goal is not only to provide information, but also to help participants explore, question, and apply what they learn.

A simple recommended format for using an activity is the following:

1. Opening

Begin with a short introduction to the topic and the aim of the session. This should help participants understand why the theme matters and what they will explore.

2. Activity implementation

Run the selected activity following the instructions provided in the toolkit. Depending on the format, this may involve pair work, small-group work, plenary discussion, or practical task-solving.

3. Reflection

After the activity, invite participants to reflect on what happened, what they noticed, and what they learned. Reflection is important because it helps transform the experience into a meaningful learning outcome.

4. Key messages

Close the session by highlighting the main takeaways and practical lessons participants should remember and apply.

As a general guideline, the toolkit can support short sessions of 30–45 minutes, standard workshops of 60–90 minutes, or longer sessions that combine several activities around one topic. Facilitators can also use several activities across a series of sessions if they want to build a broader learning process over time.

TARGET GROUPS

Although the toolkit as a resource is mainly used by facilitators and youth professionals, the activities are designed primarily for young people. The main participant profile includes young people who are active online and may be exposed to risks such as phishing, scams, identity theft, fake profiles, misinformation, manipulation, privacy breaches, or unsafe digital habits.

At the same time, the toolkit can also be used with participants who have lower digital confidence or more limited prior knowledge. Some activities may be particularly useful for mixed groups, including participants with different levels of experience, confidence, or access to technology.

When choosing activities, users should consider:

- the age of participants
- their familiarity with online platforms and digital tools
- their previous knowledge of cybersecurity topics
- their confidence in group work and discussion
- the learning setting, such as a youth centre, school, training course, or local workshop

This helps ensure that the selected activity is appropriate, relevant, and realistic for the specific group.

ADAPTING ACTIVITIES TO DIFFERENT GROUPS

The toolkit is intended to be adaptable. Activities do not need to be implemented in exactly the same way every time. Users are encouraged to adjust the level, examples, pace, and format according to the needs of the participants.

For younger groups or participants with lower digital confidence, activities can be simplified by using more familiar examples, shorter instructions, and clearer practical tasks. For older or more experienced groups, the same activity can be expanded through more complex scenarios, deeper analysis, or additional reflection tasks. In some cases, activities may need to be shortened, split into stages, or supported with more explanation.

Adaptation can include:

- simplifying the language used in instructions
- changing examples so they reflect the platforms and situations participants know
- reducing the number of steps or discussion questions
- extending the reflection stage for groups ready for deeper analysis
- replacing digital elements with paper-based or discussion-based alternatives when access to devices is limited

This flexibility is important because different groups learn in different ways, and not all participants come with the same experiences, confidence, or digital habits. A toolkit is most useful when it can be adjusted without losing its core purpose.



HOW TO CHOOSE THE RIGHT ACTIVITY

Users should select activities according to the purpose of their session. Some activities are better suited to introducing a topic, while others are more useful for practicing decision-making, discussing real-life online situations, or reflecting on personal digital behaviour.

The toolkit can be used:

- to introduce basic cybersecurity concepts
- to explore a specific topic such as phishing, scams, privacy, fake profiles, password safety, or misinformation
- to encourage teamwork and problem-solving
- to support reflection after a workshop or youth lab
- to complement broader activities on digital citizenship, participation, or media literacy

Choosing the right activity also means being realistic about time, group size, and the attention span of participants. It is often better to use one activity well, with enough time for reflection, than to rush through several activities without meaningful learning.

This toolkit should be used as a flexible and user-friendly resource that supports the planning and delivery of non-formal cybersecurity learning. It helps users identify suitable activities, understand how they are structured, and adapt them to different contexts and participant profiles. By combining practical methods with relevant digital themes, it supports engaging and meaningful learning experiences that help young people better understand online risks and respond to them more confidently.



The background is a solid dark blue. On the left side, there is a large, stylized graphic of a circuit board or a brain-like structure composed of white lines and dots. In the top right corner, there are some faint, concentric circular lines. In the middle right, there is a small, white, geometric shape resembling a stylized 'E' or a circuit component. In the bottom right corner, there are some faint, concentric circular lines and a small number '23'.

LEARNING ACTIVITIES

ESCAP(E+): MISINFORMATION DETECTIVE TEAM EDITION

LEARNING OBJECTIVES

Objective 1	Develop the ability to identify misinformation and misleading content.
Objective 2	Understand how information can be true, false or taken out of context.
Objective 3	Strengthen critical thinking, teamwork and decision-making skills.

TARGET GROUP

Audience	Young people (16-30), youth workers and educators
Prior Knowledge	Basic experience using social media and online content

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 55-60 min Debrief: 15-20 min

GROUP SIZE

Min / Max	10-20
------------------	-------

MATERIALS NEEDED

Physical	None
Digital	Kahoot, phones/laptops, screen/projector https://kahoot.it/challenge/04208904?challenge-id=36d2f2fd-bdf0-447c-96fb-149651d2390a_1775577027740
Preparation	Create Kahoot quiz Prepare explanations Select key questions for discussion

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - Introduce the concept of misinformation.

Explain key ideas:

- not all information online is accurate
- some content is misleading rather than completely false
- importance of verifying information and thinking critically

Step 2: Explain the activity (10 min) - Explain that participants will take part in a gamified quiz using Kahoot. For each question, they must:

- decide if the content is true, false or misleading
- answer within a limited time
- reflect on their choices

Step 3: Kahoot quiz (30-35 min) - Participants answer a series of questions using Kahoot.

For each question, participants must:

- analyse the content
- select the correct answer within the time limit

Each question follows the same format: participants must decide whether the content is true, false or misleading.

Step 4: Answer reveal and discussion (20-25 min)

After each question:

- review the correct answer shown in Kahoot
- briefly ask participants why they chose their answer
- explain why the content is true, false or misleading

For previous selected questions, allow a short discussion to explore the reasoning in more depth.

Highlight:

- what makes the content believable
- what signals misinformation

Step 5: Final debrief (15-20 min) - Summarize key learning points.

Discuss how participants can:

- verify information
- avoid spreading misinformation
- apply these skills in daily life

DEBRIEFING QUESTIONS

- 1 Which case was the most difficult to evaluate?
- 2 What made some information seem believable?
- 3 Why is misleading information dangerous?
- 4 How did working in teams influence your decisions?
- 5 What strategies can you use to verify information?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Not all information online is completely true or false
- ✓ Key message 2: Some content is misleading or taken out of context
- ✓ Key message 3: Always check sources and verify information
- ✓ Key message 4: Think critically before sharing content

ESCAP(E+): DIGITAL TRAP - ESCAPE THE SCAM!

LEARNING OBJECTIVES

Objective 1	Develop the ability to identify common online scam tactics
Objective 2	Understand how scams use urgency, manipulation and deception
Objective 3	Strengthen critical thinking and safe decision-making online

TARGET GROUP

Audience	Young people (16-30), youth workers and educators
Prior Knowledge	Basic understanding of social media and online communication

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 55-60 min Debrief: 15-20 min

GROUP SIZE

Min / Max	10-20
-----------	-------

MATERIALS NEEDED

Physical	None
Digital	Laptop, projector and google forms (escape room)
Preparation	Create and test the google forms escape room Set up sections and answer-based navigation (correct / incorrect answers) Prepare instructions for participants Prepare follow-up discussion questions

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - Introduce the topic of online scams.

Briefly explain key concepts:

- Online scams
- Urgency and manipulation
- Fake websites and misleading offers

Engage participants by asking about their experiences with scams.

Step 2: Explain the activity (5 min) - Introduce the escape room as a mission.

Explain that participants must:

- Complete challenges
- Answer correctly to progress
- Identify scam tactics

Step 3: Escape room activity (15-20 min) - Participants complete the google forms escape room individually.

They go through different challenges related to:

- Scam messages
- Fake websites
- Misleading offers
- Personal data safety

Step 4: Group discussion (20-25 min) - Review the challenges with the group.

Ask participants to explain their answers and reasoning.

Highlight key scam tactics:

- Urgency
- Emotional manipulation
- Misleading information

Step 5: Group Activity - create a scam challenge (20-25 min) - Divide participants into small groups. Each group creates a short scam scenario and turns it into a mini challenge (similar to escape room).

They must include:

- A short situation
- A question
- Multiple choices

Groups present their challenge and others try to identify the scam.

DEBRIEFING QUESTIONS

- 1 What was the most difficult challenge and why?
- 2 Which scam tactic did you find most convincing?
- 3 Why do people fall for online scams?
- 4 What will you do differently after this activity?
- 5 How can you help others stay safe online?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Online scams often look realistic and trustworthy
- ✓ Key message 2: Urgency and emotional pressure are common manipulation tactics
- ✓ Key message 3: Always verify links, sources and requests for personal data
- ✓ Key message 4: Think before you click and protect your personal information

ESCAP(E+): TRUST OR TRAP? - FAKE PROFILE INVESTIGATION

LEARNING OBJECTIVES

Objective 1	Develop the ability to identify fake profiles on social media
Objective 2	Understand common signs of online deception and impersonation
Objective 3	Strengthen decision-making and critical thinking skills online

TARGET GROUP

Audience	Young people (16-30), youth workers and educators
Prior Knowledge	Basic experience using social media platforms

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 55-60 min Debrief: 15-20 min

GROUP SIZE

Min / Max	10-20
-----------	-------

MATERIALS NEEDED

Physical	None
Digital	<i>Optional: laptop, projector or slides to present scenarios</i>
Preparation	Prepare fake profile scenarios Prepare guiding questions for discussion Prepare visual examples of fake profiles (optional)

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - Introduce the topic of fake profiles on social media.

Explain key concepts:

- Fake profiles
- Impersonation
- Online risks (scams, manipulation, data theft)

Step 2: Explain the activity (5 min) - Explain that participants will analyse different situations and decide what to do. They must:

- Identify suspicious elements
- Make a decision
- Explain their reasoning

Step 3: Scenario Analysis (30-35 min) - Present fake profile scenarios one at a time. Participants:

- Analyze the situation
- Decide what they would do
- Discuss in pairs or small groups

Encourage participants to justify their decisions.

Step 4: Group discussion (20-25 min) - Discuss each scenario with the whole group. Ask:

- What are the red flags?
- What would you check?
- Why is this risky?

Step 5: Final debrief (15-20 min) - Summarize key learning points and connect to real-life behaviour.

Discuss how participants can protect themselves from fake profiles.

Scenarios

Scenario 1: Suspicious follow request

You receive a follow request from a profile with:

- Very few photos
- No bio
- Recently created account

What would you do? Why?

Scenario 2: Unknown message

A profile sends you a message: "Hey, I think we met before. Can you help me with something?"

How would you respond?

Scenario 3: Professional but Suspicious Profile

A profile looks professional but:

- Images look like stock photos
- Very low interaction

Is this profile trustworthy? Why or why not?

Scenario 4: Moving to Another Platform

Someone asks you to continue the conversation on WhatsApp or Telegram.

Why could this be risky?

DEBRIEFING QUESTIONS

- 1 What made you suspicious about the profiles?**
- 2 Which scenario was the most difficult to evaluate?**
- 3 Why do people trust fake profiles?**
- 4 What would you check before trusting a profile?**
- 5 How can you protect yourself online?**

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Fake profiles can look realistic and trustworthy**
- ✓ Key message 2: Not all online interactions are safe or genuine**
- ✓ Key message 3: Always verify profiles before engaging**
- ✓ Key message 4: Be cautious when sharing personal information**

ESCAP(E+): VIRAL OR MANIPULATED? SOCIAL MEDIA ROLE-PLAY

LEARNING OBJECTIVES

Objective 1	Understand how social media content can influence opinions and behaviour
Objective 2	Identify common manipulation tactics (clickbait, emotional content, misinformation)
Objective 3	Develop critical thinking when engaging with viral content

TARGET GROUP

Audience	Young people (16-30), youth workers and educators
Prior Knowledge	Basic experience using social media platforms

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 60 min Debrief: 15 min

GROUP SIZE

Min / Max	10-20
-----------	-------

MATERIALS NEEDED

Physical	None
Digital	None (optional use of phones if participants want to simulate social media)
Preparation	Prepare role-play scenarios Assign roles for each group

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - Introduce the topic of social media manipulation.

Briefly explain key concepts:

Viral content

Manipulation

Emotional influence

Step 2: Explain the activity (5 min) - Explain the role-play and objectives.

Divide participants into groups of 3 and assign roles:

Content creator

User

Observer

Step 3: Scenario distribution (5 min) - Give each group one scenario and make sure participants understand the task (create a short social media interaction that includes manipulation).

Step 4: Role-play preparation (15 min) - Groups prepare their role-play.

They must:

Create a short post

Include a manipulation tactic

Prepare a short interaction

Step 5: Role-play performance (25 min) - Each group performs their role-play (1-2 minutes each). Other participants observe and identify the manipulation tactics used.

Step 6: Group analysis (10-15 min) - After each performance, ask:

What is the manipulation tactic?

Why is it misleading?

Step 7: Final Debrief (15 min) - Facilitate reflection and connect to real-life social media behaviour

Scenarios

Scenario 1: Clickbait

A post is designed to attract attention using an exaggerated or misleading title. The task is to create a short interaction where the content uses a dramatic or exaggerated message to make people click or react.

Scenario 2: Emotional manipulation

A post is spread online that tries to make people feel strong emotions in order to influence their reactions. The task is to create a short interaction where the content uses fear, anger, or sympathy to make people believe and/or share it.

Scenario 3: Misleading information

A post shares information that is partially true but presented in a misleading way. The task is to create a short interaction where the content includes incomplete or distorted information.

Scenario 4: Influencer promotion

An influencer promotes a product or idea without clearly explaining all the details. The task is to create a short interaction where the audience is influenced without full transparency.

DEBRIEFING QUESTIONS

- 1 Which role was most challenging and why?**
- 2 Which manipulation tactic was most convincing?**
- 3 How did it feel to be influenced or to influence others?**
- 4 Why does manipulated content spread so easily?**
- 5 How can you protect yourself online?**

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Not everything that goes viral is true**
- ✓ Key message 2: Social media content is often designed to influence behaviour**
- ✓ Key message 3: Emotional content spreads faster and is more persuasive**
- ✓ Key message 4: Critical thinking is essential when consuming online content**

ESCAP(E+): HOOKED OR NOT? PHISHING PROBLEM SOLVING CHALLENGE

LEARNING OBJECTIVES

Objective 1	Develop the ability to identify phishing attempts across email, SMS and social media.
Objective 2	Understand the techniques attackers use to deceive victims, including urgency, impersonation and social engineering.
Objective 3	Apply practical strategies to verify suspicious messages and protect personal data.

TARGET GROUP

Audience	Young people aged 16–30, youth workers and educators.
Prior Knowledge	Basic experience using email, messaging apps and social media platforms.

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 55–60 min Debrief: 15–20 min

GROUP SIZE

Min / Max	10–20 participants (working in small groups of 3–5)
-----------	---

MATERIALS NEEDED

Physical	Printed scenario cards (one set per group), flip chart or whiteboard for group notes, markers, sticky notes for voting
Digital	Laptop and projector to display scenarios (optional), presentation slides with key vocabulary and scenario visuals.
Preparation	Print scenario cards for each group. Prepare a brief introductory presentation on phishing concepts. Prepare guiding questions for each scenario. Familiarise yourself with the scenarios and their correct red flags so you can guide discussions confidently

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min)

Introduce the topic of phishing. Explain that phishing is one of the most common cyber threats and that anyone can be targeted.

Ask the group: “Has anyone ever received a suspicious email or message? What made it seem off?”

Use responses to open the discussion without shaming. Briefly explain key concepts:

Phishing – a fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source.

Spear phishing – a targeted phishing attack aimed at a specific person or organisation.

Smishing – phishing via SMS text messages.

Vishing – phishing via voice calls.

Social engineering – manipulating people into giving up confidential information.

Step 2: Explain the Activity (5 min)

Explain that participants will work in small groups to analyse realistic phishing scenarios. For each scenario, they must: identify the red flags and suspicious elements, decide what action they would take and prepare a brief explanation of their reasoning to share with the whole group. Divide participants into groups of 3–5 and distribute one scenario card per group.

Step 3: Scenario Analysis (30–35 min)

Groups analyse their assigned scenarios. The facilitator circulates between groups to provide guidance and ask probing questions.

After 15 minutes, groups rotate scenario cards so each group analyses at least two different scenarios.

Scenarios:

Scenario 1 (Urgent Bank Email): You receive an email from “your bank” saying your account has been compromised. It asks you to click a link and verify your identity immediately or your account will be frozen. The email address is support@b4nk-secure.com. The link goes to b4nk-secure.com/verify. Red flags: misspelled domain, urgency, generic greeting.

Scenario 2 (Prize SMS): You receive a text message: “Congratulations! You’ve won a 500 euro gift card. Claim it now at bit.ly/fr33prize. Offer expires in 1 hour!” Red flags: unsolicited prize, shortened URL, time pressure, too good to be true.

Scenario 3 (Social Media Friend Request): You receive a message from a friend’s account saying: “Hey, is this you in this video? It looks really embarrassing!” with a link. When you check, your friend’s profile looks slightly different and was created recently. Red flags: emotional bait, suspicious link, cloned account.

Scenario 4 (Job Offer Email): You receive an email offering you a remote job with a high salary. The company name sounds legitimate, but the email asks you to provide your national ID, bank details and a “processing fee” before starting. Red flags: request for personal/financial data upfront, processing fee, unsolicited job offer.

Scenario 5 (IT Department Request): You receive an email from “IT Support” at your school or workplace asking you to update your password by clicking a link. The sender address is it-support@yourschool.mail-update.com. Red flags: subdomain trick, urgency, link to external domain instead of official site.

Step 4: Group Presentations and Discussion (20–25 min)

Each group presents their scenario analysis to the whole group (2–3 minutes per group).

After each presentation, the facilitator asks: What are the key red flags? What would you do in this situation?

What information was the attacker trying to obtain? Encourage other groups to add observations. Highlight common patterns across scenarios: urgency, impersonation, emotional triggers and requests for sensitive information.

Step 5: Final Debrief (15–20 min)

Summarise the key learning points from all scenarios. Discuss practical steps participants can take: always verify the sender’s address carefully, never click links in unsolicited messages, contact organisations directly using official channels, enable two-factor authentication, report suspicious messages. Connect the learning to real-life behaviour and ask participants to share one action they will take after the session.

DEBRIEFING QUESTIONS

- 1 Which phishing scenario was most convincing and why?
- 2 What red flags did you find most difficult to spot?
- 3 Have you or someone you know ever fallen for a phishing attempt? What happened?
- 4 Why do phishing attacks continue to be so effective despite awareness campaigns?
- 5 What specific steps will you take to protect yourself from phishing in the future?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Phishing is the most common form of cyberattack and it targets everyone – no one is immune regardless of age or technical skill.
- ✓ Key message 2: Attackers exploit urgency, fear and trust to trick people into revealing sensitive information. Recognising these emotional triggers is the first line of defense.
- ✓ Key message 3: Never click links or provide personal information in response to unsolicited messages. Always verify through official channels.
- ✓ Key message 4: Reporting suspicious messages helps protect not just yourself but your entire community. When in doubt, stop, think and verify.

ESCAP(E+): SCROLL SMART SOCIAL MEDIA MANIPULATION QUIZ

LEARNING OBJECTIVES

Objective 1	Recognise common social media manipulation tactics such as clickbait, emotional exploitation and fake engagement.
Objective 2	Understand how algorithms and user behaviour contribute to the spread of manipulative content online.
Objective 3	Strengthen critical thinking, teamwork and decision-making skills when engaging with social media content.

TARGET GROUP

Audience	Young people aged 16–30, youth workers and educators.
Prior Knowledge	Basic experience using social media platforms (e.g. Instagram, TikTok, X/Twitter, Facebook).

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Quiz: 50 min (3 rounds) Debrief: 25 min

GROUP SIZE

Min / Max	10–30 participants (can play individually or in teams of 2–4)
-----------	---

MATERIALS NEEDED

Physical	Whiteboard or flip chart for notes during debrief, printed fallback question cards (in case of technical issues).
Digital	Facilitator laptop or tablet connected to a projector or large screen. Participants use smartphones or devices with internet access (one per participant or per team). Platform: Kahoot! (kahoot.com) – free account. Participants join via kahoot.it or the Kahoot app using a game PIN.

Preparation

Create a free Kahoot! account at kahoot.com. Build the quiz using the questions and answer options provided in the facilitation guide below. Set each question timer to 20 seconds for standard questions and 30 seconds for scenario-based ones. Run a test on your own device to confirm the game PIN system works. Prepare a slide with the session agenda and key vocabulary (clickbait, algorithm, bot, emotional manipulation, astroturfing). If internet access is unreliable, prepare printed fallback question cards.

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) – Welcome participants and frame the session: Social media is a powerful tool, but it is also used to manipulate opinions, emotions and behaviour, often without us realising it.

Ask the group: “Have you ever shared a post and later found out it was misleading? What made it convincing?”

Use responses to generate curiosity without shaming.

Briefly explain the structure: three quiz rounds with a competitive leaderboard, followed by a group debrief.

Key vocabulary to introduce quickly (2 minutes):

- Clickbait – content designed to attract clicks using exaggerated or misleading headlines.
- Algorithm – a system that decides what content you see based on your behaviour.
- Bot/Fake account – automated or fake profiles used to amplify content or opinions.
- Emotional manipulation – content designed to trigger strong feelings to influence reactions.
- Astroturfing – making a manipulated campaign look like a grassroots movement.

Step 2: Join the Game (5 min) – Display the game PIN on screen. Ask participants to open kahoot.it on their phone (or the Kahoot app) and enter the PIN. They choose a nickname (for themselves or their team). If playing in teams, assign teams and have one person per team join on behalf of the group.

Step 3: Round 1 – Warm-Up Quiz (15 min, 5 questions) – Launch Round 1 in Kahoot.

These questions establish baseline knowledge in a low-stakes, playful way. After each question, Kahoot reveals the correct answer automatically.

STEP-BY-STEP FACILITATION GUIDE

Take 30 seconds after each question to briefly explain why – especially for wrong answers that reveal common misconceptions.

Round 1 Questions:

Q1. What is “clickbait”?

(a) A type of computer virus | (b) Content with exaggerated headlines designed to get clicks | (c) A social media privacy setting | (d) A tool for blocking ads

→ Correct: B

Q2. Which of the following is a sign that a social media account might be fake?

(a) It has a profile photo | (b) It was created very recently, has few followers, and posts repetitive content | (c) It follows celebrities | (d) It uses hashtags

→ Correct: B

Q3. Why does emotionally charged content spread faster on social media?

(a) It is always more accurate | (b) Algorithms prioritise content that generates strong reactions | (c) Only emotional people use social media | (d) It is promoted by governments

→ Correct: B

Q4. True or false: If a post has thousands of likes and shares, the information in it must be true.

(a) True | (b) False

→ Correct: B

Q5. What is “astroturfing” in the context of social media?

(a) A gardening trend popular on Instagram | (b) Creating the false impression that a campaign has widespread grassroots support | (c) Using green filters on photos | (d) Planting trees as part of an online challenge

→ Correct: B

Step 4: Round 2 – Scenario Quiz (20 min, 5 questions) – These questions present realistic situations. Participants must apply what they have learned rather than recall a fact. Set timers to 30 seconds.

After each scenario, spend up to one minute on discussion.

Ask a participant who got it right to explain their reasoning before you confirm.

Round 2 Questions (Scenario-Based):

Q6. Lena sees a post claiming “BREAKING: A major European city bans all social media for under-18s” The post has no source link and uses dramatic language. What should she do?

(a) Share it immediately to warn her friends | (b) Comment asking if it is true | (c) Search for the story on trusted news sites before reacting | (d) Report the post as spam

→ Correct: C

Q7. Marco notices that a trending hashtag is being used by hundreds of accounts that all post the same message, were created in the same week, and have no personal photos. What is most likely happening?

(a) A popular new challenge | (b) A coordinated bot campaign to manipulate public opinion | (c) A glitch in the platform | (d) A marketing strategy by a well-known brand

→ Correct: B

Q8. Sofia follows an influencer who posts about a “miracle health supplement.” The influencer does not disclose being paid for the post. What manipulation tactic is being used?

(a) Clickbait | (b) Emotional manipulation | (c) Hidden sponsored content / undisclosed advertising | (d) Phishing

→ Correct: C

Q9. A viral video shows a politician saying something outrageous. The clip is only 10 seconds long and cuts mid-sentence. What should you consider?

(a) Politicians always say outrageous things, so it must be real | (b) The clip may be taken out of context or edited to change the meaning | (c) If it is viral, it must be accurate | (d) Short clips are always more trustworthy → Correct: B

Q10. During election season, Amir sees an emotional post about a candidate that includes shocking statistics but no source. He notices the post is shared mostly by accounts with no personal content. What combination of manipulation tactics is at play?

(a) Clickbait and astroturfing | (b) Emotional manipulation and coordinated inauthentic behaviour | (c) Phishing and identity theft | (d) Spam and hacking

→ Correct: B

Step 5: Challenge Round and Debrief (25 min) – The challenge round features harder questions and a shorter timer (15 seconds). These are designed to stretch participants who found the earlier rounds easy.

The facilitator should build up the tension – announce that points are doubled in this round.

Challenge Round Questions:

Q11. A social media platform's algorithm is most likely to show you content that:

- (a) Is the most factually accurate | (b) Keeps you scrolling by matching your existing interests and emotional triggers | (c) Is the most recently posted | (d) Has been verified by fact-checkers

→ Correct: B

Q12. Which of the following is the BEST strategy to protect yourself from social media manipulation?

- (a) Only follow accounts with large follower counts | (b) Cross-check information with multiple reliable sources, question emotional reactions, and verify before sharing | (c) Avoid social media entirely | (d) Only read content from people you know personally

→ Correct: B

Q13. A friend sends you a petition link saying "Sign now – 1 million people already have!" The website looks unofficial, asks for personal data, and the cause is vaguely described. What is the most likely risk?

- (a) It is a legitimate campaign | (b) It is a data harvesting scheme using social pressure to collect personal information | (c) It is a government survey | (d) It is a school project

→ Correct: B

Display the final Kahoot leaderboard. Acknowledge top scorers briefly. Then transition into the debrief: step away from the game format and invite reflection. Use the debriefing questions below.

DEBRIEFING QUESTIONS

- | | |
|---|---|
| 1 | Which question surprised you most and what did you learn from it? |
| 2 | Have you ever been influenced by manipulative content without realising it? What made it convincing? |
| 3 | Why does manipulative content spread so easily on social media? What role do algorithms play? |
| 4 | How did working in teams influence your decisions? Did you change your mind after discussing with others? |
| 5 | What is one specific habit you will change when consuming or sharing content on social media? |

KEY CYBERSECURITY MESSAGES



Key message 1: Not everything that goes viral is true. Social media content is often designed to trigger emotions and drive engagement, not to inform.



Key message 2: Manipulation tactics such as clickbait, fake accounts, emotional exploitation and astroturfing are widespread and often difficult to spot without critical thinking.



Key message 3: Always verify information by checking multiple reliable sources before believing or sharing content. Pause, question and check.



Key message 4: Understanding how algorithms work empowers you to take control of your feed and make more informed decisions about the content you consume and share.

WHO OWNS YOUR DATA? (CASE STUDY DISCUSSION ON DATA PRIVACY)

LEARNING OBJECTIVES

Objective 1	To understand how personal data is collected, stored, and used by online platforms and mobile applications
Objective 2	To identify scenarios in which personal privacy may be compromised without the user's awareness
Objective 3	To develop practical strategies for protecting personal data in everyday digital life

TARGET GROUP

Audience	Young people aged 16-25, youth workers, and educators
Prior Knowledge	Basic familiarity with smartphones and social media platforms. No technical background required.

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity: 60 min Debrief: 15 min

GROUP SIZE

Min / Max	10 - 30 participants
-----------	----------------------

MATERIALS NEEDED

Physical	Printed case study cards (one set per group), sticky notes, markers, flip chart or whiteboard
Digital	Laptop or projector for displaying instructions and prompts (optional use). Participants may use their phones to look up real privacy policies
Preparation	Prepare and print the four case study cards (One per small group). Write the discussion prompts on a chart or prepare a slide. Familiarise yourself with each case study scenario before the session.

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - Open with a short provocation: Ask participants to raise their hand if they have ever read a full privacy policy or terms of service. Use the (usually very low) response to frame the discussion. Briefly explain the concept of data privacy and why it matters for young people online. Introduce the key terms:

- Personal data (name, location, browsing habits, contacts)
- Data collection (what apps gather and why)
- Third-party sharing (who else receives your data)
- Your rights as a user (right to access, delete, withdraw consent)

Step 2: Explain the activity (5 min) - Divide participants into four groups. Explain that each group will receive a different case study based on a real-world scenario. Their task is to read the case, discuss it, and answer the guided questions on the card. Each group will then present their findings to the rest of the room.

Step 3: Case study analysis (25 min) - Distribute one case study card per group. Allow groups to read and discuss independently. Encourage them to draw on their own experiences. The facilitator circulates to prompt deeper thinking without giving away answers.

Step 4: Group presentations (15 min) - Each group presents their case (2-3 minutes each) and shares what surprised them most. Other participants may react or add connections to their own experience after each presentation.

Step 5: Step 5: Connecting the cases (5 min) - Facilitate a brief whole-group comparison: What do all four cases have in common? What patterns do participants notice about how data flows online?

Step 6: Debrief (15 min) - Use the debriefing questions below. Close by asking each participant to name one concrete action they will take to better protect their personal data.

Case Studies

Case 1: The Free App That Knows Everything

Elif (She) downloads a free flashcard study app just before her university exams. To sign up, she clicks 'Accept All' on the permissions screen without reading it. The app requests access to her microphone, contacts, location, and photo library. Three weeks later she starts receiving targeted ads for tutoring services she never searched for, and a friend mentions receiving a promotional message 'from her.'

Discussion prompts: What permissions did Elif grant? Why might an app need access to your contacts or microphone? Who might have received her data and why? What could she have done differently?

Case 2: The Social Login

Mehmet (He) signs up for a new online shopping website using the 'Continue with Facebook' button because it is faster than creating a new account. He does not notice the small text explaining that the shopping site will have access to his public Facebook profile, friend list, and email address. Over the next month, his Facebook feed fills with ads for products he browsed on the shopping site.

Discussion prompts: What data was shared when Mehmet clicked 'Continue with Facebook'? Who benefits from this arrangement and how? Is this a security risk, a privacy risk, or both? What are the trade-offs of convenience versus control?

Case 3: The Data Breach You Never Heard About

Zeynep (She) has used the same email and password for five online accounts since she was 16. One day she receives an email from an unknown sender that includes her password in the subject line. She later discovers that a smaller website she forgot she had signed up for suffered a data breach two years ago, and her credentials were sold on the web. She has never received any official notification from the site.

Discussion prompts: How did Zeynep's data end up at risk even though she did not do anything obviously wrong? What is the danger of reusing passwords across platforms? Do companies have an obligation to tell users when their data is compromised? What would you do if this happened to you?

Case 4: Location Data and the Journey You Did Not Share

Deniz (He) uses a popular mapping app for navigation and leaves location access on at all times because it is more convenient. He later reads a news article explaining that the app's parent company sells anonymised location data to third parties, including insurers and retail chains. He also discovers that his phone's photos have GPS coordinates embedded in them, and that he once accidentally shared his home address by posting a photo on social media.

Discussion prompts: Is location data sensitive even when it is described as anonymised? Who might be interested in knowing where you go every day and why? What hidden metadata might your photos contain? How would you adjust your phone settings after learning this?

DEBRIEFING QUESTIONS

- 1 Which case study felt closest to something you or someone you know has experienced? What made it feel familiar?
- 2 Did any of the cases surprise you? What assumptions about digital privacy did this activity challenge?
- 3 When companies collect data, is it always harmful? Where is the line between a useful service and an invasion of privacy?
- 4 What rights do you have over your own data? Do you think most young people know about these rights?
- 5 What is one specific, realistic change you will make this week to better protect your personal data?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Your personal data has real value. Treat every permission request and sign-up form as a decision, not a formality.
- ✓ Key message 2: 'Free' services are often funded by your data. Understanding this exchange is the first step to making informed choices online.
- ✓ Key message 3: Small habits make big differences. Using unique passwords, reviewing app permissions, and disabling unnecessary location access significantly reduce your exposure to data-related risks.
- ✓ Key message 4: You have rights. Under data protection framework, you can request access to, correction of, or deletion of your personal data held by organisations.

LEVEL UP! (GAMIFIED QUIZ ON PASSWORD SECURITY)

LEARNING OBJECTIVES

Objective 1	To recognize the characteristics of strong and weak passwords and understand why password strength matters
Objective 2	To identify common threats to password security, including phishing, and credential stuffing etc.
Objective 3	Apply good password practices such as using unique patterns, enabling two-factor authentication, and considering a password manager

TARGET GROUP

Audience	Young people aged 16-25, youth workers, and educators. Quiz is suitable for the participants whose prior cybersecurity knowledge is poor
Prior Knowledge	None required. Familiarity with smartphones and online accounts is sufficient.

DURATION

Total Time	75 minutes
Breakdown	Introduction: 10 min Quiz:45 min (3 parts) Debrief: 20 min

GROUP SIZE

Min / Max	10-30 participants (They can be play individually or in teams of 2-4 participants)
-----------	--

MATERIALS NEEDED

Physical	Whiteboard or chart for the notes during debrief, printed fallback question cards (in case of technical issues)
----------	---

Digital	A facilitator as laptop or tablet connected to a projector or large screen Participants use smartphones or digital tools with internet access (one per participant or per team) Platform: Kahoot! (kahoot.com) - Free account. Participants may directly join via kahoot.it or the Kahoot app using a game PIN
Preparation	Create a free Kahoot! account at kahoot.com. Build the quiz using the questions and answer options provided in the facilitation guide below. Set each question timer to 20 seconds for standard questions and 30 seconds for scenario-based ones. Run a test on your own device to confirm the game PIN system works. Prepare a slide with the session agenda and key vocabulary (password, brute force, 2FA, password manager). (If internet access is unreliable at the venue, prepare printed fallback question cards.)

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (10 min) - Welcome participants and frame the session: Passwords are the first line of defence for almost every online account, yet most people have habits that put them at serious risk.

Ask the group: 'How many passwords do you have? Do you reuse any of them?' Use responses to generate curiosity without shaming. Briefly explain the structure of the session: Three quiz rounds with a competitive leaderboard, followed by a group debrief.

Key vocabulary to introduce quickly (2 minutes):

- Brute force attack – a programme that tries thousands of password combinations per second
- Phishing – a fake message or site designed to steal your credentials
- Credential stuffing – using leaked username/password pairs from one breach to access other accounts
- Two-factor authentication (2FA) – a second verification step beyond the password
- Password manager – an encrypted application that stores and generates unique passwords

Step 2: Join the game (5 min) - Display the game PIN on screen. Ask participants to open kahoot.it on their phone (or the Kahoot app) and enter the PIN. They choose a nickname (for themselves or their own groups). (If playing in teams, assign teams and have one person per team join on behalf of the group.)

Step 3: Round 1 – Warm-up Quiz (15 min, 6 questions) - Launch Round 1 in Kahoot. These questions establish baseline knowledge in a low-stakes, playful way. After each question, Kahoot reveals the correct answer automatically. Take 30 seconds after each question to briefly explain why – especially for wrong answers that reveal common misconceptions. Do not lecture; keep it quick and light.

Round 1 Questions

- Q1. Which of the following is the strongest password? (a) password123 | (b) MyDog2010! | (c) Tr!4#bQz9@Lm | (d) qwerty → Correct: C
- Q2. How many characters should a strong password have at minimum? (a) 6 | (b) 8 | (c) 12 | (d) 20 → Correct: C
- Q3. Which of these makes a password easier to crack? (a) Using a mix of symbols and numbers | (b) Using your birthday | (c) Using 15+ characters | (d) Using a randomly generated string → Correct: B
- Q4. True or false: Using the same password on multiple accounts is safe as long as the password is strong. (a) True | (b) False → Correct: B
- Q5. What does two-factor authentication (2FA) do? (a) Doubles the length of your password | (b) Adds a second verification step after your password | (c) Generates two passwords at once | (d) Logs you in from two devices at the same time → Correct: B
- Q6. Which is NOT a job of a password manager? (a) Generating strong, unique passwords | (b) Storing passwords in encrypted form | (c) Sharing your passwords with trusted contacts | (d) Auto-filling login forms securely → Correct: C

Step 4: Round 2 – Scenario Quiz (20 min, 5 questions) - These questions present realistic situations. Participants must apply what they have learned rather than recall a fact. Set timers to 30 seconds. After each scenario, spend up to one minute on discussion. Ask a participant who got it right to explain their reasoning before you confirm.

Round 2 Questions (Scenario-Based)

- Q7. Selin (She) receives an email from 'Google Security' asking her to verify her password immediately or her account will be deleted. The link in the email looks slightly different from google.com. What should she do? (a) Click the link and verify her password quickly | (b) Ignore the email and delete it | (c) Check the sender address, not click the link, and go directly to google.com to check her account | (d) Forward the email to her friends to warn them → Correct: C

Q8. Ahmet (He) uses 'istanbul2005' as his password for his email, Instagram, and bank account. His email provider suffers a data breach and his credentials are leaked. What is the likely consequence? (a) Only his email is at risk | (b) All three accounts are at risk because the same password was reused | (c) His bank account is safe because banks have better security | (d) Nothing serious, since his password contains numbers → Correct: B

- Q9. Fatma (She) wants to create a password she can actually remember. Which method is most secure? (a) Her childhood nickname followed by her birth year | (b) A short but complex password like 'X@9!' | (c) A long passphrase of four random words, such as 'orange-cloud-bicycle-17' | (d) Her first name backwards with a capital letter → Correct: C

- Q10. Murat (He) has 2FA enabled on his account via SMS. A hacker somehow gets his password. Can the hacker access his account? (a) Yes, the password is enough | (b) No, because 2FA requires a second step that only Murat controls | (c) Only if the hacker also knows his username | (d) Yes, SMS codes are easy to intercept → Correct: B (Note for facilitator: briefly acknowledge that SMS-based 2FA is better than nothing, but authenticator apps are even more secure)

- Q11. A website Deniz (He) signed up for years ago emails him to say his data was breached. His password for that site is the same one he uses for his work email. What should he do first? (a) Wait to see if anything bad happens | (b) Change only the breached site's password | (c) Immediately change the password for every account that shared the same password | (d) Delete his account on the breached site → Correct: C

Step 5: Challenge Round (10 min, 3 questions) - The challenge round features harder questions and a shorter timer (15 seconds). These are designed to stretch participants who found the earlier rounds easy, and to generate surprise. The facilitator should build up the tension – announce that points are doubled in this round.

Challenge Round Questions

- Q12. A brute force attack tries every possible combination. Approximately how long does it take to crack an 8-character lowercase-only password today? (a) Several years | (b) A few weeks | (c) A few hours or less | (d) It is impossible to crack → Correct: C (Modern computers can try billions of combinations per second; 8-character lowercase-only passwords can be cracked in minutes to hours)

- Q13. Which of the following password practices provides the highest real-world protection? (a) Changing your password every 30 days | (b) Using a unique, randomly generated password for every account stored in a password manager, with 2FA enabled | (c) Writing your passwords in a notebook kept at home | (d) Using a very long password that is the same across all accounts → Correct: B

Q14. You find a website that claims to check whether your password is strong. It asks you to type in your actual password. What should you do? (a) Use it – it is a helpful security tool | (b) Only use it if the website looks professional | (c) Never type your real password into any third-party checker | (d) Use it but change the last character first → Correct: C

Step 6: Leaderboard and Debrief (20 min) - Display the final Kahoot leaderboard to participants. Acknowledge top scorers briefly. Then transition into the debrief: step away from the game format and invite reflection. Use the debriefing questions below.

DEBRIEFING QUESTIONS

- 1 Which question surprised you most, and what did you learn from it?
- 2 How many of your current passwords would you now consider weak? What makes them risky?
- 3 Have you ever reused a password across multiple accounts? How do you feel about that habit now?
- 4 What would it take for you to start using a password manager? What feels like a barrier?
- 5 What is one specific password habit you will change or adopt this week?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Password length and uniqueness matter more than complexity alone. A long passphrase of random words is both memorable and highly secure.
- ✓ Key message 2: Reusing passwords is one of the most common and dangerous habits online. A single breach can unlock every account that shares the same credentials.
- ✓ Key message 3: Two-factor authentication is one of the most effective ways to protect an account even if a password is compromised.
- ✓ Key message 4: A password manager is not a risk (It is generally a solution.) It may remove the need to remember dozens of passwords while ensuring each one is unique and strong.

SCAM UNDER ATTACK: CAN YOU STOP IT IN TIME?

LEARNING OBJECTIVES

Objective 1	To help participants understand how online scams unfold in real-life digital situations.
Objective 2	To build young people's capacity to recognize scam tactics, react safely, and make informed decisions under pressure.
Objective 3	To encourage teamwork, communication, and critical thinking when responding to online threats and suspicious digital behavior.

TARGET GROUP

Audience	Young people aged 15–25, especially those who use social media, messaging apps, online shopping platforms, gaming platforms, or online banking services.
Prior Knowledge	No prior cybersecurity training is required. Basic digital experience is enough. It is helpful if participants already use common online platforms and communication tools.

DURATION

Total Time	90 minutes (can be shortened to 75 minutes if needed)
Breakdown	Introduction: 15 min Main activity: 55 min Debrief: 20 min

GROUP SIZE

Min / Max	12–30 participants (recommended setup: participants work in small response teams of 4–6 people.)
------------------	--

MATERIALS NEEDED

Physical	• Printed scenario cards • Role cards • Team instruction sheets • Flipchart paper or whiteboard • Markers • Sticky notes • Envelopes with “new developments” or “incident updates”
-----------------	--

Digital

- Laptop
- Projector
- Slides with the attack scenario timeline
- Optional timer
- Optional sound effect or visual alert slides for added urgency

Preparation

The facilitator should prepare in advance:

- A fictional but realistic online scam scenario
- Team roles or missions
- 3–5 scenario updates/escalation cards
- A decision sheet for each team
- A short final summary on safe behaviour and reporting online scams

STEP-BY-STEP FACILITATION GUIDE

Step 1: Warm-up – “Scam or Safe?”

Start with a short group discussion. Ask participants:

- What kinds of online scams have you seen recently?
- Where do scams usually appear: email, Instagram, WhatsApp, online shops, gaming, job offers?
- Why do people still fall for scams?

Write their answers on a flipchart. Briefly explain that online scams often work not because people are careless, but because scammers are skilled at creating pressure, trust, or confusion.

Step 2: Introduce the Scenario

Tell participants that they are about to enter a simulated digital crisis.

Present the story:

A youth group is preparing for an international event. During the same day, several suspicious things start happening:

- a fake message appears about registration payment,
- someone receives a “discounted travel offer” through social media,
- a team member gets a message asking to urgently confirm account details,
- a suspicious link is being shared in the group chat,
- one participant says they may already have entered personal data.

Explain that each team must act like a digital response team. Their task is to understand what is happening, decide what to do, reduce harm, and protect others.

Step 3: Team Formation and Roles

Divide participants into teams of 4–6. Each team becomes a Cyber Response Team.

Optional roles inside each team:

- Investigator – checks clues and identifies suspicious elements
- Decision Maker – helps the group choose actions
- Communicator – presents the team’s decisions
- Recorder – writes the team’s responses
- Safety Officer – checks whether the actions are realistic and safe

Explain that the scenario will evolve in stages, and teams must respond after each update.

Step 4: Scenario Phase 1 – The First Warning Signs

Give each team the first incident card.

Example situation:

A participant in the youth group receives a direct message on Instagram from a travel page offering “special event transport deals” and asking for immediate payment through a suspicious link. At the same time, an email is received that looks like it comes from the event organisers and asks users to “reconfirm registration details” by logging in.

Each team must answer:

- What are the warning signs?
- Is this likely to be a scam? Why?
- What should the group do immediately?
- What should they avoid doing?

Allow 8–10 minutes for discussion, then invite quick presentations.

Scenario Phase 2 – Escalation

Give teams a second update card.

Example escalation:

One young person clicked the link and entered their full name, phone number, and email address. Another team member says they received a text message from their “bank” asking them to verify a transaction related to the fake payment.

Teams now discuss:

- What is the risk level now?
- What immediate steps should be taken?
- Who should be informed?
- What can still be done to reduce damage?

Expected ideas may include:

- stop all further interaction,
- warn the whole group,
- change passwords if needed,
- check bank/app activity only through official channels,
- report fake pages/accounts,
- collect evidence such as screenshots,
- inform organisers or responsible adults/youth workers,
- never continue through the same suspicious link or message.

Scenario Phase 3 – Pressure and Confusion

Introduce a third twist.

Example:

A message appears in the group chat saying:

“If you do not complete the payment in the next 15 minutes, your place in the event will be cancelled.”

At the same time, another participant insists the offer might be real because the fake page uses the event logo and photos.

Teams must now decide:

- How do scams use pressure and fake trust signals?
- How can the group verify information safely?
- How should they communicate with the wider group without creating panic?

After discussion, each team presents a short action plan.

Final Team Mission – Build the Response Plan

Ask each team to prepare a final response strategy on flipchart paper under 4 headings:

- What happened?
- What are the scam signs?
- What should we do now?
- How do we prevent this next time?

Teams present their plans. The facilitator compares the responses and reinforces good practices.

Step 5: Closing Reflection

Summarise the scenario and explain that online scams are often fast-moving, emotional, and designed to make people act before thinking. Highlight that good cybersecurity is not only technical, but also social: asking questions, verifying information, warning others, and staying calm.

DEBRIEFING QUESTIONS

- 1 At which moment in the scenario did the scam become most convincing?**
- 2 What manipulation tactics did the scammers use in the scenario?**
- 3 How did time pressure affect your team's decisions?**
- 4 What should a young person do if they already clicked a suspicious link or shared some information?**
- 5 What habits can help prevent online scams in everyday digital life?**

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Online scams often combine urgency, trust, and emotional pressure to make people act quickly.**
- ✓ Key message 2: A message that looks official is not automatically real—logos, names, and branding can be copied.**
- ✓ Key message 3: If a scam is suspected, stop, verify through official channels, and warn others before more damage happens.**
- ✓ Key message 4: Even if someone makes a mistake, quick action can still reduce harm and protect accounts, money, and personal data.**

PHISHING HUNTERS: SPOT THE SCAM!

LEARNING OBJECTIVES

Objective 1

To help young people understand what phishing is and how it appears in everyday digital life.

Objective 2

To develop participants' ability to identify warning signs in suspicious emails, messages, links, fake websites, and social media interactions.

Objective 3

To strengthen critical thinking, digital safety habits, and confidence in responding safely to online scam attempts.

TARGET GROUP

Audience

Young people aged 14–25, especially those who actively use email, social media, messaging apps, online shopping platforms, or digital services.

Prior Knowledge

No advanced cybersecurity knowledge is needed. Basic familiarity with using smartphones, apps, email, and social media is enough.

DURATION

Total Time

75 minutes (can be adapted between 60 and 90 minutes depending on the group size and discussion depth)

Breakdown

Introduction: 15 min | Main activity: 45 min | Debrief: 15 min

GROUP SIZE

Min / Max

10–30 participants (Recommended format: participants work in small teams of 3–5 people)

MATERIALS NEEDED

Physical

Printed phishing/non-phishing scenario cards
Score sheet for each team
Pens or markers
Flipchart or whiteboard
Sticky notes
Small reward items for the winning team (optional)

Digital	Laptop Projector or screen PowerPoint / Canva slides with quiz rounds Optional digital quiz tools such as Kahoot, Mentimeter, Quizizz, or Google Forms timer-based quiz
Preparation	The facilitator should prepare in advance: • 12–20 phishing-related quiz questions or scenario cards • A mix of examples: emails, SMS, fake login pages, giveaway scams, impersonation messages, fake delivery messages, fake bank alerts, social media scams • A simple scoring system • A final slide or handout with key phishing safety tips • Optional badges/team names to make the activity more playful

STEP-BY-STEP FACILITATION GUIDE

Step 1: Icebreaker – “Would You Click?”

Start with a quick energiser. Show 3–4 short examples on screen such as:

- “Your parcel is delayed, click here now”
- “You won a free iPhone!”
- “Your school account will be locked today”

Ask participants to move to one side of the room for “I would click” and the other side for “I would not click.”

After each one, invite 1–2 quick reactions. This creates curiosity and shows that phishing can sometimes look convincing.

Step 2: Mini-input – What Is Phishing?

Give a short interactive explanation of phishing. Avoid a lecture format and instead ask questions like:

- Where do fake messages usually come from?
- Why do scammers want people to click?
- What emotions do they try to trigger?

Briefly explain that phishing is a scam technique used to trick people into giving away passwords, money, personal data, or access to accounts. Mention common tactics such as urgency, fear, rewards, fake authority, and imitation of trusted brands or people.

Step 3: Team Formation and Game Setup

Divide participants into teams of 3–5. Each team chooses a team name such as:

- Scam Busters
- Link Detectives
- Cyber Guardians
- Anti-Phish Squad

Explain the rules:

- Teams earn points for correct answers
- Bonus points are given for explaining why something is suspicious
- Some rounds include traps, where fast answers may lose points if they are poorly justified
- The aim is not only to win but to learn how to stay safe online

Suggested scoring:

- Correct answer: 1 point
- Correct explanation: +1 bonus point
- Excellent safety recommendation: +1 bonus point

Step 4: Main Gamified Quiz – “Spot the Scam”

Run the main activity in 3 rounds.

Round 1: Real or Phish?

Show or distribute examples of emails, text messages, or social media DMs.

Teams must decide:

Safe / Suspicious / Definitely phishing

Examples:

- A fake bank email asking to “verify your identity urgently”
- A giveaway message asking for card details for shipping
- A fake Instagram DM from a “friend” asking for a code
- A delivery message with a strange shortened link

After each example, ask teams to explain which warning signs they noticed.

Round 2: Red Flag Challenge

Each team receives a printed scenario or projected screenshot and must identify as many warning signs as possible in 2 minutes.

Possible red flags:

- spelling mistakes
- strange sender address
- suspicious link
- urgency or threats
- asking for passwords
- offers that sound too good to be true
- poor branding or fake logos
- emotional manipulation

Teams present their answers. Award points based on how many relevant details they spotted.

Round 3: What Would You Do?

Give teams short real-life scenarios and ask them to choose the safest response.

Examples:

- You get a message from your “bank” asking you to log in immediately.
- A classmate sends you a link and says “vote for me now.”
- You receive a job offer via social media asking for personal data.
- Your account gets a fake “security alert.”

Teams discuss and present their action plan.

Good answers may include:

- do not click
- verify through the official website/app
- contact the person or company through trusted channels
- report/block the sender
- check the sender and URL carefully
- ask for support from a trusted adult, teacher, or youth worker if unsure

Step 5: Final Reflection and Safety Takeaways

Count the points and announce the winning team. Keep the tone fun and encouraging.

Then shift the focus from competition to learning. Ask each team to share:

- one thing they learned
- one sign of phishing they will now notice more easily
- one safety habit they want to adopt

The facilitator closes with a short summary of the most important anti-phishing habits.

DEBRIEFING QUESTIONS

- 1 What made some phishing examples look believable at first?
- 2 Which warning signs were easiest to identify, and which were harder?
- 3 Why do people sometimes fall for phishing, even when they know about online risks?
- 4 How do emotions like fear, excitement, urgency, or curiosity influence online decisions?
- 5 What practical steps can you take from now on to protect yourself and others from phishing?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Phishing often looks trustworthy because it copies real brands, people, or institutions.
- ✓ Key message 2: Urgency, fear, and “too good to be true” rewards are common manipulation tactics used by scammers.
- ✓ Key message 3: Before clicking, always check the sender, the link, and the request carefully.
- ✓ Key message 4: If something feels suspicious, stop, verify through official channels, and ask for help if needed.

THE EXPAT AGENCY – IDENTITY THEFT CHALLENGE

LEARNING OBJECTIVES

Objective 1	Develop the ability to identify "Social Engineering" red flags in anonymous social media posts.
Objective 2	Understand the lifecycle of Identity Theft, from a "simple chat" to total data loss.
Objective 3	Strengthen digital verification skills and reporting habits within the Lithuanian/European context.

TARGET GROUP

Audience	Young people (16–30), specifically those looking for internships or jobs abroad.
Prior Knowledge	Basic use of Facebook Groups and Messaging apps (WhatsApp/Telegram).

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min Main activity (Investigation): 50 min Debrief: 25 min

GROUP SIZE

Min / Max	10–24 (Divide into "Investigative Units" of 3–4 people)
-----------	---

MATERIALS NEEDED

Physical	Printed "Evidence Packets" (Screenshots of fake expat posts, anonymous DMs).
Digital	Smartphones/Laptops, access to Draugiškas Internetas or E-police.lt for the reporting phase.
Preparation	• Print 4 sets of "Evidence Packs." • Set up a "Fake Employer" profile example. • Prepare a "Data Loss Map" (showing how a phone number leads to identity theft).

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduce the concept of "Trust Harvesting."

Explain that in 2026, scammers don't use viruses; they use **conversations**.

Highlight the specific trend in Lithuania: Anonymous users targeting expats and students

Step 2: Hand out the "Evidence Packets."

Teams must analyze three different "Job Posts" found in a fictional expat group.

The Task: They must find 4 anomalies (e.g., account created yesterday, generic stock photo, "urgent" language, or asking for ID before an interview).

Step 3: Facilitator shows a "DM Chat" screenshot where the scammer asks for a phone number and home address.

Teams must predict what the scammer can do with just those three pieces of info (Phone, Address, Full Name).

Activity: Teams use a "Privacy Matrix" to see how this info is sold on the Dark Web or used for SIM-swapping.

Step 4: Participants must find the official Lithuanian reporting portal.

The **Task:** Draft a "Community Warning" post that is clear, non-aggressive, and informative to warn other expats in the group.

Step 5: Summarize that "Anonymous" doesn't just mean "hidden"—it means "unverified."

Reinforce the rule: **No interview, no ID.**

DEBRIEFING QUESTIONS

- 1 Why did the "Anonymous" post feel more helpful than a random email?
- 2 What was the most subtle red flag you found in the "Employer's" profile?
- 3 Why do scammers block victims immediately after getting their e-mail or phone number?
- 4 How can we help friends who are "desperate" for a job stay safe from these traps?
- 5 What is the first thing you should do if you accidentally sent a photo of your ID to a stranger?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Verification is a sign of intelligence, not a sign of rudeness
- ✓ Key message 2: Your PII (Personally Identifiable Information) is the currency of 2026.
- ✓ Key message 3: If an "employer" blocks you after getting your data, they didn't lose interest—they found what they were looking for.
- ✓ Key message 4: Use official channels (LinkedIn, University Portals) rather than anonymous social media groups for job hunting.

THE HR IMPOSTOR – RECRUITMENT FRAUD CHALLENGE

LEARNING OBJECTIVES

Objective 1	Identify the psychological triggers used in "Recruitment Fraud" (urgency, authority, and exclusivity).
Objective 2	Recognize the difference between a legitimate corporate onboarding process and a data-harvesting scam.
Objective 3	Build resilience against "onboarding fee" scams and social media impersonation.

TARGET GROUP

Audience	Young job seekers (18–30), university students, and first-time workers.
Prior Knowledge	Familiarity with Instagram and the general concept of applying for jobs online.

DURATION

Total Time	90 minutes
Breakdown	Introduction: 15 min The "Profile Audit" Activity: 30 min The "Interview" Roleplay: 25 min Debrief: 20 min

GROUP SIZE

Min / Max	12–24 (Teams of 3 or 4)
-----------	-------------------------

MATERIALS NEEDED

Physical	Printed "Candidate Packs" (a fake job offer letter, an "Onboarding Checklist," and a sample invoice for equipment).
Digital	Phones to check "official" company websites for comparison.
Preparation	Create a fake Instagram profile screenshot for a well-known company (e.g., "Microsoft_Careers_Official_2026").

STEP-BY-STEP FACILITATION GUIDE

Step 1: Introduction (15 min) - The Rise of the Fake HR:

Explain that scammers are now impersonating Human Resources (HR) from famous brands.

Discuss why young people are targeted: they are eager to start a career and may not know what a standard corporate process looks like.

Step 2: The Profile Audit (30 min):

Show the "Official" brand Instagram next to the "Recruitment" Instagram.

The Task: Teams must find 5 inconsistencies (e.g., the fake profile has no "Verified" badge, the bio link uses a URL shortener like bit.ly, or the engagement/follower ratio looks suspicious).

Step 3: The Onboarding Trap (25 min):

Hand out the "Onboarding Checklist" which asks for: Full Name, Address, Social Security Number, and a "Training Fee" of 50€.

The Activity: Teams must act as "Legal Auditors." They must mark every item on the list as "Standard" or "Warning."

The Reveal: Explain that no legitimate employer asks for money or highly sensitive data (like a passport photo) over a DM before a physical/official video interview.

Step 4: The Crisis Response (20 min):

Scenario: "You've already sent your ID photo to the fake HR person. What do you do now?"

Task: Teams must research and write down the three immediate steps for Lithuania/Spain/etc. (e.g., Contacting the bank, notifying the real company's HR, and filing a report on E-police.lt).

DEBRIEFING QUESTIONS

- 1 Why is it easier to believe a message from someone claiming to be from a "famous company"?
- 2 What is the main difference between an "Application" and an "Interview"?
- 3 Why do scammers ask for "Onboarding Fees" or "Equipment Deposits"?
- 4 How can you verify if an HR person reaching out to you on social media is real?
- 5 What was the most convincing part of the fake job offer you analyzed today?

KEY CYBERSECURITY MESSAGES

- ✓ Key message 1: Real employers pay you; you never pay them to start a job.
- ✓ Key message 2: Official recruitment usually happens via corporate email (@company.com), not Instagram DMs.
- ✓ Key message 3: High-pressure tactics ("Sign in 1 hour or lose the job!") are a massive red flag.
- ✓ Key message 4: If you can't find the job posting on the company's official "Careers" website, it probably doesn't exist.

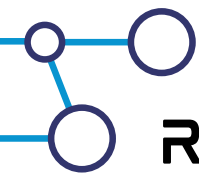


DEBRIEFING & REFLECTION

GROUP DISCUSSION TECHNIQUES

To keep cybersecurity discussions engaging and non-technical, use these active learning methods:

- **The "Scenario Carousel":** Place posters around the room, each detailing one of the regional threats identified (e.g., a "Student Rent" scam or an "Instagram Giveaway"). Small groups rotate to each station, spending 3 minutes discussing: "What is the red flag here?"
- **The "Spectrum of Risk":** Create an imaginary line in the room from "Totally Safe" to "Highly Dangerous." Read out online behaviors (e.g., "Scanning a QR code for a free pizza" or "Sharing a photo with a location tag"). Participants must move to the spot on the line that represents their opinion. This sparks immediate debate between those with different risk perceptions.
- **Fishbowl Discussion:** Four participants sit in a center circle (the fishbowl) and discuss a controversial topic—like whether social media platforms should be responsible for "Sextortion" prevention. The rest of the group observes. If someone from the outer circle wants to speak, they must "tap in" and swap seats.
- **The "Security Consultant" Roleplay:** Divide the group into "Scammers" and "Cyber-Consultants." Scammers try to design the most convincing fake message; Consultants must point out exactly how to spot the fraud.



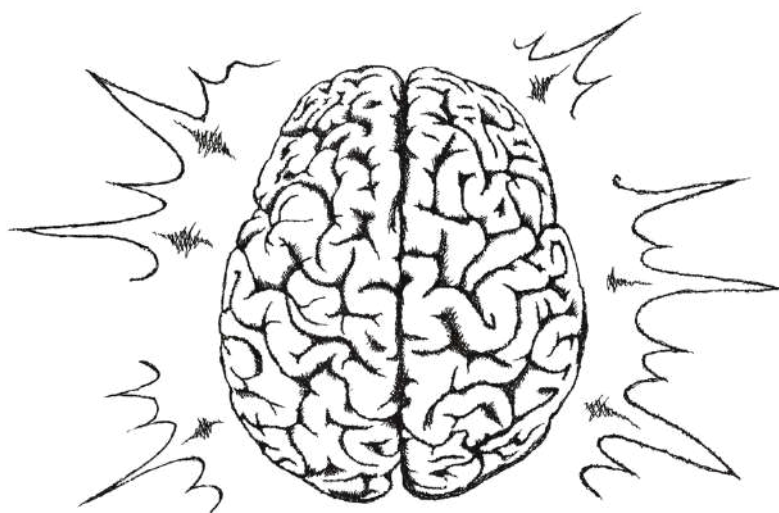
REFLECTION QUESTIONS

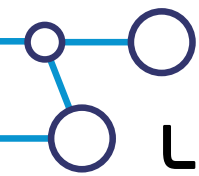
Debriefing and reflection are significant components of the learning cycle, as they allow participants to transition from simply experiencing a cyber threat to critically analysing the psychological and technical tactics used by scammers.

These questions are designed to bridge the gap between the toolkit's content and the participants' personal digital lives:



- **Personal Habits:** "Think about the last three apps you downloaded. Do you remember what permissions (camera, contacts, location) you gave them? Why did they need them?"
- **Emotional Triggers:** "Scammers often try to make you feel 'urgent' or 'scared' (like a fake account suspension). Can you think of a time a post or message made you feel like you had to act immediately? What happened?"
- **Digital Responsibility:** "If you saw a friend participating in a viral 'challenge' that looked risky or gathered too much personal data, would you say something? How would you approach that conversation?"
- **Future Resilience:** "After seeing the scams targeting your specific country (e.g., the fake internship offers), what is the one 'golden rule' you will now follow before clicking a link in an email?"





LEARNING EVALUATION

To ensure a holistic assessment of the learning journey, facilitators should integrate reflection directly into the evaluation process, as this allows for the measurement of both technical knowledge gained and the shift in personal digital attitudes.

The "Traffic Light" Check: At the end of a session, participants hold up a card:

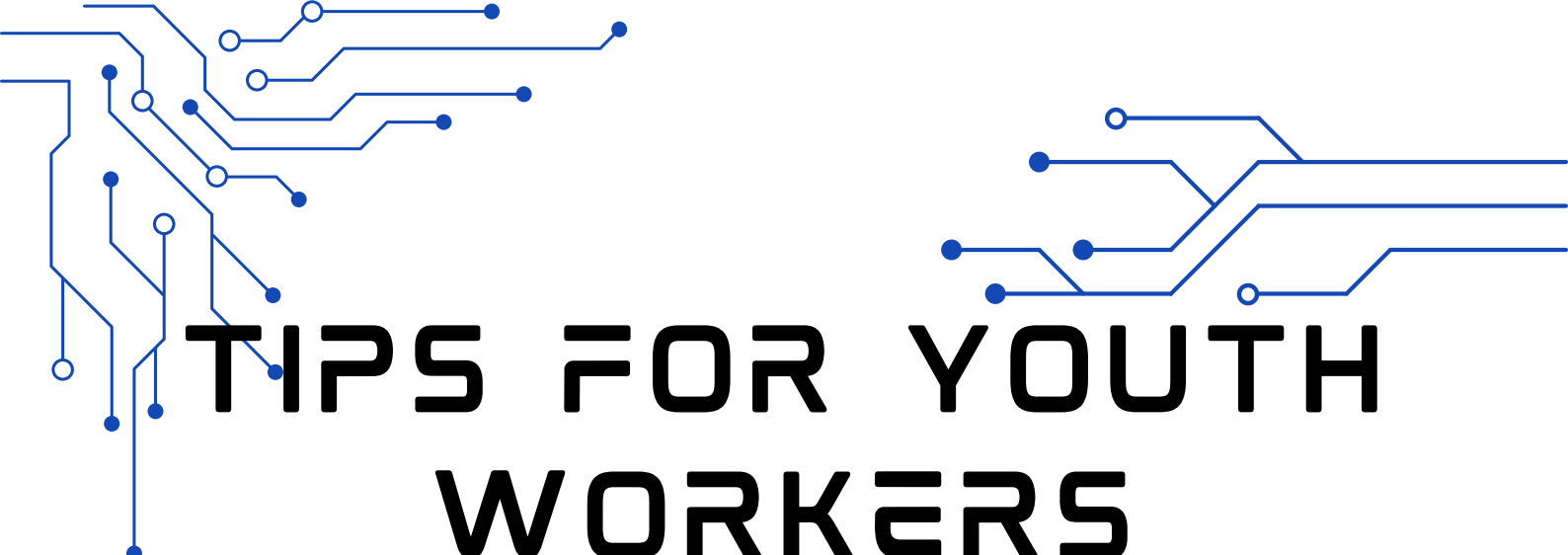
- **Green:** I feel confident identifying this risk.
- **Yellow:** I understand it, but I'm still a bit unsure how to protect myself.
- **Red:** I still find this topic too technical or confusing.

The 60-Second Pitch: Challenge participants to explain one cybersecurity concept (like "2FA" or "QR Phishing") to a younger sibling or a grandparent in under one minute. If they can simplify it, they have mastered it.

"Spot the Scam" Quiz: Show 5 real-life examples of messages (some real, some fake). A successful evaluation is when the group can identify at least 4 out of 5 and—more importantly—explain why they made that choice.

Digital Confidence Scale: Ask participants to rate their confidence in "Digital Resilience" from 1–10 before the workshop and after the workshop. The growth in that number is your key evaluation metric.





TIPS FOR YOUTH WORKERS

INTEGRATING CYBERSECURITY IN YOUTH WORK

Cybersecurity should be integrated into youth work as a natural extension of young people's daily digital experiences rather than treated as a separate or highly technical topic. Young people are constantly engaging with social media, messaging platforms, and online content, making decisions that relate to privacy, trust, and safety, often without being fully aware of the risks involved.

For youth workers, the key is to connect cybersecurity topics such as data privacy, phishing, misinformation, online scams, fake profiles, and password security to real-life situations that young people already encounter. By starting from familiar experiences, cybersecurity becomes more relevant and easier to understand. This approach allows discussions to emerge organically within broader themes such as digital wellbeing, participation, and critical thinking.

Non-formal education methods play a central role in this process. Interactive formats such as problem-solving challenges, simulations, role-play, or gamified quizzes enable young people to explore cybersecurity in a practical and engaging way. These approaches create a safe environment where participants can experience scenarios like phishing attempts or social media manipulation, test their reactions, and learn through experience.

It is important to focus on empowerment rather than fear. While raising awareness of risks is necessary, the objective is to help young people feel confident in their ability to recognise threats and make informed decisions. By embedding cybersecurity into regular youth work activities, it becomes part of an ongoing learning process that supports the development of responsible and resilient digital behaviour.

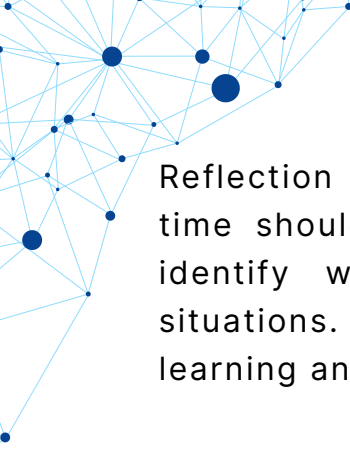
RUNNING WORKSHOPS OR YOUTH LABS

Workshops and youth labs are effective formats for delivering cybersecurity education because they encourage active participation and experiential learning. A well-designed session should guide participants through a clear process that moves from engagement to reflection.

An effective starting point is to introduce the topic through a relatable situation, such as a suspicious message, a fake online profile, or misleading content. This immediately connects the session to participants' everyday experiences and increases their engagement.

The core of the workshop should focus on interactive activities drawn from the formats included in this toolkit. Different topics can be explored through different methods. For example, phishing and online scams can be addressed through simulations or cyber attack scenarios, while misinformation and social media manipulation can be explored through case study scenarios or gamified quizzes. Role-play activities are particularly useful for understanding fake profiles or scam interactions, while mini-escape rooms allow participants to apply multiple concepts in a dynamic and immersive way.

These methods encourage young people to actively participate, make decisions, and collaborate with others. Learning becomes more effective because participants are directly involved in the process rather than passively receiving information. The role of the youth worker is to facilitate this process by guiding the activity, supporting participants when needed, and encouraging exploration without immediately providing answers.



Reflection is a crucial part of the learning process. After each activity, time should be allocated for participants to discuss their decisions, identify warning signs, and connect the experience to real-life situations. This step helps transform the activity into meaningful learning and supports behavioural change.

Creating a safe and inclusive environment is also essential. Participants should feel comfortable expressing their ideas and sharing experiences, particularly when discussing sensitive topics such as online risks or negative digital experiences. A respectful atmosphere encourages open dialogue and deeper engagement.

FACILITATING DISCUSSIONS ABOUT ONLINE SAFETY

Discussions play a key role in reinforcing learning and helping young people reflect on their digital behaviour. Effective discussions should be based on participants' experiences and linked to the activities carried out during the session. Youth workers should create a non-judgmental space where participants feel safe to share their perspectives. Young people may have different levels of awareness or may have made risky decisions online, so it is important to encourage openness rather than criticism. Listening actively and validating contributions helps build trust and supports meaningful dialogue.

Facilitators should guide discussions by asking open-ended questions that encourage reflection and critical thinking. Questions such as how to recognise trustworthy information, why people fall for scams, or how personal data can be misused help participants analyse situations and consider different perspectives. This approach supports the development of critical thinking skills, which are essential for navigating digital environments. Discussions should also help participants connect specific topics, such as phishing or fake profiles, to broader concepts like trust, identity, and responsibility online. This allows young people to better understand the impact of their actions and the importance of safe digital behaviour.

At the same time, it is important to ensure that discussions lead to practical outcomes. Participants should leave with clear ideas about how to protect themselves, such as recognising suspicious links, using secure passwords, or verifying information sources. Summarising key points at the end of the session helps reinforce learning and provides clarity.

By combining interactive activities with guided discussions, youth workers can create engaging and meaningful learning experiences. This approach supports young people in becoming more aware, confident, and responsible in their use of digital technologies.





RESOURCES & TOOLS

RECOMMENDED CYBERSECURITY PLATFORMS

EU

enisa.europa.eu

- [Cyber Education Platform](#)
- [Awareness Raising in a Box](#)
- [Awareness & Cyber Hygiene](#)
- [SMEs Cybersecurity](#)
- [European & International Cybersecurity Challenge](#)
- [CIRAS Platform](#)

digital-strategy.ec.europa.eu

- [Better Internet for Kids Strategy](#)

betterinternetforkids.eu

cert.europa.eu — CERT-EU

Estonia

itvaatlik.ee — IT Watchdog.

ria.ee — Information System Authority.

- [CERT-EE Cyber Incident Handling](#).

Lithuania

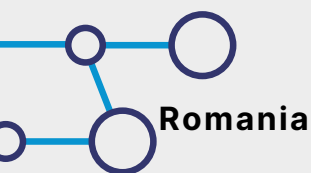
nksc.lt — National Cyber Security Centre

draugiskasinternetas.lt

Portugal

internetsegura.pt

seguranet.pt



Romania

sigurantaonline.ro

dnsc.ro — [Directoratul Național de Securitate Cibernetică](https://dnsc.ro)

Spain

is4k.es

hacksplaining.com

phishingquiz.withgoogle.com

Türkiye

usom.gov.tr — [USOM \(National CERT\)](https://usom.gov.tr)

bilgem.tubitak.gov.tr

- [Cyber Security Division](https://bilgem.tubitak.gov.tr)

EDUCATIONAL RESOURCES

EU

education.ec.europa.eu

- [Digital Education Focus](https://education.ec.europa.eu)

enisa.europa.eu

- [CyberHEAD Tool](https://enisa.europa.eu)
- [Cybereducation Platform](https://enisa.europa.eu)
- [European Cybersecurity Skills Framework](https://enisa.europa.eu)

digital-skills-jobs.europa.eu

- [Cybersecurity Skills Academy](https://digital-skills-jobs.europa.eu)

academy.europa.eu

- [Build Your Own Cyber Awareness Program](https://academy.europa.eu)

edpb.europa.eu — [European Data Protection Board](https://edpb.europa.eu)

childnet.com

thinkuknow.co.uk

better-internet-for-kids.europa.eu

- [Resource Directory](https://better-internet-for-kids.europa.eu)



europol.europa.eu

- [Cybercrime area](#)

arqus-alliance.eu

- [Cybersecurity MOOC – Citizen & Professional Guide](#)

esdc.europa.eu — European Security & Defence College

digital-strategy.ec.europa.eu

- [Communication: Cybersecurity Skills Academy](#)

Estonia

ria.ee — Information System Authority

- [CERT-EE – Handling Cyber Incidents](#)
- [National Coordination Centre \(NCC-EE\)](#)

Lithuania

better-internet-for-kids.europa.eu

- [Safer Internet Day – Lithuania](#)

cyberwiser.eu

- [Lithuania page](#)

Portugal

internetsegura.pt

- [Resources](#)

seguranet.pt

- [Training / Formação](#)

Romania

sigurantaonline.ro

- [The Websters S3 – Întâmplări din Viața Digitală \(PDF\)](#)
- [The Websters S4 – Întâmplări din Viața Digitală \(PDF, 2025\)](#)

dnsc.ro — Directoratul Național de Securitate Cibernetică

- [Ghid Securitate Cibernetică 2021](#)
- [Ghid Control Parental – Protecția Minorilor în Mediul Digital](#)

Spain

incibe.es — National Cybersecurity Institute

Türkiye

btkakademi.gov.tr — BTK Academy

USEFUL WEBSITES

EU

enisa.europa.eu — ENISA

saferinternet.org

euvsdisinfo.eu

ecs-org.eu — European Cyber Security Organisation

digital-strategy.ec.europa.eu

- [NIS2 Directive](#)
- [Related content – topic 153](#)
- [Related content – topic 49](#)
- [Related content – topic 99](#)

eucpn.org — EU Crime Prevention Network

- [EU Kids Online – Final Report](#)

safety.google

Estonia

ria.ee — Information System Authority

- [National Cyber Security Centre \(NCSC-EE\)](#)
- [Reporting a Cyber Incident](#)

raport.cert.ee — CERT-EE Annual Report

Lithuania

vaikulinija.lt — Child Line

epolicija.lt — E-Police

Portugal

cncs.gov.pt — National Cybersecurity Centre

- [Cybersecurity \(EN\)](#)

Romania

salvaticopiii.ro — Salvați Copiii

- [Siguranța pe Internet](#)

cybersecurity.certsign.ro

- [Cyber4Kids](#)

unbreakable.ro — Competiție națională de cybersecurity

cyberskill.ro

Spain

incibe.es — National Cybersecurity Institute

osi.es — Internet Security Office

Türkiye

guvenlinet.org.tr — Safe Internet

kvkk.gov.tr — Personal Data Protection Authority

REFERENCES

Chapter 1

Eurostat (2024). Young people – digital world statistics
<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250715-1>

European Commission (2021). Digital Education Action Plan (2021–2027)
<https://education.ec.europa.eu/focus-topics/digital-education/actions>

European Commission. Erasmus+ Programme
https://commission.europa.eu/education/set-projects-education-and-training/erasmus-funding-programme_en

ENISA (2023). Cybersecurity education and awareness resources
<https://www.enisa.europa.eu/tools/enisa-cybereducation-platform>

Chapter 3

Cedefop (2024) - Terminology of European education and training policy

<https://www.cedefop.europa.eu/en/publications/3095>

David Kolb (1984): “Experiential learning: experience as the source of learning and development”

https://www.fullerton.edu/cice/_resources/pdfs/sl_documents/Experiential%20Learning%20-%20Experience%20As%20The%20Source%20Of%20Learning%20and%20Development.pdf

European Commission (2020) – European Skills Agenda

https://employment-social-affairs.ec.europa.eu/policies-and-activities/skills-and-qualifications/european-skills-agenda_en

Garamkhand Surendeleg et al., “The Role of Gamification in Education – A Literature Review”, Contemporary Engineering Sciences, Vol. 7

<https://www.m-hikari.com/ces/ces2014/ces29-32-2014/02surendelegCES29-32-2014.pdf>

SALTO – Youth, “Non -formal methods. Guide to empower youth.” (2023)

https://www.salto-youth.net/downloads/toolbox_tool_download-file-3759/Guide-of-Non-formal%20methods.pdf

Scientific research, Hamari, J., Koivisto, J., & Sarsa, H. (2014). "Does Gamification Work? A Literature Review of Empirical Studies on Gamification." 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 6-9 January 2014, 3025-3034.

<https://www.scirp.org/reference/referencespapers?referenceid=2757206>

UNESCO Digital Library, Youth and skills: putting education to work, EFA global monitoring report, 2012

<https://unesdoc.unesco.org/ark:/48223/pf0000218003>

University of Cambridge, Libraries and Archives, Apollo, Johnson, M., & Majewska, D. (2022). "Formal, non-formal, and informal learning: What are they, and how can we research them?" Cambridge University Press & Assessment.

<https://www.repository.cam.ac.uk/items/b4200743-6f60-4d46-a668-c382f5400041>