



EM&M

EMotional intelligence & cybersecurity
environMents in youth education



MANUAL FOR YOUTH WORKERS AND STAKEHOLDERS

Project Reference Number: 2024-2-RO01-KA220-YOU-000293190



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 National Agency for Community Programmes in the Field of Education and Vocational Training (ANPCDEFP). Neither the European Union nor the ANPCDEFP can be held responsible for them.



Contents

Contents	2
Open Licence.....	8
Introduction	9
Module 1 - Fundamentals of Cybersecurity and Emotional Intelligence in Youth Education.....	10
Module Overview	10
Module Content.....	10
Why Fundamentals Matter	10
Core Cybersecurity Concepts in Youth-friendly Language	10
Emotional Intelligence and Online Behaviour	11
Typical Youth Threat Patterns and Persuasion Tactics	12
Inclusive Facilitation and Safeguarding Posture.....	14
Teaching Routines That Transfer	15
Light Assessment of Understanding.....	16
Expanded Glossary	16
Module 2 - Training Framework.....	18
Module Overview	18
Learning Objectives	20
Module Content.....	20
Introduction to the Training Framework	20
A Framework Built on Real Needs	21
Why Emotional Intelligence Matters in Cybersecurity	21
What the EM&M Training Framework Provides	22
Connection to Module 3	23
Foundations of the EM&M Training Framework	23
Foundation 1: Infrastructure & Access.....	23
Foundation 2: Pedagogical Innovation.....	24
Foundation 3: Emotional & Social Support	24
How the Three Foundations Work Together	25
Key Takeaways for Youth Workers (Quick Summary)	26
Key Elements of the EM&M Training Framework	26
Element 1: Blended Learning Approaches.....	26

Element 2: Emotional Intelligence Embedded in Cybersecurity.....	27
Element 3: Addressing Barriers and Challenges	27
Element 4: Preventive Cybersecurity Focus.....	28
Quick Summary: What These Four Elements Achieve Together	29
Linking Emotional Intelligence, Blended Learning & the Main Online Threats	30
The Core Framework Map.....	30
Practical Guidelines for Youth Workers	32
Guideline 1: Assess Youth Needs Before You Begin	32
Guideline 2: Build an Emotionally Safe Learning Environment	32
Guideline 3: Integrate EI Moments into Every Cybersecurity Activity	33
Guideline 4: Use Blended Learning to Keep Youth Engaged	33
Guideline 5: Use Realistic Scenarios Based on Youth Experience.....	34
Guideline 6: Choose Tools That Support Inclusion	34
Guideline 7: Encourage Peer Support and Youth Leadership.....	35
Guideline 8: Evaluate, Reflect, and Adapt Continuously	35
Quick-Use Summary for Youth Workers	35
Applying the EM&M Training Framework in Youth Work Practice	36
What You Can Now Do as a Youth Worker	36
Before You Implement: A Youth Worker Readiness Checklist.....	36
How to Start Implementing the Framework Step-by-Step.....	37
Preparing Youth Workers for Module 3.....	38
Final Encouragement for Youth Workers.....	39
Module 3 - Inclusive Blended Teaching & Learning Methods	40
Module Overview	40
What Is Blended Learning in This Context?	40
Purpose of Module 3	40
Conceptual Framework	41
Blended Pedagogy for Online Safety	41
Emotional Intelligence (EI) and Online Risks	42
Universal Design for Learning (UDL) for Digital Safety	42
Inclusion and Digital Equity in Online Safety Education	42
Pedagogical Model	43

Connect: Building Trust and Emotional Safety.....	44
Explore: Introducing Concepts with Curiosity and Critical Thinking.....	45
Practice: Applying Skills in Safe, Supported Ways.....	45
Reflect: Deepening Understanding Through Self-Awareness	46
Share: Amplifying Learning Through Community	47
The Cyclical Nature of the Model	47
Practical Tips for Youth Workers.....	48
Implementation Guidelines	48
Introduction	48
Design for Inclusion and Accessibility	48
Create Emotionally Safe Spaces.....	49
Integrate Micro-Learning for Online Risks	49
Choose Accessible and Ethical Digital Tools	50
Facilitate Hybrid Engagement.....	51
Ethical and Data Protection Considerations.....	51
Evaluation and Reflection.....	52
Knowledge and Skills Assessment.....	52
Behavioural Change Observation	52
Engagement Analytics.....	53
Reflection Logs and Journals	53
Inclusion Audit	54
Key Takeaways	54
Module 4 - Online Vulnerability Assessment and Threat Recognition Exercises	56
Module Overview	56
Learning Objectives	56
Module Content.....	57
Understanding Online Vulnerability	57
Threat Recognition: From Awareness to Action	59
Vulnerability Assessment Tools	62
Gamification and Scenario-Based Learning	63
Blended Delivery Guidelines.....	65
Module 5 - My Role as Youth Ambassador for Security Culture.....	68

Module Overview	68
Learning Objectives	69
Module Content.....	69
Understanding Security Culture	69
The Role of the Youth Worker as Ambassador	70
Supporting Young People Through Emotional and Digital Challenges	73
Emotional Intelligence in Digital Mediation	74
Practical Skills for Becoming an Ambassador	75
Module 6 - Repository of Further Information and Resources.....	76
Activities	85
Activities Module 1	85
Activity 1	85
Activity 2	87
Activity 3	90
Activity 4	93
Activities Module 2	97
Activity 1: Cyber Emotions Map.....	97
Activity 2: Digital Escape Room – Cyber Threat Edition	97
Activity 3: EI & Cybersecurity Role-Play.....	97
Activity 4: Cyber Hygiene Checklist Challenge	97
Activity 5: Stress Under the Screen – Coping Workshop.....	97
Activity 6: Cyber Ambassador Peer Circle	98
Activity 7: Storytelling with Emotions & Security	98
Activity 8: Quickfire Quiz & Reflection	98
Activities Module 3	98
Activity 1: Digital Empathy Mirror	98
Activity 2: Cyber Scenario Lab	100
Activity 3: Inclusive Session Designer.....	101
Activity 4: Gamify Emotions Online	103
Activity 5: Reflective E-Journal	104
Activities Module 4	106
Activity 1: Spot the Risk – Interactive Quiz	106
Activity 2: Behind the Click – Emotion Triggers	108

Activity 3: Cyber Detective – Case Files.....	111
Activity 4: My Digital Mirror – Self-Assessment.....	115
Activity 5: Cyber Diary – One Day Online.....	117
Activity 6: Vulnerability Map – Workshop	120
Activities Module 5	124
Practical activities to perform with youth.....	125
Activity 1: The Digital Trust Tree.....	125
Activity 2: Emotion Filter.....	126
Activity 3: Ambassador Map	127
Activity 4: #MindfulMedia Campaign	128
Activity 5: Pause-Reflect-Respond.....	129
Activity 6: Youth–Adult Dialogue Lab.....	130
Activity 7: “Digital Bridge – Talking Across Generations”	131
References	133
Module 1	133
Module 2.....	133
Module 3.....	134
Module 4.....	135
Annexes	136
Annexes Module 1	136
Annex A – Concept Map Worksheet	136
Annex B – Case Vignette Sheet	136
Annex C – EI Micro-skills One-Pager.....	137
Annex D – Think-Aloud Script Template.....	138
Annex E – Misconception Cards	139
Annexes Module 2	140
Annex 1: Cyber Hygiene Checklist	140
Annex 2: Emotional Intelligence Coping Techniques Guide.....	140
Annex 3: Role-Play Scenario Cards	140
Annex 4: Peer Circle Guide	141
Annexes Module 3	142
Annex A: Inclusive Session Plan Template.....	142
Annex B: UDL & Accessibility Checklist	143

Annex C: Reflection Journal Prompts	143
Annex D: Evaluation & Inclusion Grid	144
Annex E: Youth Profile Samples	145
Annex F: Peer-Mentor / Youth Ambassador Guide	146
Annexes Module 4	147
Annex 1: Handout_M4	147
Annex 2: Threat Recognition Scenario Cards	148
Annex 3: Cyber Detective Case Files	150

Open Licence

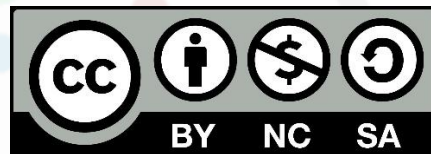
© 2026 EM&M Project Consortium

This publication was developed within the framework of the EM&M – Emotional Intelligence & Cybersecurity Environments in Youth Education Project.

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).

You are free to share and adapt the material provided that appropriate credit is given, the material is not used for commercial purposes, and any adaptations are distributed under the same license.

More information about the license is available at:
<https://creativecommons.org/licenses/by-nc-sa/4.0/>





Introduction

The EM&M Manual – Emotional Intelligence and Cybersecurity Environments in Youth Education was developed as part of the Erasmus+ EM&M (Emotional Intelligence and Cybersecurity Environments in Youth Education) project. The project responds to the growing challenges faced by young people and the professionals who work with them in an increasingly digitalized world. In this world, technological advances bring significant opportunities and risks related to online safety, emotional well-being, and responsible digital behavior.

Technology has completely changed the way we communicate, learn, and interact socially. Digital tools are great for innovation and connectivity, but they also expose young people to online threats, misinformation, and emotional stress. Research and practical experience show that there is an urgent need to pay more attention to young people's emotional intelligence and cybersecurity. This will enable them to make informed, conscious, and strong decisions on social media.

The EM&M project responds to this need with a comprehensive educational approach that integrates emotional skills development with cybersecurity education. The project aims to show how digital technologies affect emotional and social behavior. At the same time, it aims to give youth workers and educators practical tools to avoid online risks such as phishing, data misuse, online harassment, and digital addiction.

This manual has been designed as a practical resource for people working with young people, such as youth workers, educators, trainers, and stakeholders. It provides clear instructions, ways of doing things, activities, and learning resources that support education that is not formal or informal. The content shows that the project is dedicated to inclusion, digital skills and new ideas in youth work. This matches the Erasmus+ goals of being digitally ready, including everyone and providing good education for young people.

Together with the EM&M storytelling tools and the microlearning environment, this manual helps to create a sustainable learning ecosystem that empowers youth professionals to encourage safe, emotionally aware, and responsible digital participation. EM&M helps young people to understand digital spaces better. It does this by improving their technical awareness and emotional skills. This helps them to navigate digital spaces with confidence, empathy and critical thinking skills.



Module 1 - Fundamentals of Cybersecurity and Emotional Intelligence in Youth Education

Module Overview

This module prepares youth educators to introduce the core concepts of cybersecurity and emotional intelligence in a way that is engaging, age-appropriate, and relevant to young people's daily digital lives. It explains how behaviours in the cyber world affect wellbeing and risk, why emotional states influence online decision-making, and how educators can foster proactive, resilient responses to digital threats. The emphasis is on conceptual clarity, a shared vocabulary, and educator readiness to guide reflective discussion before moving to hands-on practice in later modules. Simple discussion-based activities and lightweight handouts support blended delivery and low-bandwidth contexts.

By establishing strong fundamentals, youth gain a common language to talk about online safety issues – from phishing and fake friend requests to cyberbullying, online predators, and accidentally downloading malware – and understand how their feelings (like curiosity or fear of missing out) can make them more or less vulnerable. Educators will be equipped to explain core ideas clearly, invite reflection, and scaffold simple routines that learners can actually use in daily life.

Module Content

Why Fundamentals Matter

Young people live in always-on digital environments where online habits shape identity, relationships, and opportunities. Fundamental literacy in cybersecurity and emotional intelligence gives youth a shared language for understanding risks and a practical path toward safer, calmer choices online. Without these basics, a teen might not recognise a risky situation – whether it's a cyber predator's friendly overture or a scam giveaway – or they might react impulsively in ways that put them at risk (for example, sharing a private photo when pressured, or clicking a suspicious link out of fear). This module equips educators to explain core ideas clearly, invite personal reflection, and scaffold simple routines that learners can use in daily life. Shared vocabulary and concepts reduce confusion and improve help-seeking: when everyone understands terms like phishing, privacy, or self-awareness, it's easier for youth to ask for help or apply strategies in the moment.

Core Cybersecurity Concepts in Youth-friendly Language

Introduce key cybersecurity terms using clear, youth-friendly definitions and examples from everyday life:

- **Asset** – something that matters to you online (e.g. your identity, photos, personal data, access to accounts). An asset is what you want to protect.
- **Threat** – something that could cause harm to your assets. For example, threats include phishing messages, cyberbullying, malware infections, or online predators trying to exploit personal information.
- **Vulnerability** – a weakness that a threat can exploit. For example, using a weak password, oversharing private information, rushing to respond, or trusting too easily are vulnerabilities. They create openings that threats (like hackers or impersonators) can take advantage of.
- **Risk** – the chance that a threat uses a vulnerability to cause harm. Risk goes up when threats and vulnerabilities align (for instance, a phishing threat + the vulnerability of curiosity = high risk of clicking). Risk decreases when you change behaviour or strengthen protection (for example, enabling 2FA or pausing to think reduces the risk of account takeover).
- **Hygiene** – small daily habits that add up to safety. These are routine protective behaviours such as installing updates, using two-factor authentication (2FA), checking privacy settings, or pausing to verify messages before acting. Just like personal hygiene keeps you healthy, digital hygiene keeps your online life secure.

Keep these definitions simple and relatable. Use concrete examples from the learners' world to illustrate each concept. For instance, talk about account takeovers on social apps, scam prize offers, fake friend requests or impersonations, cyber predators attempting to chat, viral rumours or fake news, and pressure to share content or passwords. Show how each example involves assets, threats, vulnerabilities, and risk:

Example: A message on Instagram claims you won a new phone if you click a link. Asset at stake: your account access and data. Threat: a phishing scam. Vulnerability: excitement and fear of missing out (FOMO) might make you click without checking. Risk: high, if you're not cautious. Hygiene: the safer habit is to never click random prize links – instead, verify on an official site.

Emotional Intelligence and Online Behaviour

Emotional Intelligence can be taught as four practical skills that greatly influence online behaviour and safety:

- **Self-awareness** – noticing what you feel before you act. For example, recognising “I am feeling angry at this comment” or “I feel excited about this message” is the first step.



- **Self-management** – using short techniques to regulate stress and impulse. This could mean taking a deep breath, counting to 10, or using a 4-4-6 breathing cycle (inhale 4 seconds, hold 4, exhale 6) to steady yourself when a triggering message pops up.
- **Social awareness** – understanding others' perspectives and online dynamics. This includes empathy (recognising when a friend might be feeling upset or when a message is intended to make you panic) and spotting social cues (like knowing a message demanding “don't tell anyone” is suspicious).
- **Relationship skills** – communicating clearly and assertively, seeking help when needed, and setting boundaries online. For example, being able to politely say “No, I can't share that information” or to reach out to a trusted adult if you suspect someone is a fake friend or predator.

Teach learners that emotions influence online choices and risk perception. Being excited, angry, or scared can cloud judgment. Introduce a simple, repeatable EI cycle for safer digital action: Awareness → Reflection → Regulation → Response. In practice, this means:

- **Awareness:** Pause and notice your emotional state (e.g., “I feel anxious about this urgent email”).
- **Reflection:** Think about why you feel that way and what the situation is (e.g., “This message is trying to scare me. Is it real?”).
- **Regulation:** Take action to calm down (e.g., a breathing exercise or counting to 5).
- **Response:** Choose a safe, reasoned response (e.g., do not click the link; verify through an official app or ask someone for advice).

Teach this cycle as a repeatable routine. Learners can recall these steps under pressure. Emphasise that feelings are normal signals – feeling anxious or curious online isn't “bad,” it's human. The key is to notice those feelings and use them as a cue to slow down and think rather than immediately react.

Typical Youth Threat Patterns and Persuasion Tactics

Many online threats that target youth rely more on emotional persuasion than technical hacking. Help learners recognise common patterns where emotions are used as triggers:

- **Urgency and Fear:** Messages that say, “Act now or else...” (e.g., “Your account will be suspended in 30 minutes if you don't confirm now!”). The trigger is panic or fear of loss. Scammers and cyberbullies alike use urgency to make you react without thinking.

- **Authority:** Someone pretends to be a figure of authority (tech support, a teacher, a famous influencer) to pressure you (e.g., “This is IT support, you must send your password to fix an issue”). The emotion triggered is often anxiety or obedience to authority.
- **Empathy and Reciprocity:** A plea that tugs at your heartstrings (e.g., “Please help me, I’m stuck and I need you to send me your account code quickly!”). This triggers compassion, guilt, or the urge to help a friend – which could be abused by scammers or even cyber predators forging friendships.
- **Curiosity and Social Status:** Teasers that play on FOMO or insecurity (e.g., “Look what they posted about you! Everyone is talking about it – click here to see”). The trigger is curiosity or fear of missing out on something socially important. Similarly, a sensational piece of fake news or gossip might provoke strong curiosity or outrage, prompting impulsive sharing.
- **Reward (Too Good to Be True):** “Congratulations, you won a prize!” or “Get free followers by clicking here now”. This triggers excitement, greed, or FOMO for a reward. Scammers often use limited time offers or exclusive rewards to cloud judgment.
- **Social Proof or Peer Pressure:** (Related to FOMO) Suggestions that “everyone is doing this” or a challenge that “all your friends have tried.” This triggers the fear of missing out or the desire to conform, which can lead to risky behaviour like participating in viral challenges or clicking unverified links.

For each trigger, discuss the emotional hook and pair it with a calm response strategy. For example:

- **Urgency trigger → Calm response:** Recognise the rush, take a breath, and verify through another channel. (“I’ll log in through the official app instead of clicking this link.”)
- **Empathy trigger → Calm response:** Slow down and verify the story. (“I want to help, but I’ll call my friend directly to see if this is true.”)
- **Curiosity trigger → Calm response:** Acknowledge the temptation, then pause and check. (“This might be a trick. I’ll ask another friend if they heard about this instead of clicking.”)

By naming the trigger emotion (e.g., “This message is trying to scare me” or “This is making me really curious”) and having a pre-planned action, youth can disrupt the manipulation. Highlight that many online threats – from phishing scams to clickbait to cyberbullying taunts – rely on getting an emotional reaction rather than outsmarting you technically. Recognising those tactics is



like seeing the strings of a puppet: once you see the trick, it's easier to not get pulled along.

Inclusive Facilitation and Safeguarding Posture

When teaching these fundamentals, it's important to create an inclusive, supportive learning environment:

- **Use simple language:** Avoid jargon unless you immediately explain it. For example, don't assume everyone knows "phishing" – define it in plain words ("a fake message that tricks you into giving info") and perhaps relate it to something they've seen.
- **Normalise emotions as signals, not problems:** Make it clear that feeling scared by a warning or excited by a reward is natural. There's no shame in having a reaction; the goal is to notice it and handle it. This reduces stigma and encourages honest discussion. For instance, share that even adults feel "panic" when they get an official-sounding threat email – it's how we manage that panic that matters.
- **Anonymous participation for sensitive issues:** Provide channels for learners to contribute anonymously (like a suggestion box or online poll) when discussing sensitive experiences. Youth may be more willing to admit "I once shared my password with a fake friend" or "I posted something I regret" if they can do so privately. An anonymous prompt can surface common issues like posting private information you later regret or encountering predatory behaviour, without putting any one student on the spot.
- **Set ground rules:** At the start, establish a safe space. Suggested ground rules: confidentiality (what's shared in class stays in class), no shaming or mocking anyone's experiences, and an opt-out option for anyone who feels uncomfortable. This is crucial if discussions might bring up personal incidents of cyberbullying, harassment, or contact with strangers.
- **Be ready to safeguard:** Know your escalation pathway if a learner discloses serious harm (like they are being groomed by an online predator or severely bullied). Have resources or contacts for professional help. Youth should know you take such issues seriously and will help them get appropriate support. Part of cybersecurity fundamentals in youth education is ensuring they have trusted adults and resources to turn to when things go wrong.



Teaching Routines That Transfer

Focus on a small set of easy-to-remember routines or micro-skills that learners can practice in class and use in real life. It's better to have a few strong habits than a long list of tips they'll forget. Some foundational routines include:

- **"Stop – Breathe – Check" pause routine:** When something urgent or emotional happens online, literally stop (hands off keyboard/phone for 3 seconds), take one deep breath (or a 4-4-6 cycle), then check in with yourself and the situation. Ask: "What am I feeling? What is this message really asking me to do? Is this a threat to any of my assets? How can I verify it safely?" This 10–20 second routine can prevent countless mistakes (like clicking a bad link or sending a rash reply).
- **4-4-6 Breathing for stress relief:** Teach the simple breathing pattern: inhale for 4 seconds, hold for 4, exhale for 6 (focusing on a longer exhale). Doing this a couple of times can physiologically reduce the heart rate and calm the nervous system. It helps especially when a message triggers fear or anger, allowing clearer thinking before responding.
- **Peer double-check:** Encourage a habit of consulting a friend or trusted person before acting on something suspicious or emotionally charged. For example, "If you get a weird DM or a request that feels off, take a screenshot and send it to a friend: 'Does this look fishy to you?'" Often an outside perspective can catch a red flag you missed. This also reinforces a culture of looking out for each other online.
- **Two-step verify (don't trust links):** Instil a rule of never acting directly on a link or instruction that came from an unsolicited message. Instead, do a two-step verification: go to the official app or website yourself, or contact the person through a different channel. For example, if an email says, "Your bank account is locked, click here," you do not click – you open your banking app separately or call the bank. Or if a friend's account asks for a code, you call that friend on the phone to confirm. This habit defeats most phishing and impersonation scams, including fake prize offers and "friend in need" scams.

Use brief modelling and practice for each routine. For instance, demonstrate "Stop-Breathe-Check" with a sample message on screen, narrating your thoughts. Then have the group do a quick practice round with a different example. Provide a cue or mnemonic that will help them remember it later – maybe a visual icon or a catchphrase. The goal is to hardwire these responses so that in a real moment of stress (like receiving a scary predator message or a bullying comment), the youth defaults to the safer routine automatically.



Light Assessment of Understanding

After teaching the fundamentals, use quick, low-pressure assessments to gauge understanding and correct misconceptions:

Exit prompts: At the end of a session, ask each learner to write one sentence about what changed in their understanding today. For example, “I used to think rushing was okay, but now I see it as a vulnerability,” or “I learned what phishing means.” This helps reinforce a key takeaway and lets you see what stuck.

Think-alouds: Have a few learners volunteer to narrate how they would handle a message or situation. For instance, present a hypothetical message (“Your friend sends a link saying you’ve been posted on a cringe account”) and have the learner talk through their reaction: “I’d feel embarrassed and curious... but I would stop and breathe, remember not to click links, maybe go check the account directly or ask my friend if they really sent this.” Listening to these think-alouds shows whether they can apply concepts like threats, triggers, and routines in context. It also builds confidence in using the new vocabulary.

Glossary checks: Give learners key terms from the module (threat, vulnerability, risk, etc.) and ask them to define in their own words or give an example. You could make it a quick game (e.g., glossary bingo or matching terms to definitions). Ensure they understand each term well enough to explain it to a peer. For example, a learner might say, “A vulnerability is like a weakness – for me, oversharing is a vulnerability because I tend to post without thinking and that could be risky.”

Scenario questions: Pose a very short scenario and ask a couple of multiple-choice or yes/no questions to check understanding. For example: “If you get a DM from a stranger offering a prize if you sign up on a website, what is the threat here? What vulnerability might it exploit? What’s a safe response?” This can be done through a quick show of hands or an online poll.

The aim of assessment here isn’t to “grade” anyone, but to ensure clarity. It also helps surface any misconceptions early so you can address them (e.g., if someone still believes “if it’s from a friend it must be safe,” you can correct that). Keep the tone positive and encouraging – praise correct concepts and gently correct mistakes with clear, youth-friendly explanations.

Expanded Glossary

- **Asset:** What you value and want to protect online (accounts, data, reputation).
- **Threat:** Anything that could harm those assets (phishing scam, hacker, bully, predator, malware).



- **Vulnerability:** A weakness or gap that makes a threat more likely to succeed (weak password, quick trust, strong emotions like panic, oversharing personal info).
- **Risk:** The likelihood of a threat exploiting a vulnerability to cause harm (this can be high or low, and we take steps to reduce it).
- **Hygiene:** Daily safe habits that protect you (updates, 2FA, verifying links, thinking before posting).
- **Self-awareness:** Knowing your feelings in the moment (especially when online).
- **Self-management:** Strategies to handle your emotions and impulses (breathing exercises, pausing).
- **Social awareness:** Understanding others' emotions and intentions online (empathy, reading context, recognising manipulation).
- **Relationship skills:** Healthy ways to interact online (assertive communication, boundary setting, seeking help).
- **Persuasion trigger:** An element in a message that tries to provoke an emotion (urgency, fear, curiosity, etc.) and influence your behaviour.
- **Verification step:** An action to check if something is legitimate before you respond (like contacting a friend through a separate app or looking up the official source).

By having students internalise these terms, you empower them to discuss and tackle cyber challenges more clearly. For example, a student might later say, “I noticed the message was using urgency as a trigger, so that was a red flag – my self-awareness kicked in and I did a verification step by calling the company’s hotline.” That level of articulation is a sign of true learning and sets the stage for the more hands-on practice in later modules.

M

Module 2 - Training Framework

Module Overview

This module equips youth workers and educators with a structured and practical training framework that integrates Emotional Intelligence (EI) and Cybersecurity awareness into youth education. Building on findings from the EM&M Comparative Study and aligned with the project's blended learning methodology, Module 2 defines *what* content should be taught to young people to strengthen their emotional resilience, digital literacy, and preventive online behaviours.

The module highlights how EI skills—such as self-regulation, emotional awareness, stress management, empathy, and critical reflection—directly influence young people's vulnerability to online risks. It provides guidance to youth workers on embedding these EI skills within cybersecurity education while addressing the most common threats affecting young people today, including:

- Cyber predators and online grooming
- Fake friend requests and impersonation attempts
- Posting private information or content that may later be regretted
- Phishing tactics
- Scams involving prizes, rewards, or fear-of-missing-out (FOMO) triggers
- Cyberbullying and hostile digital communication
- Misinformation and missing or manipulated information
- Accidental malware downloads.

Grounded in evidence gathered across six partner countries, the module emphasises blended learning as the most inclusive and effective approach for youth education. It supports educators in adapting the EM&M framework to diverse local realities (urban/rural, socio-economic, cultural), balancing in-person activities with online and self-paced digital tools such as Teams, Moodle, Zoom, YouTube, Canva, and Kahoot.

Ultimately, this module provides the conceptual and structural foundation for Module 3, which expands the framework into concrete inclusive blended learning methods. Together, Modules 2 and 3 create a coherent pathway from *what* youth workers must teach to *how* they can implement this content effectively and emotionally safely.

EM&M Training Framework

Integrating Emotional Intelligence, Cybersecurity & Blended Learning

From evidence → to practice → to youth resilience



Why this framework? To help youth workers build emotionally resilient, digitally safe young people through blended learning.

Infrastructure & Access



- Devices & Connectivity
- Low-Bandwidth Options

Pedagogical Innovation



- Gamification
- Micro-learning
- Interactive Methods

Emotional & Social Support



- EI & Peer Support
- Safe Spaces

Core Framework Elements

Blended Learning

- Face-to-Face . Online . Self-Paced
- Low-Bandwidth Options

Emotional Intelligence

- Self-Awareness Regulation
- Empathy

Barrier Reduction

- Connectivity Motivation
- Workload

Preventive Cybersecurity

- Avoid Risks Before Harm

EI Cyber-Threats: Spot & Respond

Cyber Threat	Emotional Trigger	Core EI Skill	EI in Action	Safer Digital Action
Phishing	Urgency, Fear	Stress Management	Pause & Regulate Before React	Verify Sender & Link Before Clicking
Fake Profiles	Curiosity, Trust	Self-Awareness	Question Intent & Set Boundaries	Confirm Identity Before Accepting
Cyberbullying	Anger, Shame	Emotional Regulation & Empathy	Calm Down & Choose Constructive Response	Block, Report or Seek Support
Misinformation	Fear, Outrage	Critical Thinking	Emotionally Distance & Analyze	Verify Sources Before Sharing

Dual-Pathway Blended Learning



EI is not an add-on. It is a cybersecurity skill.

Learning Objectives

By the end of this module, youth workers and educators will be able to:

- Understand and apply the EM&M Training Framework in their work with young people.
- Integrate EI skills (stress management, empathy, adaptability, emotional awareness) into cybersecurity training.
- Teach preventive strategies related to the major online threats identified in the project (cyber predators, impersonation, phishing, scams, cyberbullying, misinformation, risky downloads, and oversharing).
- Adapt the framework to local contexts while ensuring inclusivity and accessibility for diverse youth groups.
- Utilise blended learning approaches that combine face-to-face facilitation, synchronous and asynchronous online interaction, and mobile-first options.
- Address engagement barriers such as motivation fatigue, connectivity challenges, and digital inequalities.
- Foster resilience and critical awareness in youth through EI-grounded and gamified learning strategies.

Module Content

Introduction to the Training Framework

Why a Training Framework for EI & Cybersecurity?

Young people today live in a digital world where emotions and technology are constantly intersected. Their online choices are often influenced by:

- peer pressure,
- impulsive reactions,
- stress or fear,
- desire for connection,
- seeking approval or validation.

These emotional dynamics can increase vulnerability to online threats such as:

- cyber predators
- impersonation
- phishing
- scams
- cyberbullying
- misinformation
- malware
- oversharing



Youth workers therefore need a clear, practical structure that helps them teach both digital safety and emotional intelligence (EI) as interconnected skills.

This is exactly what the EM&M Training Framework provides.

A Framework Built on Real Needs

The EM&M Comparative Study—conducted in six countries with 329 participants—revealed that:

Youth often struggle with:

- identifying cyber risks,
- regulating emotions during online conflicts,
- resisting manipulation (e.g., scams, fake profiles, FOMO triggers),
- evaluating information critically.

Youth workers need:

- easy-to-apply teaching structures,
- blended learning tools suitable for diverse contexts,
- methods that connect emotions with online decision-making,
- inclusive approaches for different backgrounds and digital access levels.

The framework responds by offering:

- a structured roadmap,
- adaptable learning objectives,
- preventive, emotionally grounded approaches,
- blended learning guidance,
- ready-to-use tools and activities.

Why Emotional Intelligence Matters in Cybersecurity

Online threats are rarely “just technical.” They succeed because they trigger emotions.

Online Threat	Emotional Trigger	Result
Phishing	urgency, panic	quick, risky click
Scams	excitement, reward-seeking, FOMO	irrational choices
Cyber predators	trust, loneliness	vulnerability
Cyberbullying	anger, shame	impulsive reactions

Online Threat	Emotional Trigger	Result
Fake news	fear, confusion	spread of misinformation

EI helps youth slow down, think clearly, and make safer choices.

- With strong EI skills, youth can:
- recognise emotional manipulation
- regulate stress and impulsiveness
- communicate assertively
- set boundaries
- ask for help when needed
- apply critical thinking before acting

Thus, EI becomes a digital safety tool, not just a personal development skill.

What the EM&M Training Framework Provides

The framework gives youth workers a practical, step-by-step guide for integrating EI and cybersecurity in any youth setting. It supports:

Diverse youth groups

- urban/rural
- low/high digital access
- socio-economic diversity
- culturally varied contexts
- different learning needs

Flexible blended learning

- face-to-face sessions
- synchronous online workshops
- asynchronous microlearning
- mobile-friendly tools (YouTube, Canva, Padlet, Kahoot)

Preventive empowerment

Instead of reacting to problems after they occur, the framework helps youth:

- anticipate risks,
- manage emotional triggers,
- recognise manipulation,
- develop safe habits,
- build resilience.

Connection to Module 3

To make the manual cohesive:

- Module 2 = WHAT youth workers teach: EI + cybersecurity + preventive framework + learning objectives.
- Module 3 = HOW youth workers teach it: concrete blended learning models, tools, methods, scenarios, and inclusive practices.

Together, they form a complete training pathway: from understanding → to designing → to implementing high-quality youth work sessions.

Key Takeaways for Youth Workers

- The digital world is emotional; online safety requires EI.
- Youth need preventive, emotionally grounded cybersecurity skills.
- This framework gives you a clear, accessible structure to guide your practice.
- Blended learning increases engagement and flexibility.
- Module 3 will help you turn this framework into real sessions and activities.

Foundations of the EM&M Training Framework

The EM&M Training Framework is built on three core foundations that shape how youth workers can effectively integrate Emotional Intelligence (EI) and Cybersecurity awareness into youth learning environments. These foundations ensure that the learning experience is inclusive, practical, adaptable, and emotionally supportive, regardless of context.

Foundation 1: Infrastructure & Access

Ensuring fairness, accessibility, and equal opportunity for all youth.

Before youth workers can deliver cybersecurity or EI-related content, they must address the real-world learning conditions young people face. The Comparative Study highlighted disparities in:

- Internet access (particularly in rural or low-income areas)
- Device availability (shared phones, outdated devices)
- Digital tools and platforms used across countries and organisations

Why it matters

Young people who lack stable connectivity or proper devices often disengage, fall behind, or avoid participation altogether. This directly impacts learning outcomes related to cybersecurity awareness and emotional resilience.

What youth workers should do

- Provide low-bandwidth alternatives (offline worksheets, printed materials).
- Choose mobile-first tools, since much of the youth rely on smartphones.
- Ensure all activities have a backup format (e.g., a discussion-based version for online tasks).
- Prioritise platforms familiar to youth:
- Zoom • Teams • Moodle (for structured learning)
- YouTube • Canva • TikTok-style micro videos • Padlet • Kahoot (for engagement)

Goal: No young person is excluded from learning due to technical barriers.

Foundation 2: Pedagogical Innovation

Keeping youth engaged, motivated, and active participants.

Youth workers repeatedly reported that motivation fatigue, screen exhaustion, and boring or repetitive formats reduce learning effectiveness—especially online. They also noted that youth prefer:

- Short, dynamic learning moments
- Visual content
- Hands-on problem solving
- Gamified experiences
- Opportunities for creativity

Why it matters

Cybersecurity training often becomes overly technical or abstract. Without innovation, youth disengage quickly leaving them more vulnerable to online risks.

What youth workers should integrate

- Gamification (quizzes, challenges, escape rooms, badges)
- Microlearning videos (3–7 minutes)
- Scenario-based exercises (phishing challenges, fake profile role-play)
- Interactive polls & live reactions
- Drama, improv, or storytelling techniques for emotionally charged topics
- Reflective moments connecting emotions to behaviour

Goal: Make learning meaningful, relevant, and emotionally engaging.

Foundation 3: Emotional & Social Support

Building emotional resilience as a core cybersecurity skill.

This foundation reflects the key EM&M insight: Emotions strongly influence online decisions.

Youth often fall for scams, click unsafe links, overshare information, or engage in cyberbullying due to emotional triggers like:

- anxiety
- excitement
- frustration
- loneliness
- curiosity
- desire to fit in.

The framework emphasises that EI is not optional—it's essential for safe online behaviour.

Why it matters

When youth understand and regulate their emotions, they:

- pause before clicking,
- identify manipulation faster,
- respond thoughtfully to cyberbullying,
- verify information more critically,
- avoid impulsive sharing,
- communicate more respectfully online.

What youth workers should embed

- Emotional check-ins at the start of sessions
- Stress-management exercises before cybersecurity challenges
- Discussing emotional triggers (fear, FOMO, shame, excitement)
- EI reflection questions ("How did you feel when...?")
- Peer support circles to foster safe communication
- Empathy training for conflict resolution and cyberbullying scenarios

Goal: Empower youth to stay calm, reflective, and safe in digital spaces.

How the Three Foundations Work Together

These foundations support youth workers in delivering cybersecurity training that is:

Foundation	What it contributes	Why it matters
Infrastructure Access	& Equal opportunity to participate	No youth left behind
Pedagogical Innovation	Engaging, motivating activities	Youth stay connected and learn deeply

Foundation	What it contributes	Why it matters
Emotional & Social Support	Resilience, empathy, safe decision-making	Reduces vulnerability to online threats

When combined, they create a holistic, inclusive, and transformative learning environment.

Key Takeaways for Youth Workers (Quick Summary)

- Before teaching cybersecurity content, ensure accessible learning conditions.
- Use innovative and youth-friendly methods to sustain engagement.
- Make EI a core part of every cybersecurity lesson, not an add-on.
- Focus on real-world emotional triggers underlying risky online behaviours.
- Remember: The foundation you create shapes how effectively youth will learn, apply, and retain cybersecurity skills.

Key Elements of the EM&M Training Framework

Element 1: Blended Learning Approaches

A flexible mix of in-person, online, and self-paced learning.

Blended learning is not simply adding online elements to traditional workshops—it's about designing intentional, interconnected learning experiences that match how youth prefer to engage.

What the Comparative Study revealed

- Youth workers prefer structured sessions (face-to-face or synchronous online).
- Young people prefer asynchronous, flexible, mobile-first activities.
- Engagement increases when sessions mix short explanations, hands-on tasks, and interactive digital elements.

The Framework recommends:

- Combine workshop-style sessions with digital tools (e.g., Kahoot, Canva, Padlet).
- Use microlearning (short videos, challenges, mini-quizzes) for key cybersecurity concepts.
- Provide both formal learning paths (Teams/Moodle/Zoom) and creative platforms (YouTube, Discord, Canva).
- Build "hybrid pathways" that let youth work online when motivated, offline when connectivity is limited.



Purpose: To create learning that is dynamic, accessible, and culturally adaptable, regardless of local context.

Element 2: Emotional Intelligence Embedded in Cybersecurity

EI skills as the backbone of online safety.

EI is at the heart of every aspect of the EM&M framework. Youth are more likely to fall for cyber threats when experiencing:

- stress,
- urgency,
- loneliness,
- anger,
- curiosity,
- desire for social approval.

This makes emotion management just as important as recognizing technical risks.

Key EI components integrated in cybersecurity lessons:

- Self-awareness → noticing emotional triggers before reacting
- Self-regulation → pausing before clicking, sharing, replying
- Empathy & social understanding → responding constructively to cyberbullying
- Adaptability → staying calm during digital disruptions or conflicts
- Communication skills → assertive boundary-setting with strangers or suspicious contacts

Practical examples:

- Teaching phishing recognition alongside stress-management breathing.
- Discussing cyberbullying with empathy and emotional reflection activities.
- Exploring scams by focusing on excitement, reward-seeking, and FOMO triggers.

Purpose: To help youth make safer and more emotionally grounded decisions online.

Element 3: Addressing Barriers and Challenges

Removing obstacles that prevent youth from fully participating.

Youth workers repeatedly face challenges that weaken engagement and learning effectiveness. The framework directly supports educators in overcoming these barriers.

Common challenges identified:

- poor internet connectivity
- lack of devices or shared devices
- low digital confidence
- motivation fatigue (especially online)
- screen overload
- limited time or resources for preparation

The Framework provides solutions:

- Low-bandwidth versions of every activity
- Offline alternatives for digital sessions
- Microlearning modules that reduce fatigue
- Gamified tasks for motivation
- Peer-led mentoring to strengthen involvement
- Accessible design minimizing cognitive overload

Practical strategies for youth workers:

- Use printable worksheets for phishing or scam identification.
- Offer flexible participation windows for asynchronous tasks.
- Simplify digital tools and avoid platform overload.
- Integrate movement or reflection breaks in long sessions.

Purpose: To make cybersecurity and EI education accessible, feasible, and effective for all youth, regardless of constraints.

Element 4: Preventive Cybersecurity Focus

Teaching youth to avoid risks—not just react to them.

Young people often encounter online risks before they have the training or emotional maturity to handle them. That is why the EM&M framework prioritizes prevention, not reaction.

Core preventive skills emphasized:

- recognizing phishing & scam patterns
- verifying identities online
- using secure privacy settings
- checking sources to fight misinformation
- pausing before posting or sharing
- avoiding risky downloads
- reporting cyberbullying and predatory behaviour
- maintaining cyber hygiene habits

Prevention + EI = powerful protection

Example 1:

A phishing message creates urgency → EI “pause & breathe” → critical evaluation → safe decision.

Example 2:

Cyberbullying triggers hurt → EI self-regulation → assertive communication → supportive peer response.

Tools used in the framework include:

- scenarios
- simulations
- gamified escape rooms
- role-play cards
- emotional mapping
- reflective journaling
- peer ambassador programs.

Purpose: To equip youth with daily habits and emotional strength that reduce their exposure to cyber threats.

Quick Summary: What These Four Elements Achieve Together

Element	What it gives youth workers	Benefit for youth
Blended Learning	Flexible teaching options	Engaging, accessible learning
EI Integration	Emotional stability & safer decision-making	Stronger resilience online
Overcoming Barriers	Practical tools for diverse groups	Inclusive participation
Preventive Cybersecurity	Proactive risk avoidance	Reduced vulnerability

Together, these elements transform cybersecurity training from a technical subject into a holistic youth empowerment process.

Linking Emotional Intelligence, Blended Learning & the Main Online Threats
Cybersecurity risks are not only technical—they are emotional and behavioural. Young people often fall for online threats not because they lack knowledge, but because emotions override rational decision-making. Blended learning offers flexible ways to teach EI and cybersecurity together, helping youth practice safer digital habits through realistic, engaging, and emotionally grounded activities.

This chapter provides a clear, practical mapping between:

- EI skills youth need,
- common threats they face, and
- blended learning approaches youth workers can use.

Why EI Is a Cybersecurity Skill

Online threats succeed because they exploit emotions such as fear, curiosity, excitement, loneliness, or belonging. When youth strengthen EI skills, they become less vulnerable to manipulation and more capable of making safe choices.

Key EI competencies relevant for cybersecurity:

- Self-awareness: noticing emotional reactions
- Self-regulation: pausing before acting
- Stress management: staying grounded under pressure
- Empathy: responding constructively to others
- Critical reflection: questioning information & intentions

Blended learning brings these skills to life through interactive workshops, digital simulations, mobile-friendly activities, and reflective online spaces.

The Core Framework Map

A visual overview of how EI + Blended Learning address each threat

Cyber Threat	Emotion That Increases Vulnerability	EI Skill Needed	Blended Learning Examples
Cyber Predators	loneliness, desire for validation	Boundary-setting, self-awareness	Role-play (offline), identity verification micro-video, anonymous Q&A online

Cyber Threat	Emotion That Increases Vulnerability	EI Skill Needed	Blended Learning Examples
Fake Friend Requests / Impersonation	curiosity, social pressure	Pause–reflect–decide, critical thinking	“Spot the fake profile” digital challenge, breakout discussions
Oversharing / Regretful Posts	impulsivity, excitement, need for approval	Impulse control, emotional awareness	Think-before-you-post reflection activity, social media audit
Phishing	urgency, confusion, fear	Stress management, slow thinking	Phishing simulation game, microlearning quiz
Scams / FOMO Traps	excitement, reward-seeking, fear of missing out	Emotional regulation, skepticism	Online escape room, decision-tree challenge
Cyberbullying	anger, shame, frustration	Communication, empathy, self-regulation	Drama reenactments, digital chat reconstruction, private journaling
Misinformation / Fake News	fear, outrage, emotional resonance	Critical thinking, emotional distancing	Fact-checking races, online polls, compare headlines activity
Malware Downloads	curiosity, impatience	Caution, evaluating consequences	Safe-vs-risky download quiz, mobile-friendly risk checklist

Key Takeaways for Youth Workers

- Each cyber threat is tied to specific emotional triggers.
- EI skills make youth less vulnerable and more aware.

- Blended learning allows you to teach interactively, regardless of technology conditions.
- You don't need to be a cybersecurity expert – you only need to connect emotions, behaviour, and examples.

Practical Guidelines for Youth Workers

This chapter offers clear, actionable guidance on how youth workers can integrate Emotional Intelligence (EI) and Cybersecurity into their daily practice using the EM&M Training Framework. The guidelines help educators create safe, inclusive, motivating, and blended learning environments that strengthen young people's digital resilience.

Guideline 1: Assess Youth Needs Before You Begin

Start where the young people actually are – not where you assume they are.

What to assess:

- Digital access: Devices? Internet? Shared accounts?
- Digital literacy level: Confident or unsure?
- Emotional needs: Stress, low confidence, conflict, isolation?
- Past online experiences: Cyberbullying, scams, privacy breaches.
- Learning preferences: Visual? Hands-on? Gamified? Discussion-based?

Tools you can use:

- Short anonymous questionnaires (online or paper)
- Ice-breaker discussions: "My biggest online fear is..."
- Quick polls (Mentimeter, Zoom reactions, WhatsApp)

Purpose: To tailor the training to real needs and avoid either overwhelming or boring participants.

Guideline 2: Build an Emotionally Safe Learning Environment

Young people learn better when they feel respected, supported, and heard.

Create emotional safety through:

- Opening check-ins: "How are you feeling today?"
- Group agreements: Respect, confidentiality, no judgment.
- Opt-out options: Allow stepping out during sensitive topics.
- Anonymous contribution tools: Padlet, Mentimeter, Slido.
- Support signals: Colour cards or emojis to express comfort levels.

Example:

"If at any moment the discussion feels uncomfortable, you can let me know or take a break. Your emotional wellbeing is important."



Purpose: To connect EI to cybersecurity in a respectful, trauma-informed way.

Guideline 3: Integrate EI Moments into Every Cybersecurity Activity

Even a 2-minute reflection strengthens emotional resilience. Easy EI integration techniques:

- Pause & Breathe: Before answering messages or clicking links.
- Emotion labelling: “What am I feeling right now?”
- Trigger mapping: Identify what emotions lead to risky decisions.
- Perspective-taking: “How would someone else feel in this situation?”
- Reappraisal: Reframing negative thoughts in stressful digital events.

Sample EI prompts:

- “How did this message make you feel?”
- “What emotion might lead someone to fall for this scam?”
- “What would calmness help you notice here?”

Purpose: To make EI skills automatic in everyday online behaviour.

Guideline 4: Use Blended Learning to Keep Youth Engaged

Mix formats to maintain energy and attention.

Balance your methods:

Face-to-face:

- role-plays
- discussions
- emotional mapping
- cyber hygiene workshops

Online/Synchronous:

- phishing simulation
- digital escape rooms
- collaborative boards (Padlet, Miro)

Asynchronous:

- microlearning videos
- short quizzes
- reflective journals
- Canva storytelling assignments

Pro Tip: Always provide a mobile-friendly version—many youth primarily use smartphones.



Purpose: To sustain motivation and make concepts accessible through multiple learning channels.

Guideline 5: Use Realistic Scenarios Based on Youth Experience

Authenticity increases impact.

Create relatable scenarios involving:

- fake followers
- FOMO campaign scams
- friend-of-a-friend profiles
- cyberbullying in group chats
- emotionally triggering posts
- misinformation shared in class groups
- free streaming/download “offers”

Use the 3-Step Scenario Method:

1. Present a short situation (text, video, screenshot).
2. Identify emotions, risks, intentions, consequences.
3. Discuss safer alternatives using EI tools.

Purpose: To connect theory to the real digital world of youth.

Guideline 6: Choose Tools That Support Inclusion

The tools should adapt to youth—not the other way around.

Select tools based on:

- accessibility (captions, text-to-speech, easy navigation)
- low bandwidth
- intuitive design
- safety and privacy features

Recommended tools:

- For reflection: Padlet, Google Forms, Mentimeter
- For gamification: Kahoot, Quizizz, Genially
- For creativity: Canva, Storyboarder
- For collaboration: Miro, Jamboard, Teams Channels

Avoid:

- too many platforms at once
- tools requiring accounts youth don’t want to create
- content-heavy videos longer than 7 minutes

Purpose: To reduce barriers and support diverse learning needs.



Guideline 7: Encourage Peer Support and Youth Leadership

Young people learn best from each other.

Implement peer-based approaches:

- Cyber Ambassador roles
- Peer mentoring circles
- Group projects on misinformation, scams, privacy audits
- Collaborative fact-checking challenges

Benefits:

- normalizes help-seeking behaviour
- increases motivation
- strengthens engagement
- empowers youth to develop leadership roles

Purpose: To make cybersecurity a shared responsibility, not an individual task.

Guideline 8: Evaluate, Reflect, and Adapt Continuously

Improvement is part of the process.

Evaluate through:

- pre/post questionnaires
- quick emoji check-ins (“How confident do you feel now?”)
- weekly reflection journal prompts
- observation of group interactions
- feedback on activities and tools

Ask youth:

- “What made learning easier today?”
- “What activity helped you understand your emotions online?”
- “Which online risks are still unclear?”

Adjust based on:

- youth motivation levels
- connectivity challenges
- emotional responses to certain topics
- cultural or linguistic nuances

Purpose: To keep the learning environment responsive, safe, and effective.

Quick-Use Summary for Youth Workers

Assess youth needs

Build emotional safety



Insert EI moments into every activity

Use multiple learning formats

Teach through real scenarios

Choose inclusive tools

Encourage peer learning

Evaluate & adapt continuously

Applying the EM&M Training Framework in Youth Work Practice

Module 2 has provided youth workers with a comprehensive framework linking Emotional Intelligence (EI), Cybersecurity awareness, and blended learning strategies. This chapter brings everything together and offers practical guidance on how to apply the framework effectively in real youth work settings, ensuring a smooth transition into Module 3.

What You Can Now Do as a Youth Worker

By completing this module, youth workers are now able to:

- Understand how EI shapes online decisions: youth can better recognize phishing attempts, scams, cyberbullying, and misinformation when they first understand their emotional triggers.
- Teach cybersecurity through relatable, emotionally grounded scenarios: the framework provides ways to embed storytelling, role-play, case studies, and youth-led reflection.
- Use blended learning to keep young people engaged: switching between offline discussions, online challenges, microlearning videos, and mobile activities keeps sessions dynamic and accessible.
- Address the full spectrum of common cyber threats: Including: cyber predators, fake friend requests, oversharing, phishing, scams, cyberbullying, misinformation, and malware.
- Create inclusive and emotionally safe environments: this supports respectful dialogue, helps young people share difficult experiences, and models the emotional skills needed for safe digital behaviour.

Before You Implement: A Youth Worker Readiness Checklist

A practical checklist to ensure your session is well-prepared and aligned with the EM&M Framework.

A. Emotional Preparedness

- I have planned an emotional check-in or grounding activity.
- I am prepared to discuss sensitive topics safely and respectfully.



- I can identify when a young person is stressed, overwhelmed, or triggered.

B. Content Preparedness

- I have selected 1–3 key cyber threats to focus on.
- I have built in EI moments (pause, reflect, label emotions, reframe).
- I have checked that my examples are local, relevant, and age appropriate.

C. Technical Preparedness

- I have both online and offline versions of the activity.
- I know which devices the youth will use (phone, tablet, PC).
- I have chosen tools that are accessible, safe, and easy to navigate.

D. Inclusion & Accessibility

- I checked that all materials are understandable for different literacy levels.
- I have gender-neutral and culturally sensitive examples.
- I have considered participants with low digital confidence.

E. Evaluation & Feedback

- I prepared a quick assessment (quiz, poll, reflection question).
- I will collect feedback at the end of the session.
- I have a plan for adjusting the next session based on youth responses.

How to Start Implementing the Framework Step-by-Step

A simple and flexible pathway for youth workers.

Step 1: Pick One Cybersecurity Theme

Examples: phishing, cyberbullying, impersonation, misinformation.

- Start small. Don't try to teach everything at once.

Step 2: Add an EI Skill That Matches the Threat

Examples:

- Phishing - stress management + critical thinking
- Scams - impulse control + scepticism
- Cyberbullying - empathy + emotional regulation
- Fake profiles - self-awareness + boundary-setting

Step 3: Choose a Blended Method

Pick at least one online and one offline method:

- Online: quiz, escape room, micro-video, group chat reflection
- Offline: scenario cards, emotion mapping, role-play

This makes your session interactive and inclusive.

Step 4: Create an EI Reflection Moment

Even a 1-2 minute reflection strengthens emotional resilience:

Examples:

- “How would this situation make you feel?”
- “What emotion might cloud your judgment?”
- “What would you tell a friend experiencing this?”

Step 5: End with a Practical Habit

Examples:

- “Pause before reacting”
- “Verify before trusting”
- “Think before you post”
- “Check the source”
- “Ask for help when something feels wrong”

This transforms knowledge into daily digital hygiene habits.

Preparing Youth Workers for Module 3

Module 3 will take everything learned in Module 2 and turn it into ready-to-use teaching practices.

Module 2 = *WHAT to teach*

- The EI–Cybersecurity connection
- The eight major online threats
- Framework pillars and elements
- How blended learning supports engagement
- Practical guidelines for implementation

Module 3 = *HOW to teach it*

It will include:

- Inclusive blended learning models
- Detailed session templates
- Activity scripts (step-by-step)
- Toolkits for online/offline delivery



- Universal Design for Learning (UDL) strategies
- Accessibility and cultural adaptation guidance

Module 3 is the hands-on manual that operationalises everything you have learned here.

Final Encouragement for Youth Workers

Working with young people in digital environments can be challenging, but the EM&M Framework is designed to support you, not overwhelm you.

Remember:

- You do NOT need to be a cybersecurity expert.
- You only need to connect emotions with online behaviour.
- Consistency is more important than complexity.
- Every small skill you teach reduces young people's vulnerability.
- Your role is essential — youth trust you more than any online tool or platform.

By applying the EM&M framework, you are helping young people become:

- safer,
- more resilient,
- emotionally aware,
- critical thinkers,
- and responsible digital citizens.

You are shaping a generation that can navigate the digital world with confidence, empathy, and intelligence.

Module 3 - Inclusive Blended Teaching & Learning Methods

Module Overview

In an era where youth digital engagement, emotional wellbeing, and online safety increasingly converge, youth workers and trainers face an urgent need to adopt pedagogical approaches that weave together emotional intelligence (EI), cybersecurity awareness, and digital literacy. This module responds to that need by offering a theoretically informed and practice-oriented framework for blended learning, specifically tailored to youth work contexts.

Here, the focus is on eight critical online risk areas:

1. Cyber predators
2. Fake friend requests and impersonations
3. Posting private information and regretful posts
4. Phishing
5. Scams (prize/reward/FOMO-based)
6. Cyberbullying
7. Missing information and fake news
8. Accidental malware downloads

The module demonstrates how to use inclusive, accessible, and emotionally intelligent blended learning to help young people from diverse economic, cultural, socio-digital, and ability-based backgrounds develop emotional resilience, digital literacy, and safer online behaviours. By integrating EI-grounded techniques (empathy, self-regulation, emotional reflection) with practical digital tools, youth workers can design, deliver, and evaluate sessions that empower young people to recognise, respond to, and prevent these online risks.

What Is Blended Learning in This Context?

Here, blended learning extends beyond the simple combination of face-to-face and online modalities. It refers to the creation of interconnected learning ecosystems in which emotional, digital, and civic competences mutually reinforce one another. Central to this approach is a strong commitment to inclusion, ensuring that all young people—regardless of their background—can participate meaningfully and develop the skills they need to thrive in digital environments.

Purpose of Module 3

Module 3 provides practical methods, tools, and strategies to deliver that content in ways that are:

- Inclusive: Adaptable to diverse learner profiles (e.g., rural youth, neurodivergent learners, low digital literacy).



- Emotionally Intelligent: Grounded in EI principles (e.g., self-awareness, empathy, self-regulation).
- Blended: Combining online and offline approaches for maximum engagement and accessibility.

Actionable: Equipping youth workers with ready-to-use activities, templates, and evaluation tools.

Upon Completion of This Module, Youth Educators Will Gain:

1. A Robust Conceptual Grounding
 - A deep understanding of inclusive blended pedagogy and its role in fostering emotional resilience, digital literacy, and cybersecurity awareness.
 - Insights into how emotional intelligence (EI) intersects with online safety, and why this intersection is critical for youth development.
 - Knowledge of Universal Design for Learning (UDL) principles and how they ensure accessibility and equity in blended learning environments.
2. A Practical Toolkit
 - Methods and strategies for designing emotionally engaging and digitally literate blended sessions.
 - Digital tools (e.g., Moodle, Kahoot, Padlet, Canva) and offline alternatives to create interactive, inclusive, and safe learning experiences.
 - Micro-learning activities that can be easily integrated into existing youth programs, ensuring flexibility and adaptability.
3. The Ability to Design, Deliver, and Evaluate
 - Skills to design blended sessions that foster emotional resilience, online safety, engagement, and belonging.
 - Techniques to deliver content in ways that are emotionally intelligent, inclusive, and responsive to diverse youth profiles.
 - Tools to evaluate the effectiveness of sessions, including qualitative and quantitative measures of inclusivity, accessibility, and emotional impact.

Conceptual Framework

Blended Pedagogy for Online Safety

Blended learning in this module merges the **social richness of in-person interactions** with the **flexibility of digital delivery**, creating a **holistic learning ecosystem** that addresses the **eight key online risk areas**. According to Garrison & Vaughan (2008), effective blended design intentionally integrates **online and face-to-face experiences** to enhance **social, cognitive, and**



teaching presence. In youth work, this integration allows for **continuous emotional connection**—participants can extend discussions about **cyberbullying, phishing, or impersonation** from offline sessions into **digital forums**, sustaining reflection and engagement between meetings.

Emotional Intelligence (EI) and Online Risks

EI - the ability to **recognise, understand, and manage one's own emotions and those of others** (Salovey & Mayer, 1990)—is central to this framework. Embedding EI within blended learning helps youth workers and learners **manage frustration, conflict, and empathy** in online interactions.

For example:

- An **EI-based discussion** on **digital empathy** can transform **cyberbullying incidents** into opportunities for growth.
- **Self-regulation techniques** can help youth **resist impulsive responses** to **scams, phishing, or FOMO triggers**.
- **Empathy exercises** can reduce the likelihood of **posting regretful content** or falling for **impersonation attempts**.

Universal Design for Learning (UDL) for Digital Safety

CAST (2018) defines UDL as designing learning environments that **anticipate variability** by providing **multiple means of engagement, representation, and expression**. In this module, UDL ensures that all materials and activities are **accessible and adaptable** to diverse youth profiles, including those with **limited digital access, disabilities, or language barriers**.

Examples include:

- **Subtitles and transcripts** for videos on **phishing or malware prevention**.
- **Printable worksheets** for offline activities on **privacy risks or fake news**.
- **Low-tech alternatives** for youth in **rural or low-income contexts** to participate in discussions about **cyber predators or scams**.

Inclusion and Digital Equity in Online Safety Education

Inclusive blended learning addresses the **digital divide** by offering **both high-tech and low-tech options**, ensuring **equitable participation** for all youth.

This module emphasises:

- **Culturally relevant examples** for discussions on **cyberbullying or impersonation**.
- **Gender-balanced and neutral language** in activities about **privacy risks or regretful posts**.

- **Adaptable tools** (e.g., Padlet, Kahoot, Moodle) to accommodate **varied digital literacy levels** when teaching about **misinformation or malware**.

Keywords: Blended learning, emotional intelligence, universal design, digital equity, cyberbullying, phishing, scams, impersonation, privacy risks, fake news, malware, inclusion.

Pedagogical Model

This model provides a **cyclical, emotionally engaging, and inclusive** approach to teaching about the **eight online risk areas**. Each phase is designed to **build knowledge, skills, and emotional resilience** in young people.

Phase	Purpose	Examples of Practice	EI / Digital Focus
Connect	Build inclusion, trust, and emotional safety	Ice-breaker: "Share a time you felt unsafe online—was it due to cyberbullying, a scam, or impersonation? " Digital name wall for privacy risks or fake friend requests .	Empathy, self-awareness, and trust-building
Explore	Introduce concepts and risks related to the eight online risk areas	Short video on how phishing works + live poll: "What emotions might make someone click a suspicious link?" Discussion on FOMO scams or misinformation tactics .	Curiosity, awareness, and critical thinking
Practice	Apply learning through collaborative, hands-on activities	Role-plays: Responding to a cyber predator or fake friend request . Simulation: "What would you do if you accidentally downloaded malware? "	Self-regulation, decision-making, and peer support
Reflect	Analyse emotions, behaviours, and outcomes	Journals: "How did you feel during the phishing simulation? " Emotional mapping for regretful posts or cyberbullying incidents . Padlet boards: "What would you do differently if faced with a scam or impersonation attempt? "	Adaptability, critical reflection, and emotional resilience

Phase	Purpose	Examples of Practice	EI / Digital Focus
Share	Empower peer learning, leadership, and community engagement	Youth presentations: "How to spot fake news or a phishing email ." Online showcases: "My strategy for privacy protection and safe downloads ."	Social skills, agency, and peer mentorship

Keywords: Experiential learning, peer interaction, trust-building, self-regulation, digital citizenship, online safety.

Connect: Building Trust and Emotional Safety Purpose

The **Connect phase** focuses on **building relationships, trust, and emotional safety**—the foundation for effective learning. Youth need to feel **seen, heard, and valued** before engaging deeply with content, especially when addressing sensitive topics like **cyberbullying or privacy risks**.

Key Actions

- **Icebreakers and Check-Ins:** Use activities that encourage youth to **share their emotions, experiences, and expectations**. Example: "Two Truths and a Lie" (digital version: "Two Facts and a Fib" about online experiences).
- **Group Agreements:** Co-create **norms for respectful communication** (e.g., "We listen without judgment," "We keep personal stories confidential").
- **Diverse Representation:** Ensure all youth see themselves reflected in the **content and examples** used (e.g., case studies featuring different cultures, abilities, and genders).

EI Skills Developed

- **Self-Awareness:** Youth recognize their **emotions and biases** as they enter the learning space.
- **Empathy:** Youth practice **listening and validating** peers' experiences.
- **Belonging:** Youth feel **connected to the group**, reducing anxiety about participation.

Blended Learning Example



- **Online:** Use a **Padlet wall** where youth post emojis or short phrases representing how they feel about today's topic (e.g., cybersecurity).
- **Offline:** Follow up with a **circle discussion** where youth elaborate on their posts.

Explore: Introducing Concepts with Curiosity and Critical Thinking

Purpose

The **Explore phase** is about **sparking curiosity** and **introducing key concepts** in a way that encourages **critical thinking and emotional engagement**. Youth are invited to **ask questions, challenge assumptions, and connect** new ideas to their own lives.

Key Actions

- **Provocative Questions:** Start with open-ended questions like, *"What makes someone vulnerable to a phishing scam?"* or *"How do you think emotions play into sharing personal info online?"*
- **Multimedia Content:** Use **videos, infographics, or podcasts** to present information in engaging ways. Example: A short video on **"How Scammers Manipulate Emotions"** followed by a discussion.
- **Real-World Scenarios:** Present **case studies or news stories** about cyber risks (e.g., a teen who fell for a fake friend request).

EI Skills Developed

- **Curiosity:** Youth become **intrinsically motivated** to learn more.
- **Critical Thinking:** Youth **analyze and question** information rather than accepting it at face value.
- **Emotional Awareness:** Youth recognize how **emotions influence decisions** (e.g., fear leading to impulsive clicks).

Blended Learning Example

- **Online:** Youth watch a **TED-Ed video** on misinformation and post **one question** it raised for them on a shared document.
- **Offline:** In small groups, youth **discuss their questions** and brainstorm ways to verify online information.

Practice: Applying Skills in Safe, Supported Ways

Purpose

The **Practice phase** is where youth **apply what they've learned** in **low-stakes, supportive environments**. This phase focuses on **skill-building through experiential and collaborative activities**, helping youth **internalize** EI and digital safety strategies.

Key Actions

- **Role-Playing:** Simulate **real-life digital dilemmas** (e.g., responding to a cyberbully, spotting a phishing email). Example: "You receive a message saying, 'Click this link or your account will be deleted.' What do you do?"
- **Gamification:** Use **quizzes, escape rooms, or simulations** to reinforce learning. Example: A **Kahoot game** where youth identify red flags in fake social media profiles.
- **Peer Teaching:** Youth **teach each other** (e.g., one group explains how to set privacy settings, another demonstrates how to report harassment).

EI Skills Developed

- **Self-Regulation:** Youth practice **pausing and thinking** before acting online.
- **Problem-Solving:** Youth **develop strategies** to handle digital challenges.
- **Collaboration:** Youth work **together to solve problems**, building social skills.

Blended Learning Example

- **Online:** Youth complete a **digital escape room** where they solve puzzles related to online privacy.
- **Offline:** Debrief with a **group discussion** on what they learned and how they'd apply it in real life.

Reflect: Deepening Understanding Through Self-Awareness

Purpose

The **Reflect phase** encourages youth to **look inward** and **connect learning to their personal experiences**. Reflection helps youth **internalize lessons**, recognize growth, and identify areas for further development.

Key Actions

- **Journaling:** Youth write or record **reflections** on prompts like, "How did today's activity change how you think about sharing online?"
- **Group Sharing:** Youth **volunteer to share insights** in a circle or small group.
- **Creative Expression:** Youth create **art, poetry, or memes** to represent their learning.

EI Skills Developed

- **Self-Reflection:** Youth **examine their own behaviors and emotions**.

- **Growth Mindset:** Youth see **mistakes as learning opportunities**.
- **Empathy:** Youth **consider others' perspectives** and experiences.

Blended Learning Example

- **Online:** Youth submit a **short voice note or written reflection** on a platform like Flipgrid.
- **Offline:** Youth share their reflections in **pairs or small groups**, deepening the discussion.

Share: Amplifying Learning Through Community Purpose

The **Share phase** focuses on **amplifying youth voices** and **extending learning beyond the group**. Youth **teach others, create public projects, or advocate** for digital safety in their communities, reinforcing their own understanding and building confidence.

Key Actions

- **Youth-Led Workshops:** Youth **design and facilitate** mini-workshops for peers or younger students.
- **Digital Campaigns:** Youth create **PSAs, blogs, or social media posts** about cyber safety.
- **Community Projects:** Youth **collaborate with local organizations** (e.g., libraries, schools) to promote digital literacy.

EI Skills Developed

- **Leadership:** Youth **take ownership** of their learning and mentor others.
- **Advocacy:** Youth **use their voices** to promote safe and responsible digital behaviour.
- **Confidence:** Youth **gain pride** in their ability to make a difference.

Blended Learning Example

- **Online:** Youth create a **TikTok video or Instagram post** summarizing key lessons from the module.
- **Offline:** Youth present their projects at a **community event or school assembly**.

The Cyclical Nature of the Model

The five phases—**Connect, Explore, Practice, Reflect, Share**—are **not linear** but **cyclical**. After sharing, youth often **return to the Connect phase** with deeper trust and new questions, creating a **continuous loop of learning and growth**.



This model ensures that youth **build skills incrementally**, with **EI and digital competences** reinforcing each other at every step.

Practical Tips for Youth Workers

1. **Start Small:** Begin with **one or two phases** and gradually integrate the full cycle.
2. **Be Flexible:** Adapt the model to **your group's needs**—some youth may need more time to connect or reflect.
3. **Model EI:** Show youth how **you regulate your emotions, think critically, and reflect**—they'll follow your lead.
4. **Use Tech Intentionally:** Choose digital tools that **enhance engagement** without overwhelming youth (e.g., Padlet for reflection, Kahoot for practice).
5. **Celebrate Growth:** Acknowledge **small wins** and progress, not just final outcomes.

Implementation Guidelines

Introduction

This section provides **practical, step-by-step guidelines** for youth workers to **design, deliver, and evaluate** inclusive blended learning sessions. Whether you're teaching about **cybersecurity, emotional intelligence (EI), or digital literacy**, these guidelines will help you create **engaging, accessible, and effective** learning experiences for diverse youth groups.

Design for Inclusion and Accessibility

To ensure all youth—regardless of background, ability, or digital access—can engage with the **eight online risk areas**, follow these steps:

- **Map Learners' Needs:** Assess participants' **digital access levels, comfort with technology, and potential barriers** (e.g., language, disability, or socio-economic status).
 - Example: For youth with **limited digital access**, provide **printed materials** on **phishing, scams, or privacy risks** alongside digital resources.
- **Provide Multiple Means of Engagement:** Use **Universal Design for Learning (UDL)** to create **flexible, inclusive activities** for each risk area:
 - **Cyberbullying:** Offer role-play scripts (for in-person sessions) and interactive forums (for online discussions).
 - **Fake News:** Use visual infographics (for visual learners) and audio podcasts (for auditory learners) to explain misinformation tactics.
 - **Impersonation:** Include real-life case studies and anonymous chat simulations to explore emotional responses.



- **Culturally Relevant and Gender-Balanced Content:** Ensure examples and scenarios reflect **diverse cultural contexts** and **gender identities** to make discussions on **cyber predators, scams, or regretful posts** relatable and inclusive.

Create Emotionally Safe Spaces

Emotional safety is critical when addressing **sensitive online risks** like **cyberbullying, impersonation, or malware**. Use these strategies:

- **Emotional Check-Ins:** Start each session with a **check-in activity** focused on the **risk area** being discussed.
 - Example: “How do you feel about sharing personal information online?” (for **privacy risks**) or “Have you ever felt pressured by a **FOMO scam**?”
- **Establish Digital Citizenship Norms:** Co-create **group agreements** on respect, consent, and confidentiality.
 - Example: “We agree not to share others’ personal stories about **cyberbullying** or **regretful posts** without permission.”
- **Opt-Out Choices and Follow-Up Support:** Offer **alternative activities** for participants uncomfortable with certain topics (e.g., **cyber predators** or **malware**).
 - Example: Provide a **private reflection journal** for those who prefer not to discuss **scams** or **impersonation** in group settings.

Integrate Micro-Learning for Online Risks

Micro-learning breaks down complex topics into **short, engaging activities** (5–10 minutes) that focus on **one risk area at a time**:

- **Phishing:**
 - **Activity:** “Spot the Red Flags” – A **10-minute quiz** identifying suspicious elements in emails or messages.
 - **Tool:** Kahoot or Quizizz.
- **Scams (FOMO-Based):**
 - **Activity:** “Pressure Test” – A **short video** demonstrating how scammers use urgency, followed by a **discussion prompt**: “What emotions did this trigger?”
- **Fake News:**
 - **Activity:** “Fact or Fiction?” – A **5-minute challenge** to fact-check a viral post using **reverse image search** or **reliable sources**.
- **Cyberbullying:**
 - **Activity:** “Empathy in Action” – A **role-play scenario** where participants practice responding to hostile messages with empathy.

- **Tools for Micro-Learning:**
 - **Moodle** (for quizzes on **privacy** or **malware**).
 - **Canva Docs** (for creating **infographics** on **impersonation** or **scams**).
 - **Padlet** (for sharing personal strategies to avoid regretful posts).

Choose Accessible and Ethical Digital Tools

Select platforms that comply with **privacy**, **accessibility**, and **ethical standards** to teach about the **eight risk areas**:

Risk Area	Recommended Tools	Purpose
Cyberbullying	Padlet, Jamboard, Miro	Collaborative discussions, anonymous sharing, and emotional mapping.
Phishing/Scams	Kahoot, Quizizz, Moodle	Gamified quizzes to test knowledge of red flags and emotional triggers .
Fake News/Misinformation	Canva Docs, Google Slides	Creating fact-checking guides or infographics to debunk myths.
Privacy Risks	Mentimeter, Google Forms	Reflective polls: "What personal info would you never share online?"
Impersonation	Zoom (with captions), Flipgrid	Role-play videos or discussions on verifying identities and emotional responses .
Malware	Interactive simulations (e.g., Cybersecurity Labs)	Hands-on practice in identifying malicious links or downloads .
Regretful Posts	Padlet, Reflection Journals	Sharing lessons learned and alternative actions in a supportive space.

Risk Area	Recommended Tools	Purpose
Cyber Predators	Secure, moderated forums (e.g., Teams)	Discussing safe and online interactions and reporting mechanisms.

Facilitate Hybrid Engagement

Blend **live workshops** with **asynchronous reflection** to allow youth to **process emotions privately** before public discussions:

- **Example for Cyberbullying:**
 - **Live Workshop:** Role-play responses to **hostile messages**.
 - **Asynchronous Reflection:** Private journal prompt: "How did you feel during the role-play? What would you do differently?"
- **Example for Phishing/Scams:**
 - **Live Workshop:** Group analysis of a **suspicious email**.
 - **Asynchronous Reflection:** Padlet post: "What clues did you miss? How can you apply this to real life?"
- **Example for Fake News:**
 - **Live Workshop:** Debate the **impact of misinformation**.
 - **Asynchronous Reflection:** Research and share a **fact-checked article** on the topic.

Ethical and Data Protection Considerations

- **Anonymise Sensitive Content:** Remove personal details from case studies on cyberbullying or regretful posts.
- **Secure Platforms:** Use GDPR-compliant tools (e.g., Moodle, Teams) for discussions on privacy risks or impersonation.
- **Consent and Confidentiality:** Ensure participants understand how their data (e.g., journal entries) will be used and protected.

Key Takeaways for Youth Workers

1. **Plan with Purpose:** Align every activity with **clear objectives** and **EI skills**.
2. **Design for All:** Use **UDL** to ensure **accessibility and engagement**.
3. **Choose Tools Wisely:** Select **digital and offline tools** that enhance learning without overwhelming youth.
4. **Facilitate with EI:** Model **emotional awareness** and create a **safe, supportive environment**.
5. **Evaluate and Adapt:** Use **feedback and observations** to refine your approach.



Keywords: Inclusive design, emotional safety, micro-learning, accessibility, digital tools, hybrid engagement, UDL, privacy, ethical considerations.

Evaluation and Reflection

Inclusive blended learning requires multi-level evaluation to assess knowledge, skills, attitudes, and emotional resilience related to the eight online risk areas. Use the following methods to measure impact and refine practice:

Knowledge and Skills Assessment

Evaluate participants' understanding of **online risks** and their ability to apply **EI and digital safety strategies**:

- **Pre/Post-Tests:**
 - **Cyberbullying:** Quiz on **recognising hostile communication** and **empathic responses**.
 - **Phishing/Scams:** Test ability to **identify red flags** in emails or messages.
 - **Fake News:** Fact-checking exercise to **spot misinformation**.
 - **Privacy Risks:** Scenario-based questions on **sharing personal information safely**.
 - **Malware:** Identification of **suspicious links or downloads**.
- **Skills Demonstrations:**
 - Role-plays for **responding to cyber predators, impersonation, or FOMO scams**.
 - Simulations for **reporting cyberbullying or regretful posts**.

Behavioural Change Observation

Track **changes in behaviour and emotional responses** during activities focused on the **eight risk areas**:

Risk Area	Observation Focus	Tools/Methods
Cyberbullying	Empathy, de-escalation, and peer support in discussions.	Group activities, peer feedback.
Phishing/Scams	Critical thinking and self-regulation when faced with suspicious content.	Live polls, scenario analyses.
Fake News	Ability to question sources and avoid sharing unverified information.	Debates, fact-checking tasks.



Risk Area	Observation Focus	Tools/Methods
Impersonation	Caution and emotional awareness when verifying online identities.	Role-plays, reflection journals.
Privacy Risks	Decision-making about sharing personal information.	Case studies, group discussions.
Regretful Posts	Self-reflection on past posts and future intentions.	Journal prompts, Padlet sharing.
Malware	Vigilance in identifying and avoiding malicious content.	Interactive simulations, quizzes.
Cyber Predators	Assertiveness in setting boundaries and seeking help.	Role-plays, scenario analyses.

Engagement Analytics

Use **digital platform data** to assess participation and engagement with **online risk content**:

- **Padlet/Kahoot:** Track responses to **phishing quizzes** or **cyberbullying discussions**.
- **Moodle/Teams:** Monitor completion of **micro-learning modules** on **scams, fake news, or privacy**.
- **Mentimeter/Google Forms:** Analyse **emotional check-in** responses related to **impersonation or malware**.

Reflection Logs and Journals

Encourage **weekly reflections** to connect **emotions, actions, and learning** across the **eight risk areas**:

- **Prompt Examples:**
 - **Cyberbullying:** "Describe a time you witnessed or experienced cyberbullying. How did you feel? What would you do now?"
 - **Phishing:** "What emotions might make someone fall for a scam? How can you use **self-regulation** to stay safe?"
 - **Fake News:** "How did you verify a piece of information this week? What challenges did you face?"

- **Privacy Risks:** “What personal information do you wish you hadn’t shared? Why?”
- **Malware:** “What steps do you take to avoid accidental downloads? How do you feel when you’re unsure about a link?”
- **Facilitator Feedback:** Review journals to **identify recurring emotional triggers** (e.g., fear, curiosity) and **adapt activities** accordingly.

Inclusion Audit

Use a **checklist** to evaluate the **accessibility and inclusivity** of activities for all youth:

Criteria	Examples
UDL Compliance	Are materials available in multiple formats (text, audio, visual) for phishing or scams ?
Cultural Relevance	Do examples reflect diverse experiences of cyberbullying or impersonation ?
Digital Accessibility	Are low-tech alternatives provided for malware or privacy activities?
Emotional Safety	Were opt-out choices offered for sensitive topics like cyber predators ?
Language Clarity	Is language neutral and understandable for discussions on regretful posts or fake news ?

Key Takeaways

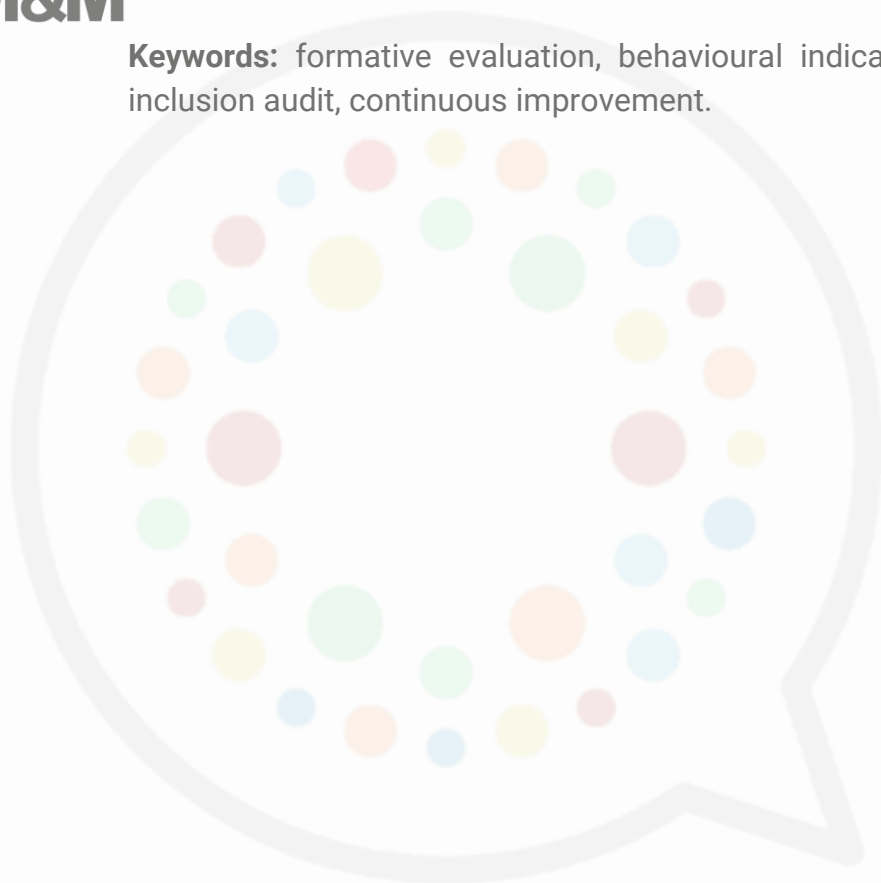
1. **Evaluation is ongoing:** Use **formative and summative assessments** to guide and measure learning.
2. **Reflection deepens learning:** Encourage youth to **connect lessons to their lives** through journaling, discussion, or creative expression.
3. **Inclusivity matters:** Regularly audit your sessions to ensure **all youth feel included and supported**.
4. **Adapt and improve:** Use feedback to **refine your practice** and better meet youth’s needs.

Youth workers should model reflection by maintaining their own facilitation diary—documenting emotional tone, group dynamics, and improvements for future cycles. Evaluation data feed directly into the EM&M project’s continuous-improvement framework.



EM&M

Keywords: formative evaluation, behavioural indicators, reflection journals, inclusion audit, continuous improvement.



Module 4 - Online Vulnerability Assessment and Threat Recognition Exercises

Module Overview

Module 4 equips youth workers and educators with practical tools, assessments, and exercises to help young people identify, understand, and respond to online threats in emotionally intelligent ways. It builds on the fundamentals from Module 1, moving into hands-on activities that blend technical awareness with Emotional Intelligence (EI) skills. The focus is on strengthening youth resilience, critical thinking, and calm decision-making when facing cyber threats. This module provides step-by-step activities, ready-to-use assessment tools, and scenario-based learning experiences that link behavioural and emotional vulnerabilities to concrete preventive strategies.

A key aspect of Module 4 is adaptability: it's designed for blended delivery across diverse contexts and infrastructures. Whether a youth worker has a high-tech lab or just a single smartphone in a community center, the exercises can be adjusted (many have mobile-first or low-bandwidth options). We also integrate gamification elements and popular platforms (like Kahoot, Padlet, or Discord) to meet youth where they are and make learning engaging. This module aligns with the shared handbook structure and blended teaching approach of the program, and it incorporates insights from the comparative study on youth cyber behaviours.

In essence, Module 4 takes the “what” and “why” from Module 1 (and other earlier modules) and turns it into the “how” – how to assess vulnerabilities, how to recognise threats quickly, and how to practice EI-based responses. The ultimate goal is to promote preventive digital behaviours and peer support structures that can sustain safe online practices over time, even after the formal training ends.

Learning Objectives

By the end of this module, youth workers and educators will be able to:

- **Identify** common online vulnerabilities among youth across multiple dimensions: technical (e.g., outdated software), behavioural (e.g., oversharing, impulsive clicking), emotional (e.g., stress responses), and social (e.g., peer pressure, trusting strangers).
- **Implement** short, accessible self-assessments to gauge a young person's risk exposure and awareness level. (For instance, using a checklist or quiz to reveal if someone is prone to trust online strangers or skip privacy settings.)

- **Facilitate** threat recognition exercises that combine spotting technical cues (like a fake URL or a suspicious profile) with emotional reflection (noticing how a scam attempt made them feel) and regulation (using EI techniques to stay calm).
- **Integrate** EI strategies - such as stress management, adaptability, empathy, and calm communication - into cybersecurity training activities. Rather than teaching cyber awareness and emotional skills separately, they will blend them (e.g., teaching breathing techniques in the middle of a phishing simulation).
- **Deliver** blended, inclusive, and gamified sessions using tools commonly preferred by the target group. They'll also be able to adapt these exercises to low-connectivity settings. For example, knowing how to run a "quiz" game offline with pen-and-paper if Kahoot isn't available, or how to tweak a role-play for a small informal group versus a classroom.
- **Promote** preventive behaviours and peer support in youth communities. This means encouraging habits like regular privacy checks, critical thinking before sharing information, helping friends identify scams, and creating a culture where youths remind each other to stay safe (becoming a "human firewall" together).

Module Content

Understanding Online Vulnerability

In cybersecurity, a vulnerability is basically a weakness or gap that could be exploited by a threat. This module broadens that concept to include not just technical weaknesses, but also human and emotional factors. We look at categories of vulnerability such as:

- **Technical Vulnerabilities:** Hardware or software weaknesses. For example, using outdated software, not installing security updates, weak passwords, no antivirus, or using default settings. These are like "open windows" in one's digital house. They can lead to issues like accidentally downloading malware (if your system isn't patched) or getting hacked because your password is guessable.
- **Behavioural Vulnerabilities:** Unsafe habits or behaviours online. For example, oversharing personal information (posting your phone number or address publicly, or sharing intimate photos), impulsively clicking on things without scepticism, accepting friend requests from strangers, or using the same password everywhere. These behaviours increase risk. Posting private information that you might later regret is a classic behavioural vulnerability - once something is online, it's hard to take back, and it could be used against you (like a cyberbully or predator saving that info).

- **Emotional Vulnerabilities:** Ways in which our feelings can make us less safe online. Emotions influence risk perception; for instance, if someone is feeling lonely or craving validation, they might be more trusting of an online stranger (predators often exploit this, posing as a friend or romantic interest). If someone is angry or upset, they might react by posting something aggressive or clicking a malicious link out of spite (not thinking clearly). Even positive emotions like excitement can be a vulnerability (getting overly excited about a “prize” and not noticing the scam).
- **Social Vulnerabilities:** These overlap with behavioural and emotional but involve the social environment. Peer pressure, herd behaviour, and trust in online communities fall here. For example, if “everyone is doing this new trending challenge,” a teen might ignore the risks (malware or privacy issues) because of social pressure. Or trusting a recommendation just because a friend shared it, without checking credibility (which is how misinformation spreads). Fake friend requests or impersonation is another social vulnerability area - youth might accept a request because they have mutual friends, not realising it’s a fake profile (possibly a cyber predator or scammer).

(Note: In Module 1, we introduced “vulnerability” simply. Here we expand it. Some models combine social with behavioural or emotional, but we find it useful to discuss social factors explicitly, hence the separate mention.)

How emotions influence risk: A purely technical issue can be worsened by human factors - e.g., an outdated app (technical) becomes a problem only if someone clicks a malicious link (behavioural) which they did because they were curious or fearful (emotional).

E.g.: A teenager fell victim to an online grooming situation (predator case). Analysis: The social vulnerability was that she trusted someone who flattered her in a game chat; the emotional vulnerability was her low self-esteem (she craved the compliments); the predator exploited that to extract personal photos (behavioural vulnerability: she shared private info). No advanced hacking was needed - just emotional manipulation.

Another example: A group of students spread a fake news article about a health scare. They didn’t verify it (behavioural vulnerability: not checking sources) because it made them anxious and it was trending (emotional + social factors: fear and herd behaviour). This led to panic and some even clicking a link in the fake news that stole their data (there was a phishing link in the article).



One more: A student's laptop got a virus after downloading free pirated music software (technical vulnerability: no antivirus and downloading from untrusted source; behavioural: desire for free stuff overcame caution; emotional: maybe excitement or peer influence because friends were also getting freebies).

The key point: Understanding one's vulnerabilities is empowering, not embarrassing. Everyone has vulnerabilities; by identifying them, we can take action (like strengthening a weak point). And while we can't eliminate all vulnerabilities (we're human, we'll have emotions and make mistakes), we can build awareness to reduce how much they expose us.

Threat Recognition: From Awareness to Action

Here we connect common threats that youth face with the psychological responses those threats often trigger, and how to train youth to go from initial awareness of a threat to taking proper action.

Common youth-oriented threats:

- **Phishing:** Fraudulent attempts to steal information (via email, texts, DMs). This includes things like fake login pages, "reset your password" scams, or phony prize links. Phishing is very prevalent and often tailored to what youth care about (e.g., free game skins, event tickets, or social media account verifications).
- **Fake Profiles & Impersonation:** Accounts that are not who they claim to be. This could be a stranger posing as a peer to gain trust (sometimes with predatory intent), or someone impersonating a known figure (like a fake celebrity account asking for money for charity), or a hacker who took over a real friend's account. These lead to scams or grooming.
- **Cyber Predators & Grooming:** Adults (or sometimes other youth) who befriend minors online to exploit or abuse them. They often use fake profiles and emotional manipulation (flattery, gifts, empathy) to gain the victim's trust over time. This is a serious threat with emotional and physical safety implications.
- **Identity Theft & Account Takeovers:** Stealing personal data or hijacking accounts. Youth may think they have "no identity to steal," but stealing a gaming account or social account is identity theft too. Also, if they reuse passwords and one leaks, attackers can take over accounts and then scam their friends or ruin their reputation.
- **Misinformation/Disinformation:** The spread of false information, which can mislead youth into unsafe actions or simply make them anxious or angry. For instance, fake news about a scholarship opportunity that's actually a scam link, or rumours that incite bullying ("So-and-so did something terrible..." when it's not true). Teaching youth to recognise

missing context or fishy claims and to verify news is part of threat recognition.

- **Cyberbullying and Harassment:** While not “technical threats,” these are pervasive online dangers for youth. Nasty messages, public shaming posts, rumour-spreading - they threaten a young person’s emotional well-being and can lead to unsafe choices (like meeting an aggressor to confront them or retaliating and getting into worse trouble).
- **Malware & “Accidental” Downloads:** Tricks that lead youth to unknowingly download viruses or malicious apps. For example, a pop-up says, “Your device is infected, click to clean” (ironic trick that actually installs malware), or a free download for a game cheat that is actually malware. Young people may not always recognise the signs of a fake download site or a malicious app.
- **Scams and Fraud:** Beyond phishing, things like online shopping scams (paying for a product that never arrives), “get rich quick” schemes targeting teens (maybe via social media ads), or romance scams (older teens might be targeted on dating apps or platforms, not realising the person is fake and after money).

For each threat type, the typical emotional or psychological response it tries to provoke should be mentioned:

- **Phishing** often uses fear (account problem) or excitement (you won something).
- **Impersonation** uses trust and confusion (you think it’s your friend or someone legit).
- **Predators** use empathy, love, and secrecy (they make the youth feel understood, special, and may instil fear of telling others).
- **Misinformation** uses strong emotions like anger or urgency (outrage at something, or fear-based rumours).
- **Cyberbullying** triggers hurt, anger, or shame.
- **Malware** prompts might use fear (scareware “you’re infected!”) or curiosity (“click here for a surprise”).
- **Scams** use greed, excitement, or sometimes compassion (as in fake charity scams).

Psychological responses to threat stimuli: It’s important to discuss how our brains react to these triggers. Often, it’s fight, flight, or freeze - or in cognitive terms, panic, denial, or impulsivity. For example:

- **Fear/Panic:** A phishing alert might cause panic, and the person hastily follows instructions (fight impulse to solve it quickly).

- **Denial/Ignore:** Some might see a threat (like a news about a virus outbreak) and go into denial (“this can’t be real”), which can also be dangerous if they ignore legit warnings. Or a student might ignore signs of a predator because they don’t want it to be true.
- **Impulsivity:** An excited or angry state can make someone act without thinking (click a link, send a mean reply, etc.) almost automatically.
- **Overwhelm/Freeze:** Sometimes too many warnings or threats lead to numbness - a youth might see so many “security alerts” they just glaze over (which some scammers exploit by sending multiple emails, so the person gives up and clicks one).

The goal is to get from awareness to action calmly. So how do we teach youth to go from “I sense a threat” (or even better, spot cues of a threat before it fully hits) to “I will act (or not act) in a safe way”? We apply EI-based prevention: Awareness-Reflection- Regulation-Response (the same cycle from Module 1, now in action).

So, when teaching threat recognition:

1. Start with Awareness of cues: e.g., noticing a URL is strange, or noticing “this person is overly nice too soon,” or “this message has lots of typos.” Also, self-awareness of emotions: “I feel myself getting upset at this comment.”
2. Then Reflection: analyse why it’s a threat or why you feel that way. “This seems fishy because why would a contest ask for money? My heart is pounding, could be because this is scaring me - maybe that’s what they want.”
3. Then Regulation: manage the emotion (take a breath, don’t react immediately, maybe talk to someone). This prevents knee-jerk mistakes.
4. Finally, Response: take an action step - which might be not responding to the bait, but rather reporting the user, or verifying info elsewhere, or using a technical tool (like running an antivirus scan, changing a password, etc.), or simply blocking someone.

Teach youth a sort of checklist for threat recognition:

1. Spot - Is anything off or trying to make me emotional? (If yes, pause.)
2. Think - What kind of threat could this be? (Phish, scam, bully, etc.) What do they want me to do?
3. Feel - What am I feeling? Name it (I’m scared/excited/etc.) so I can control it.
4. Breathe/Calm - Take a moment to not let that feeling run the show.

5. Verify - Check through another method if possible (don't trust the message content blindly).
6. Act Safely - Choose to ignore, block, get help, or respond with caution as needed.

Through repetitive exercises (like those in this module's activities), youth will ideally build a habit that when something odd happens online, their default is to pause and analyse rather than to react blindly. An analogy: like teaching defensive driving – you train drivers to recognise potential hazards (a child on the sidewalk might run into the road, a car ahead is swerving) and respond calmly (brake, steer smoothly) instead of either not noticing or overreacting.

Vulnerability Assessment Tools

This section covers how to gauge the current awareness and habits of youth regarding online safety – basically, quick self-assessments and diagnostics – and how to use those results to spark reflection and improvement.

Designing short, accessible self-assessments: We provide or suggest questionnaires, checklists, or quizzes that youth can take to find out where they stand on cyber safety behaviours and emotional readiness. Key qualities of these tools:

- **Short:** 5-10 questions, so as not to lose attention. They can be done in 5 minutes.
- **Youth-friendly language:** No jargon in the questions. For instance, instead of "Do you practice good cyber hygiene daily?" ask "Do you update your apps and phone when they tell you to?"
- **Covers technical, behavioural, emotional aspects:** For example, questions might include: "I use different passwords for different accounts" (technical habit), "I often post personal stuff online without thinking" (behavioural habit), "When I get upset by something online, I react immediately" (emotional habit), "If a friend sends me a weird link, I'll click it because I trust them" (social/behavioural habit).
- **Likert or multiple-choice format:** Easier for youth to respond. E.g., Almost Always / Sometimes / Rarely / Never - as shown in Handout_M4 (Annex 1). This is less intimidating than open-ended and provides some quantifiable measure.
- **Using digital tools for anonymous responses:** Many youths open up more when responses are anonymous. Suggest using tools like Google Forms, Kahoot (survey mode), Mentimeter, or even a simple poll on Discord/Telegram if working with an online group. These allow instant aggregation of results too. If tech is not available, the same can be done with paper slips collected in a box to ensure privacy.

- **Group reflection on patterns:** After the self-assessment, it's crucial to discuss what the general results show (without singling anyone out). For example, you might say, "It looks like only 2 out of 20 of us always pause before responding to unexpected messages - that's something we can work on," or "Many of you said you rarely update your apps; updates can patch security holes, so let's talk about why updates matter."

The idea is to find patterns of behaviour and emotion:

- Do many young people admit to acting when emotional? Then stress management should be emphasised.
- Do few young people use privacy settings or 2FA? Then technical quick fixes can be implemented.
- Are they comfortable seeking help (did they tick they ask for help often or not)? If not, maybe there's a trust issue or lack of knowledge on where to get help – so we address that.

One can create a simple chart or tally from the responses to visualise it. For example, question "I recognise when emotion is used to make me act fast" - if mostly "Rarely" or "Never," then clearly, they need practice in spotting emotional manipulation.

These tools are not to score or shame anyone, but to provide a baseline and a personalised insight. Emphasise: "This isn't a test. There's no grade. It's to make you think about what you do now, so you can decide if you want to do anything differently going forward." It turns abstract advice into something more concrete: "Oh, I answered 'Never' to updating my phone – that's a risk I didn't realise I was taking."

Often, even just taking the quiz prompts self-reflection: "Wow, I answered that I often click without thinking - maybe I should change that." As an educator, you can capitalize on that by having them set a micro-goal.

Encourage sharing in pairs or small groups after (if they're comfortable): "Did anything in your answers surprise you?" or "What's one thing you think you're doing well and one thing you might improve?" This peer discussion normalises that everyone has some "Rarely" responses – nobody's perfect - but everyone can choose something to get better at.

Gamification and Scenario-Based Learning

This section explains why we use games and scenarios, and how to integrate these with emotional learning components.

Why gamification increases awareness retention: Gamification means using game elements (points, competition, challenges, rewards) to make learning fun



and engaging. For cybersecurity, a field that can be dry or scary, games make it approachable. Youth are used to playing games, so attention and retention go up when they're having fun. A quiz with a leaderboard (like Kahoot) can make them eager to know the right answers about phishing. A "find the flag" challenge can motivate them to learn a security trick to win. Research has shown that well-designed cybersecurity games improve learning outcomes by immersing participants in experiences rather than just lectures.

Important: gamification should not overshadow the learning goals. It's a means to an end. We use it to hook interest and encourage participation, especially for topics like safe online behaviour that can sound preachy otherwise.

Emotional learning through role-play and problem-solving: Scenario-based learning (like role-plays, case studies, simulations) is powerful because it puts youth in a context to apply skills. It's learning by doing. Adding role-play especially lets them feel some of the emotions in a controlled setting. For example, a role-play of a peer pressuring another to share a password can stir feelings of discomfort and show them how hard it can be – but also let them practice refusing. This builds emotional resilience for the real thing.

We integrate emotional intelligence by:

- Debriefing not just "what happened" in the scenario, but "how did it feel?" and "how did you manage that feeling?"
- Encouraging empathy in games: e.g., in a cyberbullying scenario, having someone play the target and someone the bully can increase empathy when discussed after.
- Encouraging team problem-solving in games: e.g., a group puzzle to spot all red flags in a fake profile gets them talking and managing maybe a little stress or time pressure together, which builds social-emotional skills like communication and teamwork.

Integration with platforms:

- **Genially or Canva:** These can be used to create interactive content or digital escape room puzzles related to cybersecurity (like a series of clues and locks to open using cyber knowledge).
- **Padlet:** Great for collaborative brainstorming or posting answers in a gamey way (like a digital gallery walk of ideas).
- **Moodle:** If a formal learning environment is available, there are gamified lesson formats or quiz modules.
- **Discord:** Many young people use Discord; it can host quizzes (through bots) or just be a space to run scenario discussions or even real-time

“simulations” (like simulate a phishing attack via a Discord message to see reactions in a safe way).

- **Kahoot/Mentimeter/Quizizz:** for quizzes, polls, interactive questions with competitive elements.
- **Canva/Genially for story games:** You can create a “choose your own adventure” story where their choices lead to different outcomes (good if technology allows).
- **Creately or Miro:** for mind-mapping or vulnerability mapping games.

The idea is also to note low-tech adaptations: if no devices, you can still gamify by using printed cards, having teams compete to sort cards fastest, or turn scenarios into a board game format, etc. (This is detailed more in next section, but it’s worth acknowledging here.)

Linking cybersecurity challenges with EI triggers: When designing these game scenarios, deliberately include emotional elements:

- A timed quiz induces pressure (how do they handle that? Debrief it).
- A role-play might involve someone acting angry or begging (triggers empathy or anxiety).
- A team game might have competition (triggers excitement or stress).

After/during each, pause to reflect: How did that make you feel? Did anyone feel rushed or frustrated? That’s similar to real life - how do we handle it? For example, in a simulation of a “cyber incident under pressure,” you might see teams get flustered – later point out, “Notice how the countdown made you all anxious – that’s exactly what attackers hope for. What strategies worked to stay calm?”

By doing this, you ensure the emotional side isn’t lost in the excitement. Youth learn not just the technical skill (spot the fake URL), but also an emotional skill (stay calm even if a timer is ticking or a person is yelling).

Blended Delivery Guidelines

This part offers practical advice for running the above content in various settings, ensuring inclusivity and engagement regardless of resources.

Balancing online and offline components: The ideal mix might vary, but a blended approach could involve, say, 50% in-person discussion/activities and 50% online tools. Online components (like a Kahoot quiz or a digital scavenger hunt) are great for visual engagement and scalability; offline components (like a circle discussion or physical role-play) are great for personal connection and for low-tech environments.



An example ratio could be: start with an offline icebreaker, then an online quiz, then an offline role-play, then maybe an online collaborative Padlet reflection.

If connectivity is an issue, plan a low-tech fallback for each online activity. E.g., if Kahoot fails, have the quiz printed or just read questions aloud and use show of hands or written answers with teams. If an online form can't be accessed, do the questions orally or on paper.

Conversely, if in a lockdown or remote scenario, ensure every offline idea has an online equivalent: e.g., role-plays can be done via Zoom breakouts, or vulnerability maps can be drawn in a shared Miro board.

Managing engagement in low-connectivity environments:

Some tips:

- Pre-download or print materials (screenshots of phishing examples, etc.) if you can't rely on live internet.
- Use SMS-based or chat-based solutions if internet is absent but phones are present (for instance, a quiz could even be done via an SMS poll or just texting answers to the facilitator).
- Leverage storytelling and imagination more when you can't show videos or flashy content. A well-told story of a relatable scenario can captivate an audience without any tech.
- Encourage role-play and discussions, which require no tech at all but are very engaging and interactive.
- Keep any tech use very lightweight (e.g., an offline PowerPoint or a single phone with data that can load a few pages which you then describe to others).

Inclusive facilitation for mixed groups: You might have youth with different backgrounds (urban vs rural tech exposure, different genders, varying skill levels):

- Avoid assumptions. Don't assume everyone knows certain apps or everyone has the same experience. Clarify and define terms as needed. For example, some might not be on Instagram but use TikTok - try to use examples from multiple platforms.
- Gender considerations: Be mindful that in some contexts, girls might experience certain threats (like predators or harassment) differently than boys, or vice versa (boys might underreport being bullied due to stigma, etc.). Ensure examples include a range of perspectives (e.g., mention that anyone can be a victim of a scam or predator; don't frame it as only one gender is targeted).



- Encourage sharing from all but also respect if some are quiet. Use small group discussions to give everyone a voice. Sometimes those from less privileged backgrounds might hesitate; smaller groups feel safer.
- If there's a big skill gap (some are very cyber-savvy, others not at all), consider pairing them in mixed-skill teams for activities so they learn from each other. The savvy ones might shine in spotting technical flags, while the less savvy might offer a fresh perspective or ask questions that lead to important clarifications.
- Provide alternative ways to participate: writing, drawing, speaking - not just one. For instance, in a "spot the risk" exercise, someone could circle things on a printout if they aren't comfortable speaking up.

Adapting exercises to context: If you're in a school vs an NGO drop-in centre vs a library, consider:

- Time constraints: In a school you might have short class periods; choose or break activities accordingly. In a workshop, you might have a longer block; you can combine a couple of activities or go deeper.
- Formal vs informal: In formal classrooms, you might need to align with curriculum or get certain approvals. In informal settings, you can be more flexible or creative.
- Cultural context: Some topics (like discussing predators or certain scam examples) might be sensitive in certain cultures. Adapt scenarios to be culturally appropriate and relevant. For example, maybe emphasise scams around popular local apps or local language examples.
- Physical space: If you have a big room, you can do moving games (like posting "True" "False" signs in corners and have youth move to them). If space is tight, keep activities seated or use small group at tables.

Finally, no matter how delivered, the core is to get youth engaged, thinking, feeling, and doing. The content is only effective if they are active participants, not passive listeners.



Module 5 - My Role as Youth Ambassador for Security Culture

Module Overview

This module provides information on how youth workers can take on the role of ambassadors for security culture who both educate and support young people in developing mindful, emotionally intelligent, and responsible digital behaviours. Acting as ambassadors, youth workers serve as credible messengers who build trust, guide young people toward safe online practices, and advocate for their voices to be heard in matters that affect their digital engagement.

Security culture goes beyond technical protection or risk prevention. It is about cultivating shared values, daily habits, and social norms that promote trust, respect, empathy, and collective responsibility in digital spaces. Youth workers play a pivotal role in translating these values into practice, guiding young people to recognise risks, manage emotions, and make informed decisions when interacting online.

When trained and supported, youth workers as ambassadors are able to:

Model secure and ethical digital habits that young people can use in their daily interactions.

Design and deliver micro-campaigns, workshops, and peer-learning sessions that raise awareness about online risks and emotional well-being.

Provide accurate resources to help young people access professional or community support when challenges arise.

Mediate online conflicts using emotional intelligence skills such as self-regulation, empathy, and assertive communication.

Beyond their educational role, youth workers act as advocates and bridge-builders between young people and the wider community. They represent youth perspectives in dialogues with institutions, NGOs, and decision-makers on various issues, including digital inclusion, mental health, sustainability, and civic engagement.

The module offers practical methodologies, examples, and tools that enable youth workers to integrate this ambassadorial approach into their daily work. It supports them in designing participatory activities, mentoring young leaders, and promoting a culture of security, empathy, and shared responsibility across online and offline spaces.

Learning Objectives

By the end of this module, youth workers will be able to:

1. Understand and apply the principles of security culture, fostering safe, responsible, and empathetic online behaviour among young people.
2. Adopt the ambassadorial approach, serving as role models who demonstrate secure digital habits and emotional intelligence in online interactions.
3. Educate and support young people in making mindful digital decisions, recognising risks, and responding constructively to online challenges.
4. Design and implement awareness-raising initiatives, such as workshops, campaigns, and peer-learning sessions, that promote a shared culture of online safety.
5. Provide guidance and conflict mediation when young people face digital dilemmas, using empathy, self-regulation, and assertive communication.
6. Act as advocates and bridge-builders, amplifying youth voices and connecting them with institutions and stakeholders to strengthen inclusive, sustainable, and resilient digital communities.

Module Content

Understanding Security Culture

In the EM&M framework, security culture goes beyond cybersecurity or data protection. It is a shared set of values, attitudes, and behaviours that promote emotional safety, ethical responsibility, and collective trust in digital environments.

It combines technical awareness (knowing how to stay safe online) with emotional and social intelligence (knowing how to react, connect, and support others mindfully).

A youth worker promoting a security culture supports young people to:

- Recognise digital risks and emotional triggers.
- Build resilience against manipulation, misinformation, and online hostility.
- Use empathy and self-awareness to guide their online actions.
- Understand that emotional safety is part of digital safety.

Security culture, therefore, represents a community mindset: protecting oneself and others through respect, responsibility, and active care in the digital world.

Tip: Invite young people to co-design a short “Digital Kindness Poster” with five rules for safe and respectful online behaviour. Display it in your youth space or on social media to promote collective responsibility.



The Role of the Youth Worker as Ambassador

Youth workers are not just educators; they are mentors, leaders, and advocates who influence how young people perceive and engage with the digital world. When acting as ambassadors, they become credible messengers trusted by youth and recognised by communities for their commitment to digital well-being.

Leading by example

Youth workers demonstrate integrity and self-awareness in digital interactions. Their conduct, online and offline, models the responsible behaviour they aim to instil. They show that secure engagement is not only about avoiding threats but about living digital values: authenticity, respect, inclusion, and empathy.

Example: A youth worker who transparently discusses a personal experience of cyberbullying and how they handled it through emotional regulation provides both guidance and reassurance to young people.

Tip: Occasionally show your group how you verify news before sharing it or how you handle disagreement respectfully in comments. Real examples make role modelling visible and relatable.

Acting as mentors

As mentors, ambassadors accompany young people in reflecting on their digital identity, online choices, and emotional responses. They ask guiding questions rather than giving direct answers, encouraging critical thinking:

- *How did that online interaction make you feel?*
- *What could you do differently next time?*
- *Who could you reach out to if something feels wrong?*

Mentoring is about empowering self-awareness and agency rather than control.

In this direction, through supportive and reflective dialogue, ambassadors' role consists of helping the youth explore:

- How being thoughtful before posting can protect them from unwanted attention or harm later.
- How adjusting privacy settings allows them to choose who can view their content, message them, or comment on their posts.
- How reporting or restricting harmful interactions can help them regain control of their online environment.

- How tools like blocking, muting, or limiting comments can reduce exposure to negative or distressing behaviour, often without the other person knowing.
- How reviewing or editing past posts can support a digital identity they feel comfortable with.

This can be achieved by prompting questions, such as:

- Before posting this, how might you feel if someone used it out of context later?
- What information about yourself feels safe to share? What feels too personal?
- Who can see your content right now, and who would you prefer to see it?

Tip: Organise “digital reflection circles” where youth share weekly online experiences and discuss emotions or challenges they faced. Use these sessions to normalise emotional reflection in digital contexts.

Advocates and bridge-builders

Ambassadors connect youth with stakeholders such as schools, NGOs, municipalities, and online safety initiatives, ensuring young people’s voices shape digital inclusion and well-being policies. They also mediate between generations, helping adults understand the digital realities of youth and helping youth communicate their needs confidently and respectfully.

Tip: Facilitate an intergenerational discussion between parents and young people about “trust online.” Have each side express their concerns and expectations, then build a “digital agreement” together.

Leadership and Communication for Security Culture

Developing a security culture among young people requires leadership grounded in empathy and emotional intelligence.

Leadership as service

Youth ambassadors lead not by authority but by example. They serve as catalysts for empowerment, encouraging others to adopt safe, mindful, and inclusive digital behaviours.

Leadership here means:

- Listening before acting
- Building trust-based relationships
- Fostering participation and shared ownership



Tip: Encourage your group to take leadership in designing their own awareness actions, such as creating digital posters, short videos, or hashtags promoting online empathy or factchecking.

Advocacy and visibility

Ambassadors amplify young voices. By supporting youth-led initiatives, campaigns, or peer mentoring, they give visibility to positive digital practices. They can help young people co-design short awareness actions (posters, podcasts, reels) to promote kindness, fact-checking, or online empathy.

Tip: Support youth to run a social media campaign (e.g., “#ThinkBeforeYouType” or “#EmotionCheck”) and help them measure its reach and engagement.

Case Study: UNICEF’s “Kindly”

A practical example of empathy in the cyber world is UNICEF’s Kindly initiative, an AI-powered platform designed to help young people reflect on the emotional tone of their messages before posting them. Kindly does not punish or shame; instead, it encourages young people to take a moment to consider how their words might impact others, and explore alternative, kinder messages. This reflective, supportive approach demonstrates how emotional intelligence in digital spaces can be showcased without authority or enforcement. Both youth and adults use Kindly to examine their online communication, learning to translate emotional intelligence into everyday digital behaviour.

For ambassadors, Kindly illustrates a practical example of how to create environments that help youth engage safely, think critically, and regulate their emotional responses. It also shows the power of advocacy and visibility, as UNICEF elevates youth voices by encouraging them to co-create content, test features, and share their experiences. Many young users have launched micro-campaigns inspired by Kindly, sharing before-and-after messages, creating kindness challenges, or producing short videos on how a moment of empathy can change an entire online interaction. These youth-led actions amplify positive digital norms and demonstrate how gentle interventions can shift group culture toward empathy, trust, and mindful communication.

This case exemplifies the ambassador’s role: supporting youth-led initiatives, modelling emotionally intelligent communication, and making kindness visible online. Through simple, relatable tools like Kindly, young people experience security culture not as a rulebook, but as a shared commitment to treat one another with dignity in digital spaces.



Supporting Young People Through Emotional and Digital Challenges

To become trusted points of contact, youth workers need to recognise barriers that prevent youth from seeking help and learn practical ways to overcome them.

Understanding barriers and acting discreetly

- Fear of judgment or shame: Young people may hide online mistakes.
- Mistrust in adults: They may fear being punished instead of supported.
- Cultural or generational gaps: Different perceptions of what is “serious” online behaviour.
- Emotional overload: Youth may struggle to articulate how digital experiences affect them.
- Acknowledging vulnerability: Remind youth that anyone can be targeted online, and that their hesitation in reporting an incident is a sign of emotional strain, not weakness.

Ambassadors must counter these barriers through empathy, patience, and confidentiality. They should focus not on instructing young people to report but on removing the emotional and relational barriers that prevent them from seeking help safely. Through calm presence, empathy, and reassurance, youth workers build the trust needed for young people to open up, consider their options, and take steps that protect both themselves and their peers.

Tip: Use anonymous “question boxes” (physical or digital) so youth can submit online safety or emotional questions they might hesitate to ask directly.

Becoming a trusted support figure

Youth workers can build their credibility by:

- Showing genuine interest in youth's online lives.
- Being consistent and approachable.
- Keeping promises and respecting privacy.
- Avoiding overreaction: listen first, advise later.

Tip: Share short case studies of “what I did when...” to illustrate real problem-solving (e.g., dealing with hate comments). Stories show that seeking help is safe and normal.

Recognising and addressing digital threats

Ambassadors should be equipped to recognise early signs of:

- Cyberbullying or exclusion
- Online harassment or hate speech

- Misinformation or radical content exposure
- Emotional distress related to digital activity

Tip: Always focus first on the emotional response (“How did that make you feel?”) before the technical fix (“What can we report or block?”).

Tip: Partner with a local psychologist, NGO, or cyber unit to hold a co-session where youth learn both emotional and technical safety responses.

Emotional Intelligence in Digital Mediation

Security culture is built on emotional awareness. Conflicts, misinformation, or digital stress can only be addressed effectively if emotional intelligence (EI) is present.

The 4 EI domains in action

EI skill	Application for security culture
Self-awareness	Recognise emotions triggered by digital interactions.
Self-regulation	Avoid impulsive online reactions.
Empathy	Understand others’ feelings before judging or responding.
Social skills	Communicate assertively and build supportive relationships.

Tip: After any online group project, hold a short “emotion check-out” session where youth describe one emotion they experienced and one thing, they learned about themselves.

Mediation techniques for youth workers

- Use “pause and name”: help youth pause before replying online and name their emotion.
- Encourage perspective-taking: “What might the other person be feeling?”
- Teach assertive communication: express feelings and boundaries without aggression.
- Turn conflicts into learning opportunities by analysing causes and emotions involved.

Micro activity: Show a screenshot of an online argument and discuss how to rephrase emotional reactions using empathy and calm reasoning.

Tip: Introduce a “cool-off rule” in your group—before responding to a conflict message, everyone waits 10 minutes and reflects on their emotional state.



Practical Skills for Becoming an Ambassador

Youth workers can begin their ambassadorial journey through small, achievable actions that gradually build leadership and credibility.

Pathway	Action Examples	Expected Outcomes
Awareness Building	Deliver short info sessions on emotional safety online.	Youth become more aware of emotional risks.
Mentoring & Coaching	Offer one-to-one mentoring for youth facing online challenges.	Build trust and position youth worker as a safe contact.
Peer-Led Activities	Support young people to co-create workshops or campaigns.	Strengthens leadership and engagement.
Advocacy & Networks	Represent youth views in stakeholder dialogues.	Promotes systemic change for youth inclusion in security culture.
Reflection & Evaluation	Regularly assess impact of activities with youth feedback.	Ensures continuous improvement and responsiveness.

Tip: Document and celebrate youth-led actions (photos, testimonials, or mini case studies). Public recognition reinforces motivation and spreads positive digital behaviours.





Module 6 - Repository of Further Information and Resources

Resource Category	Resource Name	Type	Description	Link/Access Information
Cyber security	Better internet for kids (BIK)	website	The Digital Agenda for Europe aims to have every European digital. Children have particular needs and vulnerabilities on the internet; however, the internet also provides a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability.	https://better-internet-for-kids.europa.eu/en
Cybersecurity	European Union Agency for Cybersecurity (ENISA) – Publications	Website	Official EU resource providing practical cybersecurity awareness materials, campaigns, and guidance. Useful for youth workshops, threat recognition exercises, and preventive education aligned with European standards.	https://www.enisa.europa.eu/publications
Emotional intelligence	Six seconds emotional intelligence network	website	six seconds is a non-profit organization whose mission is to increase the world's emotional intelligence. six seconds researches	https://www.6seconds.org/



Resource Category	Resource Name	Type	Description	Link/Access Information
			and teaches emotional intelligence. we create evidence-based tools and methods to support transformational change in individuals and organizations	
Emotional Intelligence	CASEL – Social and Emotional Learning Framework	Website	Provides a widely used framework for Social-Emotional Learning, covering self-awareness, self-regulation, empathy, and responsible decision-making. Relevant for integrating EI into digital safety education.	https://casel.org
Youth support tools	Youthpass	Validation tool	Youthpass is a European recognition instrument for identifying and documenting learning outcomes that are acquired in projects under the Erasmus+ Youth and the European Solidarity Corps programmes. Youthpass promotes individual reflection and awareness about learning and helps to make learning outcomes visible for	https://www.youthpass.eu/en/



Resource Category	Resource Name	Type	Description	Link/Access Information
			the learners themselves as well as for others.	
Youth support tools	SALTO youth	Website	SALTO-YOUTH stands for Support, Advanced Learning and Training Opportunities for Youth. It works within the Erasmus+ Youth and the European Solidarity Corps programmes.	https://www.salto-youth.net/
Cybersecurity	EU vs Disinfo	Website	EU initiative explaining common disinformation techniques and manipulation strategies. Supports critical thinking, media literacy, and misinformation-related activities in youth education.	https://euvsdisinfo.eu
Cybersecurity	Stay Safe Online – Global Cyber Alliance	Website	Offers clear, accessible guidance on cyber hygiene and safe online habits. Can be adapted into youth-friendly checklists and preventive campaigns.	https://staysafeonline.org
Cybersecurity	DigComp 3.0: European Digital Competence Framework	Website	European framework outlining key digital competences, including safety and	https://joint-research-centre.ec.europa.eu



Resource Category	Resource Name	Type	Description	Link/Access Information
			information literacy. Useful as a reference for aligning training objectives with EU digital education policy.	a.eu/digcomp_en
Emotional Intelligence	Salovey, P., & Mayer, J. D. (1990). Emotional Intelligence	Article	Foundational academic article introducing the concept of emotional intelligence. Supports the theoretical grounding of EI-based approaches used throughout the EM&M manual.	https://doi.org/10.2190/DUGG-P24E-52WK-6CDG
Youth Support Tools	Council of Europe – Digital Citizenship Education	Website	Provides values-based resources for promoting ethical, safe, and participatory digital engagement among young people.	https://www.coe.int/en/web/education/dce-for-educators
Cybersecurity	Livingstone, S., & Third, A. (2017). <i>Children and young people's rights in the digital age. An emerging agenda</i> . New Media & Society, 19(5), 657–670.	Article	Strong basis for youth participation, voice, and advocacy in digital contexts.	https://doi.org/10.1177/1461444816686318



Resource Category	Resource Name	Type	Description	Link/Access Information
Cybersecurity	UNICEF- Cyberbullying: What It Is and How to Stop It	Website	Information about cyberbullying and how to handle it.	https://www.unicef.org/stories/how-to-stop-cyberbullying?utm
Youth Support Tools	European Commission: Digital Education Action Plan	Publication	Offers clear, accessible guidance on cyber hygiene and safe online habits. Can be adapted into youth-friendly checklists and preventive campaigns.	https://education.ec.europa.eu/focus-topics/digital-education/plan
Emotional Intelligence	Goleman, D. (1995). <i>Emotional Intelligence: Why It Can Matter More Than IQ</i> . New York: Bantam Books.	Book	Foundational theory underpinning self-awareness, self-regulation, empathy, and social skills used throughout the module.	https://books.google.gr/books?id=OgXxhmGiRB0C&printsec=frontcover&hl=en&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false https://www.youtube.com/watch?v=erfgEHHfK_U
Youth Support Tools	European Commission: Developing digital youth work. Policy recommendations, training needs and good	Publication	Provides examples of innovative practices in delivering digital youth work and upskilling youth workers' digital competences; Policy recommendations on the development of	https://op.europa.eu/en/publication-detail/-/publication/fbc18822-07cb-11e8-b8f5-01aa75ed71a1



Resource Category	Resource Name	Type	Description	Link/Access Information
	practice examples. For youth workers and decision-makers.		digital youth work; Identification of training needs of youth workers relevant for digital youth work.	
Youth Support Tools	UNICEF: Kindly	Website	A UNICEF initiative to end cyberbullying.	https://www.unicef.org/innovation/kindly
Cybersecurity Education	Better Internet for Kids (BIK)	EU Platform	EU-wide initiative offering resources on online safety, digital citizenship, and responsible internet use for children and young people. Useful for youth workers designing awareness sessions and parental/youth engagement activities.	https://www.beterinternetforkids.eu
Emotional Intelligence	MindTools – Emotional Intelligence Resources	Articles / Tools	Practical articles and tools for understanding and applying EI skills such as stress management, adaptability, and communication. Suitable for educator self-training and simplified youth activities.	https://www.mindtools.com
Youth Mental Health & EI	UNICEF – Mental Health & Psychosocial	Reports / Toolkits	Evidence-based guidance on youth mental health, emotional well-being, and psychosocial	https://www.unicef.org/mental-health



Resource Category	Resource Name	Type	Description	Link/Access Information
	Support Resources		support. Supports youth workers in addressing emotional responses to online risks and digital stress.	
Digital Literacy & Media	European Digital Media Observatory (EDMO)	EU Network / Resources	Provides tools and research on misinformation, factchecking, and media literacy. Useful for training youth to critically assess online information and manage emotional reactions to false content.	https://edmo.eu
Blended Learning	European Schoolnet Academy	Online Courses	Offers free professional development courses on digital pedagogy, blended learning, and innovative teaching methods. Youth workers can use courses for self-development and methodological inspiration.	https://www.europeanschoolnet.academy.eu
Blended Learning Tools	Kahoot!	Digital Tool	Gamified learning platform suitable for quizzes, knowledge checks, and interactive activities on cybersecurity and EI topics. Supports engagement and	https://kahoot.com



Resource Category	Resource Name	Type	Description	Link/Access Information
			motivation in blended learning settings.	
Blended Learning Tools	Canva for Education	Digital Tool	Visual design platform for creating posters, infographics, reflection boards, and storytelling activities. Supports creative EI reflection and cybersecurity awareness exercises.	https://www.canva.com/education
Youth Participation & Inclusion	SALTO Youth – Participation & Inclusion Resources	EU Resource Centre	Provides tools, methods, and publications supporting youth participation, inclusion, and non-formal education. Useful for adapting EM&M activities to diverse socio-economic and cultural contexts.	https://www.salto-youth.net
Romanian Context – Cybersecurity	Romanian National Cyber Security Directorate (DNSC)	Institutional Website	National authority providing cybersecurity alerts, awareness campaigns, and guidance adapted to the Romanian context. Can be used for locally relevant examples and preventive messaging.	https://www.dnsc.ro
Romanian Context – Youth Education	ANPCDEFP – Erasmus+ Youth Resources	Institutional Website	National Agency resources on Erasmus+ youth education, non-formal learning, and good practices. Useful for	https://www.anpcdefp.ro



Resource Category	Resource Name	Type	Description	Link/Access Information
			aligning EM&M activities with national youth work standards and projects.	

M

Activities

Activities Module 1

Below are several activities for Module 1. These are designed to solidify the fundamentals in an interactive way. They encourage discussion, reflection, and the use of emotional intelligence strategies in understanding cybersecurity basics. Each activity can be adapted to the group's age and context, and they emphasise different aspects of the module content (from vocabulary to practical routines). Note: Feel free to adjust scenarios to include various threats like fake profiles, phishing attempts, oversharing dilemmas, or cyberbullying incidents, ensuring all key topic areas (predators, scams, privacy, etc.) are touched across the activities.

Activity 1

Foundations Seminar – Building Shared Vocabulary and Connections

Activity Learning Objectives

- Understand and use core cybersecurity and emotional intelligence terms.
- Recognise how emotions affect online choices and risk-taking.
- Identify common digital situations where emotional awareness supports safer behaviour.

Activity overview:

This activity starts with a concise interactive lecture to introduce key terms, followed by a guided concept-mapping exercise. Educators will articulate how cybersecurity concepts (like threats and vulnerabilities) intersect with EI components (like awareness and regulation) in real-life digital moments. This helps build a mental model of how feelings and threats interconnect. It also surfaces participants' prior beliefs or misconceptions about online safety.

1. Instructions:

Mini-Lecture (5–7 minutes): Begin with a brief presentation or chalk-talk. Define the following clearly: threat, vulnerability, risk, hygiene (cybersecurity concepts) and self-awareness, self-management, social awareness, relationship skills (EI concepts). Use simple examples as given in the module content. For instance, draw a quick sketch or use an analogy (like “a vulnerability is like leaving your front door unlocked, it doesn't mean a bad guy is in your house, but it makes it easier for them to get in”). Keep it engaging – ask the group if they've heard these words or experienced situations that relate.

- ##### 2. List Daily Digital Moments:
- Invite participants to brainstorm five everyday digital moments that commonly trigger emotion for young

people. They can shout them out or write on sticky notes. Examples: an urgent notification pop-up, a public comment on their photo (could be praise or mean – either can trigger emotion), a friend request from someone they don't know, seeing a shocking news headline on social media, getting a "you won a prize" message. Try to include a variety: one that might cause anxiety (e.g. "account problem" message), one that causes excitement (prize or big news), one that causes curiosity or jealousy (a trending post or rumour), one that causes fear or anger (maybe a mean comment or cyberbullying incident). List these on the board.

3. **Concept Map Exercise:** Distribute the Concept Map Worksheet (Annex A) to each participant. Ask them to pick one of the digital moments from the list (whichever speaks to them or at random) and write that in the centre of the concept map. Then, individually or in pairs, have them fill in the surrounding nodes: identify a likely Threat in that scenario, the Vulnerability that could be at play, the Behaviour a typical youth might do, the Emotion they feel, a safer Response they should do instead, and a Verification Step to double-check. They should also draw arrows and add short notes explaining the connections (e.g., "Feeling anxious (emotion) can be a vulnerability because it might make me click the link (behaviour) without checking.>").
4. **Share and Discuss:** Collect 2–3 sample maps (either ask volunteers or pick randomly) and have the participants explain their scenario and connections. Discuss overlaps and common themes. For instance, you might notice that "rushing" appears as a vulnerability in many maps, or that "asking a friend" appears as a safe response often. Together, co-create a short, shared glossary on the board from what emerged – e.g., write "Risk = chance of harm (many mentioned this goes up when emotional)" or "Hygiene = daily safe habit (like several of you wrote 'update phone')". Ensure the formal definitions from the mini-lecture align with the participants' words.
5. **Summarise the EI–Cyber Link: End** with a summary tying it all together. Emphasise how emotional awareness leads to safer actions. For example, "So we saw in these maps that when someone felt angry or scared, they were more likely to do something risky like respond without thinking. But if they used self-awareness to notice that feeling and then self-management to pause and breathe, they could choose a safer response like verifying the info first. That's the cycle: awareness → reflection → regulation → safer action." Encourage questions to clarify any term or connection that participants still find fuzzy.



Reflection and discussion: Ask, “Which term or connection felt most clarifying today?” and “Where do you think your learners (youth) most need clearer language or concepts?” This allows educators to pinpoint which ideas they want to focus on in their own teaching. For instance, someone might say, “I realised we never talked about what a ‘vulnerability’ was with our students, so they blame themselves when something goes wrong. I want to use that word to show them it’s just something to fix, not a personal failing.” Another might say, “Understanding that emotions aren’t bad, they’re just signals – that was new to me, and I think my teens need to hear that too.”

Key takeaways:

- A shared language for cybersecurity and emotions removes confusion and stigma. When youth know the words, they can talk openly and ask for help (“I think I got phished” or “I felt pressured to share my pic and I regret it”).
- Emotions are signals, not directives. Feeling something doesn’t mean you must act on it immediately. Noticing and naming the emotion can actually help in making a safer digital choice (e.g., “I feel provoked by this comment, which is a sign I should not respond right now.”).

Activity 2

Case Vignettes & Dialogue – Emotions Behind Threats

Activity Learning Objectives

- Spot common online threats and emotional manipulation tactics.
- Recognise emotional triggers in online messages and posts.
- Practise using calm, clear language to respond safely under pressure.

Activity overview:

In this exercise, participants work with short, anonymised scenario cards (vignettes) that illustrate common online threats targeting youth. Each vignette is a brief message or post with minimal context. Educators will analyse these scenarios in pairs, identifying red flags and emotional triggers, and then brainstorm safe ways to respond. This is followed by a group discussion to normalise recognising manipulation and to share effective language for responding. The focus here is on reading between the lines of messages – what emotion is this trying to make you feel, and how can you respond with EI (staying calm and setting boundaries)?

Instructions:

1. **Distribute Case Vignette Sheets:** Provide each pair of participants with one Case Vignette. Each sheet contains a short scenario and prompts. For example:
 - a. "Support Contact: 'You've violated community rules. Click here to confirm your identity, or your account will be suspended today.'" (This one likely triggers urgency/fear.)
 - b. "Friend in a Hurry: 'Hey, it's me. I changed numbers. Can you send me your login code so I can get back in?'" (Triggers empathy/pressure to help – and could be an imposter or hacked friend scenario).
 - c. "Prize Drop: 'Congrats! You're the lucky winner of a new phone. Pay €2 shipping here to claim in the next hour.'" (Triggers excitement/greed/FOMO for a reward). (Optionally, you can create additional vignettes to cover other topics like a cyberbullying example: e.g. "Someone posted an embarrassing photo of you, comment here to respond," which triggers anger or shame; or a predator example: "Hi, I love your profile, you look mature for 14 – let's chat privately," which triggers flattery or curiosity. However, the three provided cover many core triggers.)
2. **Analyse in Pairs:** Ask pairs to read their assigned vignette. On the sheet, they should underline or note any red flags (suspicious elements) and circle words or phrases that provoke an emotional reaction. Then, they discuss what feeling likely arises (e.g., fear, urgency, sympathy, excitement). Next, have them draft a calm, two-sentence reply that the message deserves, as if they were a young person responding. This reply should be polite but firm and does not give away any personal info or click anything. For example, for the "Support Contact" scenario, a calm reply might be, "I will not click this link. I will check my account through the official app." Finally, they must suggest one verification step beyond the message – like "open the official site directly," "call my friend to confirm," or "ignore and report this message."
3. **Share Draft Responses:** Have each pair briefly share their scenario, what the trigger was, and their proposed safe response. After each share, offer feedback and then provide an exemplar response for that scenario (if they missed something). For instance, for the "Friend in a Hurry" case, after they share, you might highlight: "The red flag is them asking for your login code – that's private. The emotion trigger is you feel you need to help your friend quickly. A great response is: 'I don't share codes. Let me call you to sort this out.' And the verification is actually calling that friend (on their old number or another channel) to see if they really need

help.” Write down especially good phrases that participants come up with or supply a few useful “neutral response stems” (provided on the vignette sheet and below).

4. **Collect Common Triggers:** On a flipchart or whiteboard, make a quick list of triggers that appeared across the scenarios. You’ll likely see the ones from the content: urgency/fear, authority, empathy, reward, curiosity, etc. Next to each, have the group suggest a good neutral or assertive reply that fits. For example:
 - a. Urgency/Fear → Reply: “No rush – I will verify this through the official source.”
 - b. Empathy/Help → Reply: “I want to help, but I must verify this first through another way.”
 - c. Reward/Excitement → Reply: “Sounds great, but I don’t click on links. I’ll check the official website.”
 - d. Authority → Reply: “I don’t give out that information. I’ll contact support directly myself.”
 - e. Curiosity → Reply: “I’ll ask someone else about this. I don’t open unknown links.”

These become a collective set of “default safe replies” that educators can later teach their students.

5. **Reinforce EI → Safer Actions:** Summarise again how we just applied the EI–cyber link: **awareness** → **reflection** → **regulation** → **response**. For example, say: “In each case, first we noticed our feeling (awareness), then we reflected on why (this message is trying to make me feel X), we regulated by not reacting immediately (maybe taking a breath, thinking it through in pairs), and then we chose a response that was calm and safe. This is exactly what we want to teach youth – to read messages with their brains and their feelings in mind.”

Reflection and discussion: Pose the question, “What phrasing best balances politeness and safety when you need to slow down or say no online?” This gets participants to think about tone – how to be assertive without escalating conflict. Educators might share their go-to lines like “I don’t click links; I’ll check the app,” or “I’m not comfortable with that request.” Discuss why polite but firm language is effective (it defuses potential confrontation but still protects you). Also ask, “How did it feel to craft these replies, and how might a teen feel using them?” This can lead to insights, for example someone might say “It felt a bit awkward to write so formally to a friend – a teen might just ignore instead of reply, and that’s okay too. The key is they don’t comply.” Emphasise that ignoring or not responding is also a valid safe response in many cases.

Key takeaways:



- Many online threats rely on emotional urgency or manipulation rather than technical tricks. Simply recognising “this message is trying to make me feel panicked/excited” already gives you power to resist it.
- Having a few pre-planned neutral phrases or actions can help during high-pressure moments. Under stress, our minds can go blank; if youth have practiced responses like “Let me check and get back to you” or even just exiting the app to think, they are more likely to act calmly under pressure.
- Practicing in advance (through scenarios like these) builds confidence. It’s like a fire drill for online threats – when it really happens, you won’t be paralysed; you’ll remember you handled something similar before.

Activity 3

Think-Aloud Modelling – Slowing Down Emotional Messages

Activity Learning Objectives

- Watch and understand how to pause and respond safely to emotional online messages.
- Learn words and actions that help reduce stress and avoid risky choices.
- Practise your own step-by-step response using the think-aloud method.

Activity overview:

This activity demonstrates how an educator can model the desired decision-making process for students by thinking out loud. Participants will watch as the facilitator goes through two example messages, talking through each step (naming the feeling, pausing, verifying, responding). Then participants will craft and practice their own 60-second think-aloud for a scenario of their choice. This trains educators to be explicit in teaching the mental steps, not just the outcomes, which is critical for youth to learn how to do it themselves. Essentially, you’re showing “what’s going on in my head” as I handle a tricky message, so students can learn by example.

Instructions:

1. **Present Two Example Messages:** Prepare two short message scenarios that illustrate different emotional triggers. For instance:
 - a. Message A (Urgency): “URGENT: Your account will be locked in 5 minutes! Verify now: [link]” – using urgency/fear.
 - b. Message B (Empathy/Scam): “Hey, I’m an admin from the school group. I saw someone posted mean things about you. I can help get it removed, I just need your login info.” – using a mix of authority (admin) and empathy (offers help) or use something like

an empathy ploy: “I’m really worried about you, please click this safety form now so we know you’re OK.”. (You can adjust these examples to include other triggers like a predator scenario: “Hey cutie, I noticed you’re only 15, I’m 17, we should chat privately” – flattery trigger; but ensure appropriateness for the audience. For modelling, we usually stick to the common ones like phishing and impersonation.)

2. **Facilitator Think-Aloud Demonstration:** For each message, “perform” a think-aloud in front of the group. Exaggerate the clarity of steps since this is a demo. For example, take Message A and say out loud as if narrating your internal dialogue:
 - a. “Okay, I just got this message and my heart skipped – I notice I’m feeling really anxious and rushed. That’s a cue for me to slow down.” (You labelled the feeling and the trigger – urgency.)
 - b. “This message is using urgency to scare me. They want me to panic. So I’m going to take one deep breath first.” (You pause and manage the emotion – maybe actually do a quick inhale-exhale visibly.)
 - c. “Now, what are they asking for? They want me to click a link and give info. Big red flag – probably a phishing threat. Instead of clicking, I’ll do a verification step: I’ll go open my account through the official app to see if there’s really an issue.” (You identified the needed response.)
 - d. “So, I’m not clicking this. If it were real, I’d see a notification in the app, or I could ask our tech teacher. I’ll also let my friends know this message is going around – better to warn others.” (You conclude the response, maybe also mention a relationship skill like sharing knowledge or seeking help.)
 - e. “I’m glad I slowed down. Remember: Slowing down helps me stay safe.” (A bit of reinforcing self-talk to conclude.)

Do a similar think-aloud for Message B, demonstrating how you identify perhaps the sympathy ploy, but also notice something off (like the admin asking for login info – an authority misuse). Speak in a calm, steady voice, and maybe even model calm language you’d reply with (e.g., “I wouldn’t give my info; I’d say: ‘Thanks, but I don’t share passwords. I’ll talk to the teacher about the posts.’”). By doing two somewhat different examples, participants see the versatility of the method.

3. **Provide Think-Aloud Template:** Hand out the Think-Aloud Script Template to everyone. This template provides prompts to fill in: Feeling label, Trigger spotted, Pause, Risk question, Verification step, Reply sentence, Decision, Self-talk. Go over the template quickly to ensure they

understand each part. Emphasise that their whole script should be about 60 seconds when spoken – so concise wording is key.

4. **Participants write their own script:** Now, ask each participant to think of a message scenario they might face or worry about (or pick from ones provided, possibly the ones not used in step 1 or others relevant, e.g., a fake news share from a family group that makes them angry, or a cyberbullying comment directed at them). They should write a brief scenario description at the top (“Message type: e.g. suspicious link on Discord” or “Message type: mean comment on my post”) and then fill in the template for that scenario. Encourage them to actually imagine the emotions: “If you got that comment, how would you feel? Name it... What’s the trick or trigger? Acknowledge it... What will you do to pause? Note it... How will you verify or who will you consult? ...” and so on.
5. **Pair practice:** Once scripts are drafted, have participants split into pairs and practice delivering their think-aloud orally. One person performs their ~60-second think-aloud while the other listens. The listener can give a thumbs-up for things done well and one suggestion if something was unclear or if the flow could improve. Then they switch.
6. **Group share (optional):** Invite 1–2 volunteers (if time allows and people are willing) to perform their think-aloud in front of the whole group. After each, highlight effective phrasing or steps they used. For example, maybe one volunteer said, “I notice I’m feeling curious, which tells me I need to be careful” – you might point out, “Great, she caught the curiosity trigger and used it as a signal to be cautious, not as a reason to click.” Also, gently correct or refine anything if needed (ensure the response was actually safe, etc., though usually by this point they should be on target). Write down any especially memorable phrases or techniques on a flipchart to reinforce them (e.g., “Real support never asks for passwords” or “Breathe first, then deal with it”).

Reflection and discussion: Ask the group, “Which phrases or approach best slowed down the moment without escalating the situation or embarrassing anyone?” In essence, what language kept things calm? For example, participants might mention, “I like how one script said, ‘I’ll check through official channels’ – it’s neutral and not confrontational.” Another might say, “Using a bit of self-talk like ‘I’ve got this, stay calm’ seemed helpful.” Discuss how tone matters: a calm, confident tone can defuse a scammer or bully, whereas an angry or fearful tone might encourage them or make a youth more upset. Also discuss how narrating the process (to students) provides a blueprint they can remember. For instance, “Hearing someone go ‘Okay I feel X, so I will do Y’ is



powerful – it shows step by step. Kids often only see the result (like not clicking), but not the thinking. This makes the invisible thinking visible.”

Key takeaways:

- Modelling out loud is a powerful teaching tool. When educators demonstrate exactly how to handle a tricky online situation, including the emotional aspects, students learn not just what to do, but how to arrive at that decision.
- A calm tone and concrete steps are more memorable to youth than abstract warnings. Instead of just saying “Don’t click strange links” (easy to say, hard to follow when emotional), modelling shows how one actually resists the urge: by noticing feelings and self-talking through them.
- Narration creates a mental script for learners. Later, a student might literally recall the teacher’s voice saying, “I feel scared, but I’m going to breathe and not click,” and emulate that. It’s like giving them an internal coach to guide them in the moment of truth.

Activity 4

Misconception Challenge – True, False, or Depends?

Activity Learning Objectives

- Discover and correct common myths about cybersecurity and emotions.
- Practise giving and receiving simple explanations to understand risks better.
- Build confidence in your knowledge and safe online behaviours.

Activity overview:

Misconceptions can undermine learning – for example, a teen might believe “Only old people get scammed” or “If I use a strong password, I’m 100% safe.” This activity is a gamified discussion where participants are given a set of short statements about cybersecurity and EI. They must classify each as True, False, or Depends (contextual) and then provide a one-sentence correction or clarification. Working in groups, they’ll debate these points, then share and refine the best explanations. The twist is to do it in a kind, non-judgmental way suitable for youth. This means avoiding saying “That’s wrong,” and instead gently steering toward the truth (e.g., “Actually, scammers target young people a lot by offering free stuff...”). By the end, the group will have a collection of “corrective statements” they can use in teaching.

Instructions:

1. **Misconception Cards:** Prepare a set of ~10 statements that reflect common myths or misunderstandings (Annex E provides examples). Distribute the list as a handout or display them one by one. Example statements include:
 - a. "If my password is strong, I don't need 2FA."
 - b. "If a message comes from a friend's account, it's safe."
 - c. "Only older adults fall for scams."
 - d. "If I feel anxious, I should ignore my feelings and just act quickly."
 - e. "Official support might ask for my password to help me."
 - f. "If it's urgent, I should click first and think later."
 - g. "Using public Wi-Fi is always safe if the site is HTTPS."
 - h. "Privacy settings don't matter if I'm not famous."
 - i. "If a prize has a tiny 'shipping fee,' it's probably legit."
 - j. "Emotions make you weak online."
2. **Ensure that among these are items covering the topics we want:** password/2FA (technical), friend's account safe (imposter risk), age and scams (everyone is a target), ignoring feelings (wrong approach to EI), support asking for info (scam), urgency (red flag), public Wi-Fi (partial truth), privacy (everyone needs it), small fee scam (common scam tactic), emotions (actually can be strengths if managed). You can tweak wording to suit your audience.
3. **Group Classification:** Split participants into small groups (3-5 per group). Their task: For each statement, decide if it's True, False, or "Depends" (meaning it has nuances). Then – most importantly – come up with a one-sentence clarification that they would tell a young person to explain the reality. The clarification should be kind and constructive. For example, for "Only older adults fall for scams," they'd mark False and might write, "Scams target everyone – scammers often create special tricks for young people too." For "Using public Wi-Fi is always safe if HTTPS," they might mark Depends and clarify, "HTTPS is good but public Wi-Fi can still be risky; avoid sensitive transactions on public networks." Encourage them to use analogies or simple terms (like "second lock" for 2FA). Give them about 10-15 minutes to discuss all items.
4. **Share and Compare:** Go through each statement one by one as a full group. Ask one group what they decided and their reasoning/explanation. Then ask if other groups had a different classification or phrased their clarification differently. Where groups differ (e.g., some said "Depends" vs "False"), discuss the nuance – this is a great learning opportunity. Aim to reach a consensus on each with

the correct answer and a polished, youth-friendly explanation. As facilitator, contribute and confirm the accurate info. For instance:

- a. "If my password is strong, I don't need 2FA." – Most should say False. Explanation: "Strong passwords help, but 2FA adds a second lock that makes you much safer."
- b. "If a message comes from a friend's account, it's safe." – False. Explanation: "Accounts can be hacked or impersonated; if something seems odd, verify through another channel."
- c. "Only older adults fall for scams." – False. Explanation: "Scams target everyone; there are scams specially designed for young people (like gaming or prize scams)." Perhaps add a statistic or anecdote if you have one (to bust the "I'm too smart/young to be scammed" myth).
- d. "If I feel anxious, I should ignore my feelings and just act." – False. Explanation: "Feelings are signals. If you feel anxious, that's exactly when you should slow down and check – not ignore it."
- e. "Official support might ask for my password to help me." – False. Explanation: "Real support staff never ask for passwords or private codes."
- f. "If it's urgent, I should click first and think later." – False. (Maybe someone says "Depends" as a joke, but make it clear this is a dangerous myth.) Explanation: "Urgent messages are often red flags for scams; always take a moment to think and verify – nothing is so urgent that you can't take 10 seconds."
- g. "Using public Wi-Fi is always safe if the site is HTTPS." – likely Depends. Explanation: "HTTPS is good encryption, but on public Wi-Fi you could still be vulnerable (like connecting to a fake hotspot); better to avoid sensitive logins on public Wi-Fi or use a VPN." Keep the explanation simple and not too technical.
- h. "Privacy settings don't matter if I'm not famous." – False. Explanation: "Privacy settings help everyone. They limit who sees your info – this can prevent strangers or even future schools/jobs from seeing things you don't want public."
- i. "If a prize has a tiny 'shipping fee,' it's probably legit." – False. Explanation: "Fees and countdown timers are classic scam tactics; a legit prize won't ask you to pay upfront."
- j. "Emotions make you weak online." – False. (Or one might say "Depends" if they interpret it oddly, but steer to False.) Explanation: "Emotions can actually make you stronger online if you're aware of them. Being emotionally intelligent – knowing when you're upset or excited – helps you control your actions. It's

not weak, it's smart."

As each is discussed, write the correct verdict (T/F/Depends) and the refined clarification sentence on the board or a shared document. By the end, you have a nice list of myth-busters.

5. **Build Corrective Stems:** Point out patterns in the explanations. Many follow a structure: acknowledge the kernel of truth or the concern, then correct it. For example, "Strong passwords help, but 2FA adds a second lock." or "Scams target everyone; tactics are adapted for youth too." This structure ("yes..., but..." or stating the truth succinctly) is a great way to correct without shaming. Highlight a few useful stems participants can reuse:

- a. "X helps, but Y is also needed..." (for layered security misconceptions).
- b. "Real [authority] never [does the suspicious action] ..." (for scams – e.g., real banks never ask you to send passwords).
- c. "It might seem like... but actually..." (general refutation format).
- d. "Everyone is at risk because..."
- e. "Feeling X is a signal to do Y, not a reason to panic."
- f. "If it sounds too good to be true, it likely is."

These stems can become part of their teaching vocabulary.

Reflection and discussion: Which misconception surprised you or which do you think shows up most in your setting?" and "What's a short explanation that you find works best with your learners to correct that?" Educators might reflect that they themselves believed one of the myths before ("I used to think strong passwords were enough, but now I see how important 2FA is – I'll definitely stress that.") or identify which myths their students often repeat ("My teens always think only dumb people get scammed. I will use that 'scams target everyone' line next time I hear it."). Discuss how presenting corrections in a non-judgmental way is key to maintaining trust – we never want to make a student feel bad for holding a misconception; we want them to feel empowered with the correct knowledge.

Key takeaways:

- Clarity plus kindness reduces resistance. When correcting false beliefs, doing so with empathy and simple logic (rather than just "No, that's wrong") makes youth more open to changing their thinking.
- Having a stash of short, corrective explanations or analogies makes teaching easier. You can quickly dispel myths on the fly. (E.g., "Think of 2FA like a second lock on your door – one lock can be picked, two locks are way harder.")



This exercise often reveals that even educators can hold some outdated or false beliefs. Continuous learning is part of cybersecurity – things change, and staying updated (like knowing new scam tactics or platform features) is important.

Activities Module 2

Activity 1: Cyber Emotions Map

Threats addressed: phishing, cyberbullying, misinformation, impersonation

Objective: Help youth recognise how online threats trigger emotions and influence decision-making.

Format: Blended (discussion + online board)

Steps:

1. Present short case studies involving different online threats.
2. Youth identify emotions these threats evoke.
3. Build a collaborative "Cyber Emotions Map".
4. Discuss EI-based coping strategies.

Activity 2: Digital Escape Room – Cyber Threat Edition

Threats addressed: scams, phishing, fake profiles, malware

Objective: Train youth to identify online threats under time pressure.

Format: Online or hybrid

Steps:

1. Teams solve cybersecurity challenges.
2. Include EI prompts about pressure and stress.
3. Reflect on emotions and decisions.

Activity 3: EI & Cybersecurity Role-Play

Threats addressed: cyberbullying, impersonation, predators, misinformation

Objective: Strengthen empathy and communication in online conflict scenarios.

Format: In-person with optional online follow-up

Activity 4: Cyber Hygiene Checklist Challenge

Threats addressed: malware, phishing, oversharing

Objective: Promote daily preventive digital behaviours.

Format: Online + offline

Activity 5: Stress Under the Screen – Coping Workshop

Threats addressed: impulsive reactions to phishing, scams, cyberbullying

Objective: Teach EI-based stress management techniques.

Format: Offline or hybrid



Activity 6: Cyber Ambassador Peer Circle

Threats addressed: all eight key online threats

Objective: Build ongoing peer-support systems.

Format: Blended

Activity 7: Storytelling with Emotions & Security

Threats addressed: oversharing, cyberbullying, scams, misinformation

Objective: Connect personal digital stories with EI and cybersecurity lessons.

Format: Blended

Activity 8: Quickfire Quiz & Reflection

Threats addressed: all key threats

Objective: Reinforce knowledge through gamification.

Format: Online quiz

Activities Module 3

Activity 1: Digital Empathy Mirror

Focus: Cyberbullying and Hostile Digital Communication

Overview: This activity is designed to help participants develop emotional intelligence (EI) by recognizing how digital communication lacks nonverbal cues, which can lead to misunderstandings, conflicts, and cyberbullying. By comparing online and face-to-face interactions, participants explore how empathy, self-awareness, and emotional regulation can mitigate the risks of hostile or exclusionary digital behaviour.

Learning Objectives:

- **Recognize emotional cues** (or lack thereof) in **digital communication** (e.g., tone, word choice, emojis).
- **Understand the emotional impact** of **miscommunication** in online environments, particularly in **cyberbullying or hostile exchanges**.
- **Practise empathy** as a **protective skill** to **de-escalate digital conflicts** and **foster respectful online communities**.
- **Apply self-awareness** to **personal digital communication**, ensuring messages are **clear, kind, and intentional**.

Duration: 50 minutes (25 min online, 25 min in-person)

Group Size: 8–20 participants

Materials/Tools:

- **Anonymized chat transcripts** (3–4 examples of **cyberbullying, exclusionary language, or misunderstandings**).

- **Padlet board** for collaborative reflection.
- **Emotion cards** (e.g., anger, sadness, confusion, fear, excitement).
- **Projector or shared screen** for group discussions.
- **Printed worksheets** (for In-Person lectures).

Instructions:

1. Connect (Online):

- **Introduction:** Begin with a **short video (3–5 min)** explaining how **lack of tone and body language** in digital communication can lead to **misunderstandings and cyberbullying**.
- **Discussion Prompt:** “Have you ever sent or received a message that was misunderstood? How did it make you feel?”
- Share **3–4 anonymized chat examples** (e.g., a **hostile group chat, exclusionary language, or a sarcastic remark taken seriously**).
- Ask: “What emotions might the sender and receiver be feeling? What cues are missing in this digital exchange?”

2. Explore (In-Person):

- **Pair Work:** In pairs, participants **analyze one chat example** and discuss:
 - “What emotions are present in this exchange?”
 - “How might this conversation have gone differently face-to-face?”
- **Role-Play:** Pairs **re-enact the chat in person**, paying attention to **tone, facial expressions, and body language**.
- **Group Discussion:** “How did the meaning change when you saw and heard the person? What nonverbal cues were missing in the original chat?”

3. Practice (Blended):

- **Rewriting the Chat:** Groups **rewrite the chat** to make it **more empathetic and clearer**.
 - Example: If the original chat was **hostile**, how could it be rephrased to **show understanding and respect**?
- **Digital Reflection:** Post the **rewritten chat on Padlet** with a note: “How did empathy change the interaction? What emotions did you consider?”
- **Low-Tech Option:** Participants with limited digital access can **write their responses on worksheets** and share them in the next in-person session.

4. Reflect (Online):



- **Journal Prompt:** “What signals are often missing in online communication? How can empathy prevent misunderstandings or cyberbullying?”
- **Mentimeter Poll:** “On a scale of 1–5, how confident do you feel in recognizing and responding to cyberbullying after this activity?”
- 5. **Share (In-Person):**
 - **Group Presentations:** Each group presents their **rewritten chat** and explains their **emotional and linguistic choices**.
 - **Takeaway Discussion:** “What’s one change you’ll make in your digital communication to ensure it’s empathetic and clear?”

Reflection Questions:

- What **emotional cues** are hardest to convey digitally?
- How can **empathy** help resolve **online conflicts**?
- What’s one change you’ll make in your **digital communication** after this activity?

Key Takeaways: Empathy and **active emotional interpretation** are key to building safer, more respectful digital communities.

Activity 2: Cyber Scenario Lab

Focus: Phishing, Scams, and Impersonation

Overview: Participants collaborate to analyse and act out cyber-risk scenarios (e.g., phishing emails, impersonation attempts, FOMO scams). They map the emotions of everyone involved and co-create prevention strategies using EI techniques.

Learning Objectives:

- Recognise **emotional triggers** in **phishing and scams**.
- Practise **self-regulation** to avoid impulsive responses.
- Develop **peer-support strategies** for responding to **impersonation or scams**.

Duration: 90 minutes (60 min in-person, 30 min online follow-up)

Group Size: 10–25 participants

Materials/Tools:

- **Case cards** (scenarios: phishing email, fake friend request, FOMO scam).
- **Flipchart or digital whiteboard** (Miro/Jamboard).
- **Canva** for creating **storyboards or prevention posters**.

- **Moodle/Teams forum** for follow-up reflections.

Instructions:

1. **Connect (In-Person):**
 - Divide into teams of 4–5. Assign each team a **cyber-risk scenario** (e.g., phishing, impersonation, scam).
 - Ask: *“What emotions might the victim, observer, and offender feel in this situation?”*
2. **Explore (In-Person):**
 - Teams **map the emotions** of each person in the scenario.
 - Discuss: *“What makes this situation risky? How could EI help?”*
3. **Practice (In-Person):**
 - Teams create a **3-minute skit or storyboard** showing the **problem and a prevention strategy**.
 - Focus on **EI techniques**: self-regulation, perspective-taking, peer support.
4. **Reflect (Online):**
 - Post on **Moodle/Teams**: *“What emotions drove the behaviour in your scenario? How can EI prevent harm?”*
5. **Share (In-Person + Online):**
 - Teams present their **skits/storyboards**.
 - Follow-up: Upload **prevention tips** to a shared **youth center network**.

Reflection Questions:

- What **emotions** make people vulnerable to **scams or phishing**?
- How can **self-regulation** help someone **avoid impulsive clicks**?
- What’s one **EI strategy** you’ll use to **protect yourself online**?

Key Takeaways: Recognising the **emotional dimension** of cyber risks empowers youth to **respond constructively, not reactively**.

Activity 3: Inclusive Session Designer

Focus: Privacy Risks, Misinformation, and Malware

Overview: This design lab enables educators to **create a 30-minute blended session** that is **emotionally intelligent, inclusive, and adaptable** to diverse youth profiles. The session must address **privacy risks, misinformation, or malware** using **Universal Design for Learning (UDL)** principles.

Learning Objectives:

- Apply **UDL** to design **inclusive sessions** on **online risks**.



- Integrate **emotional and digital competences** into a cohesive lesson.
- Reflect on **accessibility, participation, and learner wellbeing**.

Duration: 90 minutes

Group Size: 6–20 educators

Materials/Tools:

- **Annex A: Inclusive Session Plan Template** (provided by PRAMMER).
- Laptop/tablet.
- Collaborative space (**Miro** or **Google Docs**).

Instructions:

1. **Connect (In-Person):**
 - Present **2–3 youth profiles** (e.g., rural youth with limited digital access; neurodivergent learner; migrant youth with language barriers).
 - Ask: *“What unique challenges might these youth face with **privacy risks, misinformation, or malware**?”*
2. **Explore (In-Person):**
 - Teams select **one risk area** (privacy, misinformation, or malware) and **one youth profile**.
 - Fill out the **session plan template**, detailing:
 - **Objectives** (e.g., “Teach how to verify sources to combat misinformation”).
 - **Blended phases** (Connect–Explore–Practice–Reflect–Share).
 - **Tools** (e.g., Padlet for privacy discussions, Kahoot for malware quizzes).
 - **Emotional prompts** (e.g., “How would you feel if your private data was leaked?”).
 - **Accessibility actions** (e.g., subtitles for videos, printed materials).
3. **Practice (Blended):**
 - Teams **present their session plans** to peers.
 - Peers provide feedback using **Annex B: UDL & Accessibility Checklist**.
4. **Reflect (Online):**
 - Journal prompt: *“How does your design meet the **emotional and digital needs** of your chosen youth profile? What adaptations were most effective?”*
5. **Share (In-Person):**

- Discuss: “How can we ensure all youth, regardless of background, feel **safe and empowered** to learn about these risks?”

Reflection Questions:

- How did your design address **privacy, misinformation, or malware** for **diverse learners**?
- Which **inclusive adaptations** (e.g., low-tech options, multilingual resources) were most impactful?
- How will you **evaluate emotional engagement** in your session?

Key Takeaways: Designing **inclusively from the start** guarantees **accessibility and psychological safety** for every participant.

Activity 4: Gamify Emotions Online

Focus: Scams (FOMO-Based), Fake News, and Phishing

Overview: This activity uses **gamification** to reinforce **emotional-digital literacy** while increasing engagement and motivation. Participants play a **quiz game** that connects **emotional triggers** to **online risks**, then reflect on how emotions influence digital decisions.

Learning Objectives:

- Review **EI and cybersecurity principles** related to **scams, fake news, and phishing**.
- Experience how **playful competition** supports **retention and motivation**.
- Reflect on how **emotions** (e.g., fear, curiosity, urgency) influence **online decision-making**.

Duration: 35 minutes (online)

Group Size: Up to 30 participants

Materials/Tools:

- **Kahoot/Quizizz** platform.
- Projector (optional).
- Follow-up discussion space (**Mentimeter** or **Padlet**).

Instructions:

1. Connect (Online):

- Introduce the game: “Today, we’ll test your knowledge of **emotional triggers in scams, fake news, and phishing!**”

2. Explore (Online):

- Launch a **Kahoot/Quizizz quiz** with questions like:

- “What emotion might cause someone to click a **phishing link**?” (Options: Fear, curiosity, urgency).
 - “Why do **FOMO scams** work so well?” (Options: They create excitement, pressure, or exclusivity).
 - “How can you verify if a news story is **fake**?” (Options: Check the source, look for biases, reverse image search).
3. **Practice (Online):**
- After each question, **highlight the emotional trigger** behind the correct answer.
 - Example: “Fear of missing out (FOMO) can make us act impulsively—like clicking a **scam link**!”
4. **Reflect (Online):**
- Post-game prompt on **Mentimeter/Padlet**: “Which emotions led to **risky answers** in the game? How can understanding emotions improve your **online decisions**?”
5. **Share (Online):**
- Ask participants to **share one change** they’ll make to feel **safer and calmer online** (e.g., “I’ll pause before clicking links”).

Reflection Questions:

- Which **emotions** made you most vulnerable to **scams or fake news** in the game?
- How can **gamification** help normalize discussions about **feelings and online safety**?
- How might you use **games** in your own blended practice to teach about **phishing or misinformation**?

Key Takeaways: Playful methods increase **emotional engagement** and help **normalize discussions** about **feelings and safety online**.

Activity 5: Reflective E-Journal

Focus: All Eight Online Risk Areas

Overview: A **structured reflection practice** that continues between sessions, encouraging **self-awareness and long-term behaviour change** in youth and educators. Participants journal weekly about their **emotional experiences** related to the **eight online risks**.

Learning Objectives:

- Develop **regular self-reflection habits**.
- Connect **emotional experiences** with **online behaviours**.
- Monitor **personal progress** toward **empathetic, safe digital conduct**.



Duration: 4–6 weeks (asynchronous)

Group Size: Individual activity

Materials/Tools:

- **Padlet** or **Google Docs** shared folder.
- **Annex C: Weekly Reflection Prompts** (provided by PRAMMER).

Instructions:

1. Connect (Online):

- Introduce the journal: *"This is your space to reflect on **emotions and online risks**—no judgment, just growth!"*

2. Explore (Asynchronous):

- Each week, participants answer **1–2 prompts**, such as:
 - *"What **digital situation** this week made you feel **proud, anxious, or angry**? (e.g., a **scam attempt, fake news, or cyberbullying**.)"*
 - *"How did you respond to a **phishing email or impersonation attempt**? What would you do differently?"*
 - *"Describe a time you **verified information** before sharing it. How did it feel?"*

3. Practice (Asynchronous):

- Facilitators **review entries weekly** and offer **empathic feedback** (e.g., *"I notice you felt frustrated by that **FOMO scam**—how could self-regulation help next time?"*).

4. Reflect (In-Person/Online):

- Final group session: *"What's one **insight** from your journal that changed your **online habits**?"*

5. Share (In-Person):

- Participants **share commitments** (e.g., *"I'll fact-check before sharing news"*) and celebrate progress.

Reflection Questions:

- How has **awareness of your emotions** changed your **online habits**?
- Which **EI strategies** (e.g., empathy, self-regulation) were most useful for **scams, cyberbullying, or privacy risks**?
- How can **journaling** support **ongoing learning** about **digital safety**?

Key Takeaways: Reflection transforms learning into habit—consistent journaling builds **digital-emotional resilience**.



Activities Module 4

Below are activities for Module 4 that educators can use to achieve the learning objectives. These exercises are highly interactive and scenario-based, giving youth a chance to practice threat recognition and safe responses in a controlled environment. They cover a range of methods (quizzes, role-play, discussions, etc.) and can be mixed and matched depending on time and resources. Importantly, each activity integrates emotional intelligence elements – helping youth not just to identify technical red flags, but also to manage their reactions. All activities can be adapted for online or offline settings.

Activity 1: Spot the Risk – Interactive Quiz

Objective: Train participants to identify threat cues in everyday digital situations and connect each cue with a safe response or action. Also, reveal how emotional reactions can affect judgment.

Format: Online (Kahoot/Quizizz, screen share) or Offline (projected or printed quiz; tally by hand).

Duration: 20-30 min.

Instructions:

1. **Prepare quiz items:** Create about 15 short question items. Ideally use visuals: screenshots or mock-ups of things like an email, a text message, a social media post, a login screen, etc. Each should depict a scenario that is either Safe or Risky. Examples:
 - A screenshot of an email that says “Your package delivery failed, click here to reschedule” from an odd address.
 - A WhatsApp message from an unknown number claiming to be a friend needing money.
 - A social media post with a sensational headline (could tie in misinformation).
 - A friend’s profile that has suddenly only 2 pics and was just made yesterday (hinting it’s a fake profile).
 - A pop-up ad that says “Virus detected! Tap to install cleaner” on a phone.
 - An Instagram DM that says “Check out this funny video of you! [link]”.
 - Also include a few genuinely safe examples to not make it too obvious (maybe a legitimate email from a known company with no red flags, or a normal friend message).
 - For each, pose a question like “Safe or Risky?” or “What would you do?” with multiple choice options.



- Additionally, include about 3 special questions that ask about feelings: e.g., after a particularly scary item, a question like “How did this message make you feel initially? A) Not concerned, B) A bit anxious, C) Very scared, D) Excited” – this prompts reflection on emotion.
- 2. **Quiz execution:** If online, launch the quiz on the chosen platform and have participants join via their devices. If offline, you can project each image and ask people to raise coloured cards or write answers. If neither is possible, even describing the scenario and having people vote by show of hands or moving to corners of the room (one corner = “Safe”, another = “Risky”) works.
- 3. **Participants decide and justify:** For each item, participants select their answer (or physically move to an answer zone). Encourage them to also think why they chose safe or risky. For instance, if someone sees the email example and chooses “Risky”, it might be because they spotted a spelling error or thought “I wasn’t expecting a package, this seems phishy.”
- 4. **Reveal answers with explanation:** After each question, reveal the correct answer (if it was indeed a phishing email, etc.) and provide a short explanation of the red flags or lack thereof. Importantly, also state “What to do next time” as a tip. Example:
 - For the fake delivery email: Correct answer: Risky. Why: Sender address is weird (not the official company), it creates urgency. What to do: Do not click the link; go to the official site or your order app to check shipments.
 - For the WhatsApp money request: Risky. Likely a scam or hacked friend. Tip: Verify by calling your friend or asking a question only they would know. Don’t send money without confirming.
 - For the sensational headline post: Likely Risky (could be misinformation). It made many feel anxious (as per their emotional response answers). Tip: Check if the source is credible; see if trusted news outlets have the story before sharing or acting.
 - For the pop-up ad: Risky. It’s scareware trying to lure a download. Tip: Don’t click pop-ups. Use your phone’s built-in security or a trusted app from the app store if you think there’s an issue.
 - For a safe example (say a genuine two-factor login screen from a site you requested): Safe. Why: It’s occurring when expected, and not via a random link; it has proper branding, etc. Still, always good to double-check the URL.

5. **Emphasize any emotional component:** e.g., “Notice how the scam tried to make you feel pressure or fear – several of you said you felt anxious. That’s the clue. Use that anxiety as a reminder to slow down.”
6. **Tally and gamify:** If using Kahoot or similar, the platform will keep score and show a leaderboard. If offline, you can keep score manually or just make it a friendly competition by applause. Acknowledge the winner(s) at the end. This isn’t about high stakes, just a bit of motivation.
7. **Reflection debrief:** After the quiz, ask, “Which types of items were hardest to identify? Which were easiest?” and “Which emotions most often led to mistakes?” For example, participants might say, “The one where I got excited about the prize was where I almost clicked – my excitement made me ignore the sketchy link.” Discuss how pause and check can mitigate that. Highlight if any participant insights came: “One of you mentioned you felt scared on that fake alert – that fear is exactly why we have to pause.” Connect it back to Awareness → Reflection → Regulation: the quiz was a practice in quick awareness; in real life, we add the reflection/regulation steps.

Tools Needed: If online – a quiz platform (Kahoot, Quizizz, Mentimeter quiz mode) and participant devices. If offline – printed screenshots or slides, and a way for participants to indicate answers (cards, papers, moving around).

Adaptation: For very low tech, you can even do a “Verbal Quiz”: describe a scenario and have people call out “Safe!” or “Risky!” and then discuss. Or turn it into a human continuum (line up from safe to risky rating). The key is interaction and immediate feedback.

Activity 2: Behind the Click – Emotion Triggers

Objective: Help participants recognise manipulation triggers in messages and practice crafting calm, assertive responses to each type of trigger. This builds a mental library of default replies to use under pressure.

Format: Could be done online using a collaborative board (Padlet or Canva) where triggers and examples are matched, or offline with printed Trigger Cards and scenario strips that groups work with on paper or a wall. Involves breakout group discussions and a collective creation of “safe response” scripts.

Duration: 30-40 min.

Instructions:

1. **Trigger Cards distribution:** There are six classic triggers we want to cover (mirroring what was discussed in Module 1 content): urgency, fear, empathy, opportunity/reward, authority, curiosity (and you might include a seventh, like social proof/FOMO, if desired, or integrate it with

curiosity/reward). Give each small group (3-4 people) one Trigger Card. For example:

- Group 1 gets Urgency (message threatening quick consequence).
- Group 2 gets Fear (scary security alert type message).
- Group 3 gets Empathy (sob story request).
- Group 4 gets Authority (someone pretending to be in charge).
- Group 5 gets Opportunity/Reward (you won something or get something exclusive).
- Group 6 gets Curiosity (tempting you to click to see gossip or secret info).

If you have fewer participants, one group can handle two triggers or skip one less common trigger.

2. **Provide examples:** Along with the trigger description, hand each group one or two example messages (or have them written on the board/paper slips).

- Urgency example: "Your account will be suspended in 30 minutes unless you confirm your password here [link]."
- Fear example: "Security Alert: Someone tried to access your photos! Send this code NOW to secure your account."
- Empathy example: "Please, my friend's little brother is in the hospital. We need donations urgently, anything helps. Click here to send help."
- Authority example: "Admin: This is tech support. We detected malware on your account. Respond with your login info so we can fix it."
- Opportunity example: "Congratulations, you've been selected to beta test a new game and get paid! Just fill this form with your details to start."
- Curiosity example: "OMG look at this photo of you I found online, is this you? [link]" or "They're saying horrible things about you in this group, thought you should see it [link]."

3. **Group task – match trigger to example & draft response:** Ask groups to first confirm that their examples indeed match their trigger (it should, by design). They should identify exactly what words or elements in the example illustrate the trigger. For instance, underlining "30 minutes" and "suspended" for urgency, or "little brother...hospital" for empathy tug. Then, each group drafts a short "safe-response script" for their example. This is typically 1-3 sentences, calm and assertive. Encourage them to use the neutral stems from Module 1 (which you can list on the board as a reminder, like "I don't share info via links; I'll check the official site." or

“I can’t help in that way, sorry.”). Also, they should include what they would actually do (the verification step or alternative action) as part of the script or right after it.

- For Urgency example: a good script might be, “I won’t rush. I’ll log into my account normally to see if there’s an issue.” (No giving info via the message.)
 - Fear example: “I won’t send any code. I’ll check my account security settings myself – if there was an alert, I’ll see it there.”
 - Empathy example: “I only donate through known charity sites or in person. I’ll verify this story through a trusted source.” or even simply, “I’m sorry, I can’t contribute that way. I hope your friend gets help.” (plus, not clicking the link)
 - Authority example: “Thanks, but I can’t share my password. I’ll contact official tech support through the website to verify this.”
 - Opportunity example: “Sounds cool, but I don’t give out personal info without checking. I’ll look up this company through official channels first.”
 - Curiosity example: “I won’t click this link. If there’s something about me, I’ll find out directly or ask a friend – this looks suspicious.”
4. **Share results:** Have each group come up and present their trigger, how the example demonstrated it, and their response script. Encourage other participants to snap their fingers or applaud good responses – keep it supportive. As each group shares, compile their response lines into a collective list of “Default Replies to Triggers” on a flipchart or slide. You’ll likely see repetition (multiple groups might have “I don’t click links from messages”), which is good – it reinforces key safe behaviours. If a group is missing something important in their response, gently ask, “Would you add anything to make it safer?” For example, if they didn’t include a verification step, suggest it and see if they agree to include it. Also, highlight any especially clever or empathetic phrasing. E.g., if someone had a polite decline like “Sorry, I can’t do that right now,” note that it’s okay to not always explain yourself at length – a simple refusal is fine.
5. **Build a collective set of replies:** By the end, you have a set of at least 6 examples reply to scripts (one per trigger). This is a great thing to share/take a photo of and perhaps distribute as a cheat-sheet later. It’s basically a youth-sourced “answer key” for suspicious messages.
6. **Extra discussion – personal triggers:** Now ask, “Which trigger affects you the most? Which are you most likely to fall for, or which is hardest

for you to resist?” and “What could be your personal pre-planned reply or strategy for that?” For instance, one might say, “Curiosity gets me. If I see something about me, I really want to click. So, my plan is to always show it to a friend first – that’s my rule now.” Another might say, “Urgency freaks me out; I think having that phrase ‘I’ll log in normally’ ready in my head will help.” This reflection personalises the lesson – each participant acknowledges their own vulnerability and arms themselves with a response.

Tools: If online, Padlet or a shared Canva/Google Slide where one column lists triggers, another column groups example screenshots (they could drag them under the right trigger), and a third column for their written response. If offline, print trigger titles on cardstock and example messages on paper strips, let them physically group them and write replies on paper to stick next to them or on flipchart.

Outcome: Participants leave with clear examples of what scam or manipulative messages look like and concrete, practiced lines to say or actions to take. This reduces the chance they’ll freeze up in a real situation – they’ll recall “I’ve seen this before – it’s just trying to rush me; I know what to do.”

Activity 3: Cyber Detective – Case Files

Objective: Give participants a chance to practice verification and threat-spotting skills on more complex, mixed-information scenarios. They must sift through evidence, identify red flags, check facts through a second source, and decide on a safe course of action (respond, report, or ignore). This simulates real-life situations where not everything is clear at first glance.

Format: Small team activity, working with provided “case files” that include multiple pieces of evidence (like a suspicious DM, a profile snippet, a link preview, etc.). Can be done online (via an LMS or shared folders) or offline (printed packets). Teams then present their findings.

Duration: 45–60 min.

Instructions:

1. Prepare case files: Create 2 or 3 distinct case scenarios. Each case file should contain:
 - A brief narrative or context blurb.
 - At least 2-3 pieces of evidence, such as:
 - A screenshot or text of a suspicious message (e.g., a contest winning notification, or a message from a friend asking a weird favour).

- A snippet of an online profile related to it (e.g., the profile of the person who sent the message, showing something off like it's new or has no mutual friends).
 - A link preview or URL that they might consider clicking (you can give the text of the URL and maybe what the website looks like superficially).
 - Some guiding tasks/questions for the team, such as: "List three red flags you find.", "How could you verify if this is legitimate?" and "What would your team decide to do: respond, ignore, report, or something else?"
2. Ensure the cases cover a range of threats, e.g.:
 - Case 1 could be "The Contest Message" – a classic phishing for personal info disguised as a prize win (covers phishing/scam).
 - Case 2: "The Friend in Need" – likely an impersonation of a friend needing money abroad (covers fake friend request/impersonation, empathy trigger).
 - Case 3: "The Fake Job Offer" or "Great Opportunity" – a teen gets an email/DM about a high-paying job requiring bank info (covers scam, authority maybe).
 - You could also imagine a Case 4 involving a cyberbullying scenario or a predator scenario (depending on time, etc.) but ensure not to overload. The first three cover quite a bit.
 3. **Team assignment:** Divide participants into teams of ~4. Assign each team one case (if fewer teams than cases, just use some cases; if more teams, two teams can do the same case and compare findings). Give them the case file materials (either through an online shared doc or printed handouts with any images attached).
 4. **Investigation phase:** Teams work together to analyse the materials (~15 minutes). They should:
 - Read the narrative to understand context.
 - Examine each piece of evidence for inconsistencies or red flags (e.g., in the contest case, they might note the prize message came from a generic Gmail, or the link is a bit.ly, or the profile that messaged them has 0 followers).
 - List red flags: encourage one member to jot down bullet points.
 - Attempt verification: If online and feasible, you could have them actually do a quick search or check (like "search the contest name + scam" on Google or check if the friend's real profile posts that they were hacked). If fully offline, they can hypothesise how they'd

verify (like “We’d call the friend’s family to see if they’re really abroad”).

- Based on the evidence and any verification, they decide what the best action is: e.g., ignore/delete the message, report the account to the platform, respond with caution (probably rarely respond in these cases), or gather more info.
- Also, ask them to note if any EI strategy was useful during their teamwork: did someone say, “hey let’s not jump to conclusions, what do we feel and what do we actually know?” or did taking a moment to double-check calm someone who was initially panicked by the scenario?

5. **Team Presentations:** Each team presents their case summary to the group:

- A quick recap of the scenario (“Ours was about winning a competition...”).
- The red flags they spotted (“The message had spelling mistakes and asked for an ID upload which is odd.”).
- How they verified or would verify (“We searched the competition online – no official info. Also, the supposed contest organiser’s profile was made yesterday, which is fishy.”).
- Their decision (“We would not click anything and report this DM as spam/phishing to the platform.” Or “We called our friend and found out their account was hacked, so we told them to secure their account.”).
- Encourage them to mention any emotional aspect: “At first, one of us was really excited thinking it was real, which shows how the scam can hook you. But another team member felt sceptical. Discussing together helped – a good takeaway is to ask someone else when you’re not sure.”

6. **Facilitator debrief checklist:** After each team, fill in any critical point they missed. For example, if a team didn’t mention the importance of not sending the ID photo (since it could be used for identity theft), bring that up: “Right, and sending your ID would be very dangerous, because scammers can use it to impersonate you – good thing you decided not to.” For each case, draw out the general lesson:

- Contest scam: Too good to be true offer + asks for personal info = likely scam. Emotional hook was excitement/greed.
- Friend in Need: Always verify through a second channel if a friend asks for money or codes. Emotional hook was empathy/friendship and urgency.

- Fake Job Offer: High pay for little work + asks for bank details upfront = scam. Emotional hook was excitement and maybe flattery (they “chose” you).
- If a predator grooming scenario was included: look for signs of someone being too interested, too quickly, asking for personal pics, etc. Lesson: Never continue if someone you met online starts getting too personal or asks for things – involve a trusted adult. Emotional hook is often validation and love, but real relationships don’t rush trust like that.
- Cyberbullying case (if one): maybe a mean post and a fake profile stirring drama. Lesson: Do not retaliate in anger (that can escalate); collect evidence, block, report, and talk to someone. Emotional hook is anger/shame.
- Summarise: The teams effectively acted as “cyber detectives,” and the big skill was verification through a second channel and team communication. Often, what one person misses, another catches – so encourage youth to consult each other in real life too.

7. **Reflection:** Ask, “What EI strategies helped the team stay calm and focused under the ambiguity or pressure of these cases?” Participants might say, “We reminded ourselves it might be a trick, so we didn’t get too excited” (self-regulation), or “We divided tasks and that kept us from freaking out” (relationship skills, teamwork), or “We actually took a second to confirm our gut feeling with a quick search” (that’s awareness and reflection in action).

Also ask, “How did working as a team change the outcome compared to if you were alone?” This will likely reinforce the value of peer support – someone alone might have fallen for it, but in a team, someone said “hold up, something’s off.” That’s what we want youth to realise: two minds are better than one in security.

Tools: If online, you can upload case file images and texts to a Google Drive/OneDrive or a Moodle forum for each team. Possibly use breakout rooms. For offline, print everything clearly (maybe in colour for screenshots) and even put them in envelopes marked “Case 1” etc., for a fun detective vibe.

Outcome: Participants practice deeper analysis and realise that threats often come with multiple clues if you look closely. They also practice the act of verifying (not just taking things at face value) – a critical digital skill. Plus, it reinforces emotional teamwork – not getting swept by the first feeling but investigating further.



Activity 4: My Digital Mirror – Self-Assessment

Objective: Encourage participants (youth or educators themselves) to reflect on their own online habits and emotions by completing a short self-assessment. Then, guide them to set one or two micro-goals for improving their digital habits in the coming week. This makes the learning personal and actionable.

Format: Individual activity followed by optional pair or group sharing. Can be done via an online form (anonymous or personal) or a printed handout. This is introspective and doesn't take too long, but discussion can be as deep as you allow.

Duration: 15-30 min.

Instructions:

1. **Distribute Self-Assessment (e.g. Handout_M4):** Provide each participant with the self-assessment. If online, send the Google Form link or if offline, give the printed questionnaire. Make sure they know this is not a test and they should answer honestly for themselves. The assessment includes statements like:
 - "When I receive an unexpected message or alert, I pause before responding." (Almost Always / Sometimes / Rarely / Never)
 - "I notice how I feel (curious, anxious, rushed) before clicking a link." (Likert scale)
 - "I verify unusual requests through a second source."
 - "I recognise when emotion is used to make me act fast (fear, pity, reward)."
 - "I ask for help or a second opinion when something seems off online."
 - "I update my devices and apps regularly."
 - "I limit what personal information I post publicly."
 - "When a mistake happens online, I can stay calm and try to fix it instead of hiding it."
 - "I support friends when they face online stress or scams."
 - "I take short breaks from screens to reset emotionally."
 - These cover technical (updates, privacy), behavioural (pausing, verifying, help-seeking), emotional (notice feelings, stay calm, take breaks), and social (support friends).
2. **Completion:** Give them time to fill this in quietly. If they're doing it on paper and it's not anonymous (i.e., they'll keep it), reassure them they won't have to show anyone their answers unless they want to. If using

an online form and you want anonymity, you could then display aggregated results for discussion without names.

3. **Scoring/reflection:** Explain that there's no pass/fail. One way to reflect is:

- If mostly "Almost Always" or "Sometimes," they have a lot of good habits – encourage them to keep it up and maybe mentor others.
- If they have many "Rarely" or "Never," those are potential growth areas. But even one improvement can significantly increase their safety.

There should also be a section for "My Insights" in the handout:

- The emotion that most often drives me online is: _____ (maybe anger? curiosity? boredom?)
- One situation where I feel least in control: _____ (e.g., late at night scrolling, or when I'm in a heated group chat, etc.)
- My personal "pause and check" signal will be: _____ (some decide maybe "when my heart beats fast, that's my signal to pause" or "if I get two messages in a row with 'URGENT', that's my cue")
- A support partner or friend who will remind me: _____ (this encourages them to identify a specific person as their "accountability buddy" or just someone to talk to about these goals).

4. **Choose micro-goals:** The handout should then ask them to tick one or two micro-goals for the week:

- ☐ Practice pausing before clicking.
- ☐ Ask one peer for a second opinion (when unsure about something).
- ☐ Adjust privacy settings (maybe make one account more private or remove a piece of personal info).
- ☐ Try 4-4-6 breathing before reacting in a heated situation.
- ☐ Other: _____ (they can fill in a custom small goal, like "enable 2FA on my Instagram" or "take a 10-min screen break daily"). It should be achievable within a week, not like "never fall for anything again" (too broad). Small steps lead to big change.

5. **Optional sharing:** If appropriate, have them share one insight and their chosen goal with a partner or small group. Alternatively, you can collect the chosen goals anonymously and read a few (to show variety). The sharing can create a sense of commitment: saying your goal out loud often reinforces the intent. It also lets peers support each other ("Hey, I

also chose to pause more; maybe we can remind each other in our group chat”).

6. **Accountability suggestion:** Suggest that they write down or set a reminder about their goal. For example, putting a Post-it note on their computer saying “Pause?” or scheduling a check-in with that friend (“Let’s see next Friday if we did our goals”). If this is a classroom or youth group, you can plan to revisit these goals in the next session – even if just to ask who feels they succeeded or what barriers they faced.
7. **Reflection:** Prompt a brief discussion: “What reminder or support will help you keep these two changes?” They might say things like, “I’ll change my phone lock screen to a message that says ‘Breathe.’” or “I told my sister about my goal, and she promised to poke me if she sees me getting angry at my phone.” This gets them thinking practically about sustaining the behaviour change.

Also ask, “How do you feel about these results? Are you surprised by any of your answers?” and “Do you feel motivated to work on any particular aspect?” Some might share, “I realised I never update my apps – that’s easy to fix and I will.” Another might say, “I rarely take breaks; I see how that makes me edgy. I’ll try to unplug before bed this week.”

Tools: If online, a Google/Microsoft Form or Mentimeter quiz (with a quiz you can show group stats for each question after). If offline, printed handouts and pens.

Outcome: This activity turns mirror on the participants, making all the abstract talk very personal. It reinforces self-awareness and commitment to improvement. By setting micro-goals, we increase the likelihood that they will actually change at least one behaviour (which is success!). It also highlights the breadth of cyber safety: it’s not just “don’t click bad links,” it’s also taking care of oneself emotionally (breaks, calm responses) and supporting others.

Activity 5: Cyber Diary – One Day Online

Objective: Increase participants’ awareness of emotional triggers in their everyday digital life and link those emotions to subsequent online behaviours. By keeping a brief diary of one day (or several days), they will identify patterns like “when X happens, I feel Y and do Z.” In the debrief, they’ll cluster common triggers and decide on one habit to change or one emotional cue to be mindful of.

Format: Individual diary (online form or paper) over 1-3 days, followed by a group debrief discussion of patterns. Optionally use a word cloud or sticky notes to visualise common feelings/triggers.



Duration: 10 min daily for 2–3 days + 20 min debrief.

Instructions:

1. **Diary template:** Provide a simple template (could be a small notebook page or a Google Form they submit each day) with columns like:
 - Time/Context: (e.g., Morning before school on Instagram, Afternoon during homework on YouTube, Evening gaming, etc.)
 - What happened online: (e.g., “Saw a mean comment on my post,” “Got 20 Snap notifications,” “Read news about...,” “Got bored and scrolled TikTok for an hour,” “Friend sent a funny meme,” “Someone forwarded a scary chain message,” etc.)
 - Emotion I felt: (e.g., happy, annoyed, left out, anxious, angry, excited, jealous, etc.)
 - What I did (behaviour): (e.g., replied something, clicked a link, forwarded it, ignored it, closed the app, confronted them, overshared something, or even something like “couldn’t stop thinking about it,” any notable action or inaction).
 - Maybe include Outcome/Reflection: (optional: “Looking back, was that a good choice? Would I do anything differently next time?” – this can be left for the debrief to fill in).
 - Encourage them to make at least 3-5 entries in a day (or if over 2-3 days, maybe 2 per day). They don’t have to log everything, just the moments when they felt a strong emotion while online or using their device.
2. **Explain & motivate:** Clarify this is a personal awareness exercise, not to hand in for grading. They can keep details private if they want (they can use shorthand or discuss generally later if something is sensitive). Emphasise honesty: “If you spent an hour doomscrolling and it made you anxious, note that. If you got super excited by a post and it made you buy something impulsively, note that. There’s no judgment, it’s to learn about ourselves.”

Also, ensure them that even “negative” emotions or “bad” behaviours in the diary are okay to write – everyone has them.
3. **Diary period:** Let them know the timeframe (say, until next meeting). If possible, send a reminder mid-way: e.g., a text or announcement: “Don’t forget to jot down any strong online moments today!”

If only doing a single day, maybe instruct them to pick tomorrow as the focus day and be mindful of noting things that day.
4. **Collect or reflect:** If using an anonymous form, you can aggregate responses for class patterns. If on paper, they keep it but will use it in discussion.

5. **Debrief discussion:** Come together after diary completion. Start by asking generally, “What kind of online moments triggered strong feelings for you?” List them as participants share (could be things like: receiving no likes on a post, seeing friends hang out without me, getting a scary news alert, being very engaged in a game, someone not replying fast, etc.). Then ask, “What were the most common feelings?” Perhaps tally or have them shout out: anxious, happy, frustrated, jealous, etc. Use a tool like Mentimeter word cloud or just write on board: “Emotions we felt online this week.” This visual can be powerful to see that anxiety or FOMO might be huge, or maybe joy and amusement are also big – it’s a mix. Next, discuss the link to behaviour: “When you felt [emotion], what did you tend to do right after?” e.g., “When I felt angry at a comment, I wrote a snarky reply (and maybe regret it).” “When I felt lonely, I started browsing random profiles for an hour.” “When I felt excited, I clicked a bunch of links about it.” Possibly, group similar triggers:
 - Social triggers: e.g., seeing posts that made them jealous or left out → feelings (insecurity) → behaviour (maybe posting something attention-seeking or just feeling down).
 - Scam/fear triggers: e.g., weird messages → feelings (anxious) → behaviour (either hurried to act or sought help).
 - Information overload triggers: e.g., too many notifications → feelings (stress) → behaviour (shut off phone or conversely, compulsively checked all).
 - You could draw a simple map on board connecting triggers to feelings to actions for recurring patterns.
6. **Select one habit to change:** Now ask each, “From your diary, what’s one pattern you noticed that you might want to change?” For example: “I see that every night I scroll late and it makes me exhausted – I want to cut that down.” or “Whenever I see news about world problems I get anxious and it ruins my mood – maybe I can limit how often I check news.” or “I realised I respond with a lot of exclamation points and urgency when I’m excited, maybe I should compose myself before I message people, so I don’t overshare or agree to things I don’t actually want.”
7. If this is a one-off workshop and not ongoing, encourage them to tell a friend or sibling about their plan for accountability.

Tools: Paper diaries or shared Google Doc template; Mentimeter or slido for an anonymous word cloud of emotions (optional).



Outcome: Participants heighten their self-awareness around digital habits. They often discover “Whoa, I didn’t realise I get angry so often on X,” or “I check my phone every time I feel bored.” This insight is the first step to change. By public (or semi-public) reflection, they also see they’re not alone in these struggles (others have FOMO or get stressed by notifications too). Choosing a concrete habit to alter makes the nebulous concept of “be better online” into a tangible action, like “I will turn off notifications during homework” or “I will not respond to messages when I’m upset; I’ll wait.” And tying it to the cue (emotion trigger) means they’re applying the EI cycle: notice feeling -> alter response. This diary effectively connects emotional cues with cybersecurity behaviours in real life.

Activity 6: Vulnerability Map – Workshop

Objective: Participants will create a visual map of vulnerabilities across four dimensions (Technical, Behavioural, Emotional, Social) and then brainstorm specific mitigations for each, along with an EI support strategy. Finally, they commit to one action per quadrant. This synthesises the module’s content by having them apply it to a big-picture view of their own or their group’s risks.

Format: Small groups or individuals drawing a quadrant chart (online using Canva/Miro or offline on poster paper with sticky notes). They list personal or observed vulnerabilities in each area, then for each, write one way to reduce that vulnerability (mitigation) and one EI-related support (like a habit or a reminder involving emotional skills). The result is a kind of security plan matrix.

Duration: 40–50 min.

Instructions:

1. **Setup quadrants:** Whether on a large poster, whiteboard, or digital canvas, draw a square divided into four labelled quadrants:
 - Technical
 - Behavioural
 - Emotional
 - Social

Briefly remind everyone what each category includes (from Module Content and earlier activities).

- Technical: hardware/software issues (passwords, updates, network safety, etc.).
- Behavioural: what we do online (clicking without thinking, oversharing, etc.).

- Emotional: how our feelings affect our online actions (impulsivity, stress, etc.).
 - Social: influences from others (peer pressure, trusting strangers, misinformation spread, etc.).
 - If working in small groups, each group gets their own “map” to fill out. If one large group, you can do one collectively on a board with everyone contributing sticky notes.
 - Identify vulnerabilities: Ask participants to think of personal or common vulnerabilities for youth in each category. They can reflect on what they’ve learned, diaries, discussions:
 - Technical examples: Weak passwords or reusing passwords; not using 2FA; using public Wi-Fi without caution; leaving devices unattended; not updating apps; sharing devices without logout; etc.
 - Behavioural examples: Clicking links in messages; oversharing on social media; accepting friend requests from people not known in real life; downloading pirated or random software; not reading permissions on apps; posting when angry (which could be emotional too); falling for scams like prize offers; etc.
 - Emotional examples: Acting out of fear or anger (like replying rudely or panicking and clicking); being too curious (clicking gossip); feeling lonely and believing a random online flirt; feeling confident “I know it all” and skipping warnings; embarrassment leading you not to seek help when something bad happens; etc.
 - Social examples: Peer pressure to join in risky online challenges; trusting things just because many people shared it; assuming someone in a community is safe because others seem to trust them; being influenced by groupthink in forums; cyberbullying dynamics (pressure to gang up or keep quiet); not wanting to be the only one with private account when friends go public; etc.
 - Have them either write each vulnerability on a separate sticky note (if physical) or text box (if digital) and place in the appropriate quadrant. Aim for at least 3-4 per quadrant from each group. Encourage specifics (“Using ‘12345’ as a password” rather than just “weak passwords” – though either is fine).
2. **Mitigation Brainstorm:** Now, for each vulnerability note, they add a mitigation – something concrete to reduce or eliminate that risk:
- For weak passwords: Use a password manager or passphrase, enable 2FA.



- For not updating: Turn on auto-updates, schedule a monthly check.
 - Public Wi-Fi: Use VPN or avoid sensitive logins on public networks.
 - Oversharing: Do a privacy settings review; think twice before posting; use a rule like “if I wouldn’t say it to a room of strangers, I won’t post it publicly.”
 - Clicking impulsively: Pause-and-check routine.
 - Accepting unknown friends: Set profile to private; only accept if I can verify who they are through mutual contacts.
 - Downloading random stuff: Only download from official app stores; check reviews and permissions.
 - Emotional: Acting out of fear: Do breathing exercises; wait 1 hour before responding to upsetting content.
 - Believing flattery: Remind self “online compliments can be fake”; verify the person’s identity through video chat with a parent present or not at all.
 - Embarrassed to report: Have an anonymous way to report in our group; remember it’s not your fault if you were scammed.
 - Social: Peer challenge: Watch “challenge” videos critically; if risky, talk to an adult before doing anything.
 - Herd behaviour: Play devil’s advocate mentally – ask “could this be wrong?” even if lots of shares; use fact-check sites.
 - Trust in communities: Use zero-trust mindset: even in safe communities, verify new people or info.
 - Each mitigation can be written next to or on the same note as the vulnerability, maybe in a different colour. Encourage specificity.
3. **Commitment line:** At the bottom of the poster or on a separate sheet, have each participant (or the group collectively) write down one action they personally commit to in each quadrant for the coming week. For example:
- Technical: “Enable 2FA on two accounts by Friday.”
 - Behavioural: “No more accepting friend requests from people I haven’t met – I will ask them who we both know first.”
 - Emotional: “When I’m upset online, I will take a 5-minute break instead of responding.”
 - Social: “If I see a friend doing something risky, I’ll gently remind them of what we learned (be a upstander).”

- These are like mini pledges that tie the workshop to future behaviour. If the module is part of an ongoing program, you can revisit these commitments later.
4. **Gallery walk (if time):** If multiple groups made maps, let everyone walk around and see each other's or present highlights. They might learn from others' vulnerabilities and mitigations they hadn't thought of.
 5. **Wrap-up reflection:** "Which single action (from any quadrant) do you think will have the biggest immediate impact on your or your group's safety?" Some might say the technical ones like 2FA give strong boost, others might value emotional ones like pausing because they click less. It's a way to reinforce that all quadrants matter, and often they interplay (e.g., emotional control could prevent a behavioural mistake like oversharing).
Also ask: "How did mapping it out help you visualise your security?" People might respond that seeing it categorised made it clear where they are weakest (maybe lots in behavioural vs technical), or it was satisfying to turn each scary vulnerability into an action step, so it feels solvable.

Tools: Large paper and markers or whiteboard for offline; or Miro/Canva/Google Jamboard for online collaborative mapping (with text boxes and maybe images/icons to make it fun).

Outcome: The vulnerability map exercise consolidates learning. Participants externalise risks from their head onto paper, which makes it less overwhelming and more like "objects" they can tackle. It also shows the breadth of cybersecurity – not just tech fixes, but habits and feelings and community aspects. By writing mitigations, they transform abstract dangers into concrete to-dos. The EI support column ensures they remember the human factor in each solution. And the commitments turn this from just a theoretical plan into a personal to-do list, increasing the chance that the training results in real behaviour change.

Key Takeaways for Youth Workers

- Emotional intelligence is a defensive weapon in cybersecurity. Teaching young people to recognise their emotional patterns – like stress, curiosity, empathy – is just as important as teaching them about firewalls and antivirus. Scammers often hack our feelings, so we must protect our feelings.
- Recognising emotional triggers helps prevent manipulation. Youth who can say, "I'm feeling really excited by this offer, which means I should be

careful,” are far less likely to fall victim to scams or peer pressure. It’s about turning emotions from a blind driver into a helpful passenger.

- Gamified learning and scenarios dramatically enhance engagement and retention. When lessons are turned into quizzes, challenges, or role-plays, youths participate more actively and remember the content longer. Games also encourage peer collaboration and discussion, which reinforces learning socially.
- Blending assessment with reflection leads to sustainable change. Using tools like self-assessments or diaries and then discussing them helps youths see their growth areas without feeling judged. It turns learning into a personal mission (e.g., “I realise I should update my phone more often; I will do that now.”). Reflection ensures they internalise why a behaviour is risky or safe, which makes them more likely to continue the good practices beyond the workshop.
- Peer support structures are key. A culture where youths help each other (like double-checking messages together or not making fun of someone for being cautious) can be one of the strongest defences. Encourage the creation of buddy systems, group norms for verifying information, and open communication about mistakes (so if someone gets tricked, they tell others to prevent it happening to someone else, rather than hiding it out of shame).

Activities Module 5

Youth ambassadors can promote security culture through awareness campaigns, social media, and by educating peers and the community on safe online practices, participating in cybersecurity events, and by creating engaging content. Other activities include organising workshops, leading security campaigns, and connecting with cybersecurity professionals to gain experience and knowledge.

Community & Peer Education

- Organise workshops and events: Host sessions, organise cybersecurity games, or set up virtual Q&As with experts to teach peers about online risks.
- Run awareness campaigns: Create posters, videos, and presentations to educate others about cybersecurity threats and preventative measures.
- Engage with online communities: Share information and resources on social media to spread awareness and encourage safe online behaviour.

- Create public service announcements (PSAs): Develop short, impactful videos or messages to highlight key cybersecurity issues.
- Attend training and webinars: Take part in programs that offer technical training, workshops, and access to a network of cybersecurity professionals.

Creative & engaging activities

- Launch a cybersecurity meme contest: Use humour to raise awareness about cybersecurity issues and encourage engagement.

Networking & Leadership

- Connect with professionals and peers: Build a professional network by attending events, joining online forums, and engaging with cybersecurity professionals.
- Lead initiatives: Take the lead in educating and empowering the next generation by proposing and implementing new ideas and projects within the community.
- Share personal stories: Inspire others by sharing your own experiences and achievements in the cybersecurity field

Practical activities to perform with youth

Activity 1: The Digital Trust Tree

Purpose:

To help young people and youth workers explore what makes them feel safe or unsafe in digital spaces, and to co-create a shared understanding of the values that build a culture of trust and respect online.

Duration: 60–75 minutes

Group Size: 8–20 participants

Materials: Flipchart paper or large poster board, coloured markers, sticky notes, optional digital whiteboard (e.g., Miro, Jamboard).

Instructions

1. Introduction (10 min)

Explain that security culture starts from shared trust. Invite participants to think about what helps them feel emotionally and digitally safe online.

2. Drawing the Tree (10 min)

On a large sheet, draw a simple tree with roots, a trunk, and branches. Label the sections as:

- *Roots = Values that support security (e.g., empathy, honesty, respect)*

- *Trunk = Habits or rules (e.g., factchecking, privacy settings)*
- *Branches & Leaves = Actions and attitudes that grow from these roots (e.g., helping friends, mindful posting).*

3. Group Work (25 min)

Divide participants into small groups to fill in each section using sticky notes or direct writing on the tree. Encourage open discussion.

4. Sharing (15 min)

Groups share their trees and identify recurring themes.

5. Synthesis (10 min)

Combine all ideas into one collective “Digital Trust Tree” and display it in the learning space or post it on social media as a youth-created statement of values.

Reflection

- What values appeared most often?
- What daily actions show these values online?
- How can we apply this “trust tree” in our own digital behaviour?

Learning Outcomes:

- Recognises the link between values and digital safety.
- Strengthens leadership through participatory discussion.
- Encourages empathy and shared responsibility in online spaces.

Activity 2: Emotion Filter

Purpose:

To support participants in identifying emotions triggered by digital interactions and developing emotional regulation strategies.

Duration: 60 minutes

Group Size: 6–15 participants

Materials: Emotion cards or printed emoji sheets, scenario cards with typical online situations (e.g., group exclusion, fake news, offensive comment).

Instructions

1. Warm-up (10 min)

Discuss how emotions influence online decisions. Ask: “When did a strong emotion affect what you posted or said online?”

2. Scenario Work (25 min)

Divide into small groups. Give each group one scenario card. Ask them to:

- Identify what emotions might arise.

- Discuss how each emotion could influence behaviour.
- Suggest constructive ways to respond mindfully.

3. **Sharing & Discussion (15 min)**

Each group presents their reflections. Highlight examples of emotional regulation or empathy.

4. **Action Plan (10 min)**

Each participant writes one personal “emotion filter” reminder, for instance: “Before posting, I’ll name my feeling and wait 5 minutes.”

Reflection

- What emotions affect your online behaviour the most?
- How does awareness change your reactions?
- What practical strategies help you regulate strong emotions?

Learning Outcomes:

- Develops self-awareness and self-regulation.
- Builds emotional intelligence for online contexts.
- Encourages empathy-based problem solving.

Activity 3: Ambassador Map

Purpose:

To help youth workers and participants identify and visualise existing support networks, stakeholders, and allies who can promote security culture.

Duration: 75 minutes

Group Size: 8–20 participants

Materials: Large paper or digital canvas, markers, and post-it notes.

Instructions

1. **Introduction (10 min)**

Explain that no ambassador acts alone. Security culture is a collective effort involving peers, organisations, and local institutions.

2. **Mapping Exercise (30 min)**

In the centre of the paper, write “Youth Ambassador.” Around it, create circles representing:

- *Peers and friends*
- *Family and mentors*
- *Schools and NGOs*
- *Authorities or online safety organisations*

Ask groups to identify examples for each circle and note how each actor can help.



3. Connection Lines (15 min)

Draw arrows showing existing connections and gaps (“Who are we missing?”).

4. Action Planning (15 min)

Each group proposes one new partnership or action (e.g., inviting a police officer or psychologist to a discussion, starting a peer-support group).

Reflection

- Who are your current allies in promoting security culture?
- What partnerships could strengthen your efforts?
- How can youth workers facilitate these connections?

Learning Outcomes:

- Builds networking and advocacy skills.
- Encourages cooperation and trust across stakeholders.
- Promotes systemic thinking about youth support.

Activity 4: #MindfulMedia Campaign

Purpose:

To empower young people to design and deliver short awareness campaigns promoting security culture, emotional intelligence, and mindful digital engagement.

Duration: 2–3 sessions of 90 minutes each

Group Size: 6–12 participants

Materials: Smartphones, internet access, Canva/PosterMyWall templates, social media accounts, campaign worksheet.

Instructions

1. Session 1 – Ideation (90 min)

- Discuss what digital issue matters most to participants (e.g., misinformation, empathy online, cyberbullying).
- Brainstorm slogans and hashtags (e.g., #ThinkBeforeYouType, #MyDigitalMood).
- Choose one campaign focus and audience.

2. Session 2 – Design (90 min)

- Create short visuals, reels, or text posts.
- Agree on a publishing plan and roles (content creator, editor, fact-checker, social media manager).

3. Session 3 – Launch and Reflection (90 min)

- Publish campaign materials.

- Track engagement (likes, comments, shares).
- Reflect on the message's emotional impact and authenticity.

Reflection

- What message resonated most with your audience?
- What did you learn about leadership and teamwork through this campaign?
- How did you ensure your content reflected empathy and responsibility?

Learning Outcomes:

- Strengthens leadership and communication skills.
- Fosters creativity and peer collaboration.
- Encourages civic participation and responsible digital expression.

Activity 5: Pause-Reflect-Respond

Purpose:

To train youth workers and young people in emotional regulation and conflict mediation for online or group situations.

Duration: 75 minutes

Group Size: 10–15 participants

Materials: Scenario cards, reflection sheets, projector (optional).

Instructions

1. Introduction (10 min)

Present the idea that impulsive reactions online can escalate conflicts, while emotional awareness can prevent harm.

2. Group Work (30 min)

In groups of 3–4, assign conflict scenarios (e.g., being excluded from a chat, receiving a mean comment, misinterpreted post). Each group role-plays:

- **Pause:** identify emotions involved.
- **Reflect:** discuss options.
- **Respond:** choose an assertive, empathetic reply.

3. Group Discussion (20 min)

Analyse which responses were most constructive and why.

4. EI Toolbox (15 min)

Co-create a list of “tools for calm communication” (deep breath, empathy statement, fact-check, seeking support).

Reflection



- What emotions make you react most strongly online?
- How can you turn emotional awareness into leadership?
- Which EI skills helped most in resolving the conflict?

Learning Outcomes:

- Strengthens self-regulation and empathy.
- Develops mediation and communication skills.
- Promotes responsible, emotionally intelligent behaviour online.

Activity 6: Youth–Adult Dialogue Lab

Purpose:

To improve intergenerational understanding of online risks, values, and behaviours, fostering a shared sense of responsibility and trust between youth and adults.

Duration: 90 minutes

Group Size: 10–20 (balanced mix of young people and adults/parents/teachers)

Materials: Discussion cards, flipchart, markers, neutral facilitator.

Instructions

1. Introduction (15 min)

Explain the goal: to bridge generational perceptions of online life and discuss what “security” and “trust” mean to each group.

2. Separate Reflection (20 min)

Youth and adults discuss separately:

- “What worries me most online?”
- “What makes me feel safe?”
- “What do I wish the other group understood?”

3. Joint Dialogue (40 min)

Bring both groups together to share reflections. Identify overlaps and differences.

Work together to create a “Digital Trust Agreement” – a simple charter of mutual expectations.

4. Closing (15 min)

Summarise insights and emphasise the importance of ongoing communication and empathy.

Reflection

- What surprised you about the other group’s perspective?
- How can this dialogue continue in your community?

- How did emotional intelligence influence your communication?

Learning Outcomes:

- Builds empathy and understanding between generations.
- Strengthens facilitation and leadership capacities.
- Promotes collaboration and advocacy for safer digital communities.

Activity 7: “Digital Bridge – Talking Across Generations”**Purpose:**

To strengthen mutual understanding between young people and their parents or adults, in general, on issues of online safety, misinformation, and emotional responses to digital threats.

Duration: 50 minutes

Group Size: 8–20 participants (ideally 50% youth, 50 % parents/adults)

Materials: Flipchart paper, markers, “emotion cards,” printed scenarios, projector (optional).

Instructions**1. Warm-up – “Generations in the Digital World” (10 min)**

- Show two contrasting digital items (e.g., a TikTok clip and a news article).
- Ask youth and adults separately: “What emotions or concerns come up for you when you see this?”
- Share quick reactions to highlight perception gaps.

2. Role-Switch Simulation (20 min)

- Create pairs, one youth and one parent/adult) and switch roles – youth acts as the parent, parent as the youth.
- Present one mini-scenario (e.g., phishing message, cyberbullying incident, fake news).
- Participants model a conversation trying to reach a joint solution.
- Observer notes examples of empathy, tone, clarity.

3. Closing (20 min)

Summarise the feelings of trying to act from a different perspective and age, and how this different perspective influenced the dialogue and the reactions.

Reflection

- How did it feel to explain a digital threat to someone from a different generation?
- What emotions surfaced on each side?



- Which listening or phrasing techniques helped reduce tension?
- How can we keep this conversation open beyond the session?

Learning Outcomes

- Improved empathy and emotional regulation across generations.
- Enhanced youth confidence in discussing digital safety at home.
- Strengthened parental understanding of emotional, not just technical, threats.

References

Module 1

European Commission. (2020). *Digital Education Action Plan 2021–2027: Resetting education and training for the digital age* (COM (2020) 624 final). Publications Office of the European Union.

European Union Agency for Cybersecurity. (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies*. ENISA.

Mayer, J. D., & Salovey, P. (1997). What is emotional intelligence? In P. Salovey & D. Sluyter (Eds.), *Emotional development and emotional intelligence: Educational implications* (pp. 3–31). Basic Books.

Collaborative for Academic, Social, and Emotional Learning. (2020). *SEL framework: What are the core competencies?* CASEL.

Module 2

Blended Learning & Pedagogy

Garrison, D. R., & Vaughan, N. D. (2008). *Blended learning in higher education: Framework, principles, and guidelines*. Jossey-Bass. <https://doi.org/10.1002/9781118269558>

UNESCO. (2022). *Guidelines on blended learning for quality education*. UNESCO Publications. <https://unesdoc.unesco.org/ark:/48223/pf0000380609>

OECD. (2023). *Teaching for the digital era: Effective strategies for blended and online learning*. OECD Publishing. <https://www.oecd.org/education/teaching-for-the-digital-era.htm>

Emotional Intelligence

Salovey, P., & Mayer, J. D. (1990). Emotional intelligence. *Imagination, Cognition and Personality*, 9(3), 185–211. <https://doi.org/10.2190/DUGG-P24E-52WK-6CDG>

Wong, C. S., & Law, K. S. (2002). The effects of leader and follower emotional intelligence on performance and attitude. *The Leadership Quarterly*, 13(3), 243–274. [https://doi.org/10.1016/S1048-9843\(02\)00099-2](https://doi.org/10.1016/S1048-9843(02)00099-2)

Universal Design for Learning & Inclusion

CAST. (2018). *Universal design for learning guidelines version 2.2*. CAST, Inc. <https://udlguidelines.cast.org/static/udlg2.2-text-a11y.pdf>

European Agency for Special Needs and Inclusive Education. (2022). *Inclusive digital education: Project examples*. EASNIE. https://www.european-agency.org/sites/default/files/_Inclusive_Digital_Education_Project_Examples.pdf

Digital Citizenship, Youth Work & Cyber Literacy

Council of Europe. (2022). *Digital citizenship education handbook*. Council of Europe Publishing. <https://www.coe.int/en/web/digital-citizenship-education>

European Commission Joint Research Centre. (2022). *DigComp 2.2: The digital competence framework for citizens*. Publications Office of the European Union. https://joint-research-centre.ec.europa.eu/digcomp_en

Vermeire, L., & Van den Broeck, W. (2024). Digital futures: A signal-based approach to inclusive digital youth work for socially vulnerable youth. *Media and Communication*, 12(2), 63–80. <https://doi.org/10.17645/mac.i446>

SALTO-YOUTH. (2023). *Curriculum for youth workers: Competence framework and training resources*. SALTO. https://www.salto-youth.net/downloads/toolbox_tool_download-file-3965/PR2_Final.pdf

Module 3

CAST Inc. (2018). *Universal Design for Learning Guidelines Version 2.2*. Wakefield, MA: CAST. <https://udlguidelines.cast.org/static/udlg2.2-text-a11y.pdf>

Council of Europe (2022). *Digital Citizenship Education Handbook*. Strasbourg: Council of Europe Publishing. <https://www.coe.int/en/web/digital-citizenship-education>

European Agency for Special Needs and Inclusive Education (2022). *Inclusive Digital Education: Project Examples*. Odense: EASNIE. https://www.european-agency.org/sites/default/files/_Inclusive_Digital_Education_Project_Examples.pdf

European Commission Joint Research Centre (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. Luxembourg: Publications Office of the European Union. https://joint-research-centre.ec.europa.eu/digcomp_en

Garrison, D. R., & Vaughan, N. D. (2008). *Blended Learning in Higher Education: Framework, Principles and Guidelines*. San Francisco: Jossey-Bass / Wiley. <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118269558>



OECD (2023). Teaching for the Digital Era: Effective Strategies for Blended and Online Learning. Paris: OECD Publishing.

<https://www.oecd.org/education/teaching-for-the-digital-era.htm>

Salovey, P., & Mayer, J. D. (1990). Emotional Intelligence. *Imagination, Cognition and Personality*, 9(3), 185–211.

<https://doi.org/10.2190/DUGG-P24E-52WK-6CDG>

SALTO-YOUTH (2023). Curriculum for Youth Workers: Competence Framework and Training Resources. Bonn: SALTO.

https://www.salto-youth.net/downloads/toolbox_tool_download-file-3965/PR2_Final.pdf

UNESCO (2022). Guidelines on Blended Learning for Quality Education. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000380609>

Vermeire, L., & Van den Broeck, W. (2024). Digital Futures: A Signal-Based Approach to Inclusive Digital Youth Work for Socially Vulnerable Youth. *Media & Communication*, 12(2), 63–80. <https://doi.org/10.17645/mac.i446>

Wong, C. S., & Law, K. S. (2002). The Effects of Leader and Follower Emotional Intelligence on Performance and Attitude. *The Leadership Quarterly*, 13(3), 243–274. [https://doi.org/10.1016/S1048-9843\(02\)00099-2](https://doi.org/10.1016/S1048-9843(02)00099-2)

Module 4

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*, 51(5), 586–611. <https://doi.org/10.1177/1046878120933312>

European Commission. (2020). *Digital Education Action Plan 2021–2027: Resetting education and training for the digital age* (COM(2020) 624 final). Publications Office of the European Union.

European Commission. (2023). *Proposal for a Council Recommendation on improving the provision of digital skills and competences in education and training*. European Commission.

European Union Agency for Cybersecurity (ENISA). (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies*. ENISA.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146–1166. <https://doi.org/10.1177/0093650215627483>

Annexes

Annexes Module 1

Annex A – Concept Map Worksheet

Instructions (for participants)

Write one everyday digital moment in the centre (e.g., “Urgent message about my account”).

Around it, add the following nodes and connect them with arrows:

- Threat
- Vulnerability
- Behaviour (what I might do)
- Emotion (what I feel)
- Safer Response (what I will do instead)
- Verification Step (how I will check)

Add a short sentence explaining each arrow (e.g., “Feeling rushed can push me to click without checking”).

Worked example

Central moment: “DM says my account will be deleted in 30 minutes.”

Threat: Phishing attempt.

Vulnerability: Rushing; reusing passwords.

Behaviour: Clicking the link to “fix it.”

Emotion: Anxiety, fear of loss.

Safer Response: Pause, breathe, open the official app directly (not the link).

Verification Step: Check notifications inside the app; ask a trusted peer to double-check.

Blank prompts to fill in

Central moment: _____

Threat: _____

Vulnerability: _____

Behaviour: _____

Emotion: _____

Safer Response: _____

Verification Step: _____

Annex B – Case Vignette Sheet

Instructions (for pairs or small groups)

Read each short scenario. Underline red flags, circle words that trigger emotion, and draft a calm, two-sentence reply plus one verification step.



Vignette 1 – “Support Contact”

“You’ve violated community rules. Click here to confirm your identity, or your account will be suspended today.”

- Likely trigger: Urgency / fear.
- Red flags (space): _____
- Calm reply (two sentences): _____
- Verification step: _____

Vignette 2 – “Friend in a Hurry”

“Hey, it’s me. I changed numbers. Can you send me your login code so I can get back in?”

- Likely trigger: Empathy / pressure to help.
- Red flags (space): _____
- Calm reply (two sentences): _____
- Verification step: _____

Vignette 3 – “Prize Drop”

“Congrats! You’re the lucky winner of a new phone. Pay €2 shipping here to claim in the next hour.”

- Likely trigger: Excitement / reward.
- Red flags (space): _____
- Calm reply (two sentences): _____
- Verification step: _____

Response stems you can use

“I don’t follow links in messages. I’ll check in the official app.”

“I never share codes or passwords. I’ll verify through another channel.”

“If it’s a real offer, I can find it on the company’s official site.”

Annex C – EI Micro-skills One-Pager

Purpose: Simple routines learners can use before clicking or replying.

1) Stop – Breathe – Check (10–20 seconds)

Stop: Take hands off keyboard/phone for 3 seconds.

Breathe: In 4 – hold 2 – out 6 (one or two cycles).

Check: What do I feel? What is the message asking for? What is one safe verification step?

2) 4-4-6 Breathing (20–30 seconds)

Inhale through the nose for 4.

Hold for 4.



Exhale through the mouth for 6 (longer out-breath).
Repeat twice. Notice your shoulders and jaw relax.

3) Peer Double-Check Message (under 1 minute)

Send a screenshot or describe the message to a trusted friend/adult.
Ask: "Does anything look off? What would you do?"
Only act after a second opinion.

4) Two-Step Verify (habit rule)

Never act from the link in a pressured message.
Open the official app/site yourself or use a saved bookmark.
If unsure, contact support via official help pages.
Youth-friendly self-talk prompts
"I don't need to rush."
"I can verify first."
"It's okay to say no politely."

Annex D – Think-Aloud Script Template Instructions (for educators)

Use this template to model your internal process out loud while handling a risky message. Keep it to ~60 seconds.

Script prompts

Feeling label: "I notice I'm feeling _____ (e.g., rushed/curious)."
Trigger spotted: "This message uses _____ (urgency/authority/reward)."
Pause: "I'll take one slow breath to think."
Risk question: "What is it asking me to do and why?"
Verification step: "Instead of clicking here, I'll open the official app/site."
Calm reply (optional): "I don't share codes or personal data. I'll check through official channels."
Decision: "I'll verify first, then decide."
Self-talk: "Slowing down helps me stay safe."

Your script (fill in):

Message type: _____
Feeling I name: _____
Trigger I spot: _____
My pause: _____
My verification step: _____
My reply sentence: _____
Final decision: _____





Annex E – Misconception Cards

Instructions (for groups)

Mark each statement True, False, or Depends, then write one sentence to clarify in youth-friendly language.

"If my password is strong, I don't need 2FA."

T / F / Depends – Clarify: _____

"If a message comes from a friend's account, it's safe."

T / F / Depends – Clarify: _____

"Only older adults fall for scams."

T / F / Depends – Clarify: _____

"If I feel anxious, I should ignore my feelings and just act."

T / F / Depends – Clarify: _____

"Official support might ask for my password to help me."

T / F / Depends – Clarify: _____

"If it's urgent, I should click first and think later."

T / F / Depends – Clarify: _____

"Using public Wi-Fi is always safe if the site is HTTPS."

T / F / Depends – Clarify: _____

"Privacy settings don't matter if I'm not famous."

T / F / Depends – Clarify: _____

"If a prize has a tiny 'shipping fee,' it's probably legit."

T / F / Depends – Clarify: _____

"Emotions make you weak online."

T / F / Depends – Clarify: _____

Facilitator note (useful corrective stems)

"Strong passwords help, but 2FA adds a second lock."

"Accounts can be hacked; verify through another channel."

"Scams target everyone; tactics are adapted to youth too."

"Feelings are signals; notice them, then verify calmly."

"Real support never asks for passwords or codes."

"Urgency is a red flag; pause and check in the official app."

"HTTPS helps, but public Wi-Fi still carries risk; avoid sensitive actions."

"Privacy settings limit exposure and future harm."

"Fees and timers are classic scam tactics."

"Emotional intelligence strengthens safety and decisions."

Annexes Module 2

Annex 1: Cyber Hygiene Checklist

This checklist helps youth evaluate their daily online practices and stay safe while managing emotional triggers.

Daily Safety Checks:

- ☐ I pause before clicking on links—especially if I feel rushed or stressed.
- ☐ I verify unknown profiles before accepting requests.
- ☐ I avoid posting when I feel angry, excited, or pressured.
- ☐ I keep my device updated (apps, browser, operating system).
- ☐ I check privacy settings on all social media accounts.
- ☐ I download files only from trusted, verified sources.
- ☐ I use strong passwords and two-factor authentication when possible.
- ☐ I verify information before sharing it.
- ☐ I reflect on how online interactions make me feel.

Annex 2: Emotional Intelligence Coping Techniques Guide

This guide supports youth in managing stress, impulsivity, and emotional vulnerability related to online threats.

Quick EI Tools:

- 4-6 Breathing: Inhale 4 seconds → Hold 4 → Exhale 6. Great for resisting scams and phishing urgency.
- Emotional Labelling: “I feel ___ because ___.” Helps avoid impulsive posts and reactions.
- Grounding Exercise: Name 5 things you see, 4 you feel, 3 you hear—useful during cyberbullying or distress.
- Pause Technique: Before responding, ask: “Is this safe? Is this true? What emotion am I feeling?”
- Positive Reappraisal: Replace panic thoughts (“This looks urgent!”) with calm ones (“I can check this calmly.”).
- Digital Time-Out: Step away when feeling overwhelmed online.

Annex 3: Role-Play Scenario Cards

Use these scenario prompts for blended or offline activities.

Scenario 1: Cyberbullying in a Group Chat

- Attacker: Write the hurtful message.
- Victim: Express how it feels.

- Observer: Suggest alternatives.
- Mediator: Model empathy and conflict resolution.

Scenario 2: Fake Friend Request

- A new profile acts friendly but asks for personal info.
- Youth identify red flags and practice safe boundaries.

Scenario 3: Phishing Email with Urgency

- A “school administrator” threatens account deletion.
- Youth practice pausing, breathing, verifying.

Scenario 4: FOMO Scam (“You Won a Prize!”)

- Explore reward-driven emotional triggers.
- Youth identify manipulation tactics.

Scenario 5: Misinformation Post

- A viral message claims a shocking event.
- Youth analyse emotional triggers and fact-check.

Scenario 6: Malware-Risky Download

- A “free streaming link” promises premium content.
- Youth discuss curiosity vs. caution.

Annex 4: Peer Circle Guide

Peer support circles empower youth-led resilience.

Structure:

- Form groups of 3–4.
- Rotate the Cyber Ambassador role monthly.
- Meet bi-weekly or monthly.

Each Session Includes:

1. Risk Spotlight: Discuss one cyber threat encountered recently.
2. Emotional Reflection: How did it make you feel? (Use EI tools.)
3. Coping Strategies: What could be done differently?
4. Prevention Challenge: Each member commits to one digital safety habit.

Ambassador Responsibilities:

- Encourage respectful dialogue.
- Share up-to-date cyber threats.
- Support peers experiencing online distress.
- Promote empathy and safe digital habits.

Annexes Module 3

Annex A: Inclusive Session Plan Template

Purpose: A **step-by-step template** for designing **30–60 minute blended sessions** that address the **eight online risk areas** while integrating **EI, UDL, and digital tools**.

Contents:

Section	Guidance
Session Title	Example: “Recognising and Responding to Phishing and Scams with Empathy”
Risk Area Focus	Select 1–2 risk areas (e.g., phishing, cyberbullying, misinformation).
Youth Profile	Describe the target group (e.g., rural youth, neurodivergent learners, migrant youth).
Learning Objectives	Example: “By the end of this session, participants will be able to identify phishing red flags and practise self-regulation to avoid impulsive clicks.”
Blended Phases	Outline activities for Connect–Explore–Practice–Reflect–Share , including tools (e.g., Kahoot for quizzes, Padlet for reflections) and EI prompts (e.g., “How would you feel if you fell for this scam?”).
Accessibility Actions	List adaptations (e.g., subtitles for videos, printed materials for malware/privacy discussions, multilingual resources).
Evaluation Methods	Specify how you’ll assess knowledge (quiz), skills (role-play), and emotional outcomes (reflection journal).

Example Use: A facilitator planning a session on **cyberbullying and digital empathy** would use this template to ensure the session includes **EI techniques, UDL adaptations, and blended activities**.

Annex B: UDL & Accessibility Checklist

Purpose: A **checklist** to ensure all sessions are **inclusive and accessible** for diverse learners, including those with **disabilities, limited digital access, or language barriers**.

Contents:

Criteria	Yes/No	Notes/Adaptations
Multiple Means of Engagement		Are there interactive, collaborative, and self-paced options for phishing/scams activities?
Multiple Means of Representation		Are materials available in text, audio, and visual formats (e.g., videos with subtitles for fake news discussions)?
Multiple Means of Expression		Can participants share reflections via writing, speaking, or art (e.g., Padlet for cyberbullying stories)?
Low-Tech Alternatives		Are printed worksheets or offline discussions available for malware/privacy topics?
Cultural Relevance		Do examples reflect diverse experiences of impersonation or cyber predators ?
Emotional Safety		Are there opt-out choices for sensitive topics (e.g., regretful posts, cyberbullying)?
Language Clarity		Is language simple and neutral for discussions on scams or fake friend requests ?

Example Use: Before delivering a session on **misinformation**, a facilitator would use this checklist to confirm that **videos have subtitles, discussions include opt-outs, and examples are culturally relevant**.

Annex C: Reflection Journal Prompts

Purpose: A **set of prompts** to guide participants' **weekly reflections** on their **emotional experiences** related to the **eight online risk areas**.

Contents:

Week 1: Cyberbullying and Digital Empathy

- “Describe a time you saw or experienced **cyberbullying**. How did it make you feel? What would you do differently now?”
- “How can empathy change the way we communicate online?”

Week 2: Phishing and Scams

- “What emotions might make someone vulnerable to a **phishing email or scam**? How can self-regulation help?”
- “Share a time you almost clicked a suspicious link. What stopped you?”

Week 3: Fake News and Misinformation

- “How did you verify a piece of information this week? What challenges did you face?”
- “Why do you think **fake news** spreads so quickly? How can we slow it down?”

Week 4: Privacy and Regretful Posts

- “What’s one piece of personal information you regret sharing? How did it affect you?”
- “How can we support friends who’ve shared something they regret?”

Week 5: Malware and Cyber Predators

- “What steps do you take to avoid **accidental malware downloads**? How do you feel when you’re unsure about a link?”
- “How can you recognise and respond to a **cyber predator**?”

Example Use: Participants use these prompts in their **e-journals** to reflect on their **emotional responses** to online risks, fostering **self-awareness and safer behaviors**.

Annex D: Evaluation & Inclusion Grid

Purpose: A **grid** to evaluate the **effectiveness, inclusivity, and emotional impact** of sessions addressing the **eight online risk areas**.

Contents:

Evaluation Area	Indicators	Tools/Methods
Knowledge	Can participants identify phishing red flags or spot fake news ?	Pre/post quizzes, Kahoot scores.



Skills	Can participants respond empathetically to cyberbullying or verify sources ?	Role-play observations, Padlet responses.
Attitudes	Do participants show increased empathy or critical thinking about online risks?	Reflection journals, group discussions.
Inclusion	Were all participants engaged , regardless of background or ability?	UDL checklist, participation logs.
Emotional Impact	Did participants feel safe and supported during discussions on scams or malware ?	Emotional check-ins, anonymous feedback.
Digital Competence	Can participants use digital tools (e.g., Padlet, Kahoot) to learn about online risks?	Platform analytics, self-assessments.

Example Use: After a session on **impersonation and scams**, a facilitator would use this grid to assess whether participants **recognised scams**, **responded empathetically**, and **felt included** in the activities.

Annex E: Youth Profile Samples

Purpose: **Sample profiles** of youth with diverse backgrounds, abilities, and digital access levels to help facilitators **design inclusive sessions**.

Contents:

1. Rural Youth with Limited Digital Access

- **Challenges:** Slow internet, limited devices.
- **Adaptations:** Printed materials, offline discussions on **privacy risks** or **malware**.

2. Neurodivergent Learner

- **Challenges:** Sensory overload, need for clear instructions.
- **Adaptations:** Visual schedules, quiet spaces for **cyberbullying** or **scams** activities.

3. Migrant Youth with Language Barriers

- **Challenges:** Limited proficiency in the session's language.

- **Adaptations:** Multilingual resources, peer buddies for **fake news** or **phishing** discussions.

4. Urban Youth with High Digital Literacy

- **Challenges:** Overconfidence in online safety.
- **Adaptations:** Advanced scenarios (e.g., **deepfake impersonation**, **complex scams**).

Example Use: A facilitator planning a session on **fake friend requests** would refer to these profiles to ensure activities are **accessible and engaging** for all participants.

Annex F: Peer-Mentor / Youth Ambassador Guide

Purpose: A **guide** for training **peer mentors** or **youth ambassadors** to support their peers in **recognising and responding** to the **eight online risk areas**.

Contents:

Section	Guidance
Role of a Peer Mentor	<i>"You're a role model! Your job is to share knowledge, listen, and support peers in staying safe online."</i>
Key Risk Areas	Overview of cyberbullying, phishing, scams, fake news, etc. with simple explanations .
EI Techniques	How to use empathy, self-regulation, and critical thinking in peer discussions.
Facilitation Tips	<i>"Use open-ended questions like, 'How did that scam attempt make you feel?'"</i>
Resources	Links to videos, quizzes, and helplines for further learning.
Safety Protocols	<i>"If a peer shares a cyberbullying experience, listen without judgment and offer to help them report it."</i>

Example Use: A youth ambassador would use this guide to lead a discussion on impersonation risks or support a peer who experienced cyberbullying.



Annexes Module 4

Annex 1: Handout_M4

Instructions for Participants:

Read each statement and mark the option that best describes you. Be truthful – this is for your own reflection, not a test. After filling it out, think about what surprised you and what you might want to improve. Discuss your insights with a peer or facilitator if you're comfortable.

When I receive an unexpected message or alert, I pause before responding.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I notice how I feel (curious, anxious, rushed) before clicking a link.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I verify unusual requests through a second source (friend, official support, etc.) rather than just trusting the message.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I recognise when emotion is used to make me act fast (for example, a message trying to scare or excite me).

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I ask for help or a second opinion when something seems "off" online.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I update my devices and apps regularly (install updates, patches).

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I limit what personal information I post publicly (like sensitive photos, full name, contact info).

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

When a mistake happens online (like I clicked something I shouldn't), I can stay calm and try to fix it instead of hiding it out of fear.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I support friends when they face online stress or scams (for example, I help them report abuse or I warn them if I notice something fishy).

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

I take short breaks from screens to reset emotionally, especially if I notice I'm stressed or upset.

☐ Almost Always ☐ Sometimes ☐ Rarely ☐ Never

Interpretation (This isn't a "score," just guidance):



- If you marked “Almost Always” or “Sometimes” for most items, you already show good awareness and habits in many areas. Identify which “Rarely/Never” you had and focus on those as growth points.
- If you marked “Rarely” or “Never” for several items, that’s okay – it means you have clear areas to improve. Pick one or two to work on first (trying to change everything at once can be hard).

My Insights: (fill in after completing the above)

The emotion that most often drives me online is: _____ (e.g., curiosity, boredom, FOMO, anger...).

One situation where I feel least in control online is: _____ (e.g., late at night on social media, when arguing in comments, when I see breaking news...).

My personal “pause and check” signal will be: _____ (What cue will remind you to pause? e.g., “When I notice I feel nervous/excited, I will take a breath,” or “If something says ‘urgent’, that’s my sign to double-check.”).

A support partner or friend who will remind me to be safe is: _____ (name someone you trust to nudge you, e.g., “I asked my brother to remind me if I’m getting too angry at games.”).

My Micro-Goal for This Week: (Choose one or two small actions to practice)

- ☐ Practice pausing before clicking on something suspicious or exciting.
- ☐ Ask one peer or adult for a second opinion on something strange I receive.
- ☐ Adjust one privacy setting on my social media (or remove something I regret posting).
- ☐ Try the 4-4-6 breathing exercise when I feel stressed by an online situation.
- ☐ Other: _____ (be specific: e.g., “Enable 2FA on my main accounts,” “Take a 1-hour break from Instagram each evening,” etc.)

(Keep this somewhere you’ll see it. You can even share your goal with a friend so they can check in on you. Small steps lead to big changes!)

Annex 2: Threat Recognition Scenario Cards

Purpose: These cards provide quick scenarios highlighting emotional manipulation in digital communication. Use them to help participants identify the emotion trigger and formulate safe responses.

(Each card lists a trigger category, an example message, the intended emotion, and a model safe response.)



Trigger 1 – Urgency

- Message: “Your account will be suspended in 30 minutes unless you confirm your password here: [malicious link]”
- Emotion Targeted: Anxiety / Fear of loss
- Safe Response: “This looks urgent, but I won’t rush. I’ll go directly to the app/website to check my account status – not clicking that link.”

Trigger 2 – Fear

- Message: “⚠ Security Alert: Someone tried to access your photos! Send this 6-digit code NOW to secure your data.”
- Emotion Targeted: Panic / Fear
- Safe Response: “I’m concerned, but I won’t send any code via message. I’ll open my account settings myself to see if there’s an alert. Real services don’t ask for codes like this via DM.”

Trigger 3 – Empathy

- Message: “Please, my friend’s child is in the hospital and needs urgent surgery. We’re collecting donations – just click here to help, even €5 would mean a lot.”
- Emotion Targeted: Compassion / Guilt
- Safe Response: “I’m sorry to hear that. I only donate through verified charities or people I personally know. I won’t click this link – I’ll consider other ways to help if I can verify this story.”

Trigger 4 – Authority

- Message: “[Admin]: This is the school IT department. Your account was flagged. Send your password so we can fix the issue, or you will be locked out.”
- Emotion Targeted: Obedience / Pressure from authority
- Safe Response: “I can’t share my password. If there’s an issue, I’ll speak to the IT department directly through official channels. (Also noting: Real admins never ask for passwords.)”

Trigger 5 – Opportunity/Reward

- Message: “🎉 Congrats! You’ve won a new iPhone in our giveaway! Just pay a €2 shipping fee here to claim within 1 hour.”
- Emotion Targeted: Excitement / Greed (and FOMO – fear of missing out)
- Safe Response: “If this were real, I shouldn’t have to pay. It sounds too good to be true, so it probably is. I’m not clicking anything or sending money.”

Trigger 6 – Curiosity

- Message: “Hey, check this out! Someone posted a really embarrassing video of you 😳. It’s going viral: [link]”
- Emotion Targeted: Curiosity / Insecurity
- Safe Response: “This message is trying to freak me out. I won’t click the link. I’ll reach out to my friend or go directly to the platform to see if there’s actually a video – but I suspect this is fake.”

(Facilitator Tip: Encourage participants to generalise these responses. The exact words might differ, but the pattern is: don’t comply with the emotional push, verify through another method, and respond (or not respond) in a way that doesn’t give the attacker what they want.)

Annex 3: Cyber Detective Case Files

Purpose

Each file contains a narrative and evidence pieces. Give teams time to analyse and respond.

Case 1 – The Contest Message

Narrative: You receive an Instagram DM from an account named “Natl_TalentAwards2025” claiming: “Congratulations! You’re a finalist in the National Youth Talent Competition. To claim your prize, please confirm your identity by clicking the link and uploading a photo ID within 24 hours.” You vaguely recall entering an online singing contest, but you’re not sure if this is the same one. The message has flashy emojis and the account has no verified badge.

Evidence: (a) Screenshot of the DM text. (b) Profile snippet of “Natl_TalentAwards2025” – 3 posts, 0 followers, following 200. (c) The link in the message is a bit.ly short URL.

Tasks for team:

- List at least 3 red flags in the message or profile (e.g., unverified account, low follower count for a “national” contest, shortened link, sense of urgency, asking for ID which contests usually don’t require via DM).
- How can you verify if this contest is real? (e.g., Check the official website of the National Youth Talent Competition – was there such a contest? Did they announce finalists publicly? Does the official site link to this Instagram account? Or message a friend who also entered the contest.)



- Decide: Do you click the link or not? Do you respond, and if so, what do you say? Or do you report this? (Probably: do not click, do not send ID. Likely fake/phishing. A safe action: find official contact info for contest organisers if you truly think it might be real and ask them. Response could be minimal or none. Reporting the account to Instagram as spam could be a call.)
- Reflection after solving: Which emotion did this attempt use? (Possibly excitement/pride at “winning” and urgency.) How did your team keep those emotions in check?

Case 2 – The Friend in Need

Narrative: You get a message from your friend Jenny via Instagram: “Hey... I’m travelling and I lost my wallet 😞. I’m stuck and need some money for a ticket to get home. Could you send like \$100 through PayPal? I’ll pay you back next week, promise!” It indeed is Jenny’s Instagram username, and you recognise her profile picture. But something is off – Jenny is usually very formal in writing, and this message seems a bit out-of-character (plus, you didn’t know she was abroad).

Evidence: (a) Screenshot of the Instagram DM conversation – in it “Jenny” also says not to call her because her phone was stolen (another excuse). (b) Your actual friend Jenny’s Instagram profile shows a slightly different username (the one messaging you has an extra underscore). (c) WhatsApp log: you have a separate chat with the real Jenny from yesterday where she said nothing about travel.

Tasks for team:

- Spot the differences that indicate this might not be your friend (impostor account with a nearly identical username? Hacked account? Check profile details, last posts, etc.).
- What steps do you take to confirm if Jenny is really in trouble? (e.g., Try to call or text her on her regular number; contact a mutual friend or her parents; ask a question only the real Jenny would know; check if the message language feels right.)
- Draft a polite refusal or safe reply to the Instagram message (or decide not to reply at all) that doesn’t burn bridges in case it is her but still protects you. E.g., “Jenny, I’m so sorry! I wish I could help. Can I reach out to your mom for you?” (A scammer might back off or get angry; a real friend would say “sure” or explain more.) Or simply, “I can’t send money but I’ll try to get in touch another way to verify you’re okay.”



- Should you report this account or situation? (Yes, likely report the impersonation/fraud to the platform once confirmed fake.)
- Reflection: What emotional trigger was at play? (Empathy and urgency). How did having a verification habit save you from potentially losing money? How would you feel if you had sent money then found out it was fake – does that motivate being cautious?

Case 3 – The Fake Job Offer

Narrative: You receive an email that appears somewhat professional at first glance: it's from "GlobalDataEntry Inc." offering you a remote part-time job for \$500/week, flexible hours. They found your profile on LinkedIn (you did put you're seeking opportunities). They say to proceed, they need you to fill a form (attached) and also send a scanned copy of your ID and a void cheque for direct deposit setup. The email has some generic phrasing and a few grammar mistakes. The sender's email is .

Evidence: (a) Email text screenshot. (b) Attachment "JobApplicationForm.pdf" (if you provide, it could be a very basic form asking for name, address, bank account number, etc.). (c) If one googles "GlobalDataEntry Inc." nothing legit comes up, or one finds a forum post about job scams. (If offline, you can provide a mock "search result" printout showing it's not on LinkedIn or has scam reports.)

Tasks for team:

- Highlight inconsistencies or warning signs in the email (e.g., salary too high for simple work, unusual request for ID and bank info so early, Gmail address not corporate, grammar issues, company not findable online, they didn't have a personal greeting or interview step).
- How to verify if this job offer is real? (e.g., Search the company name + "scam"; check the company's supposed website domain – oh, there is none; look at the sender email domain – why Gmail if a company? ask on LinkedIn or forums if anyone heard of it.) Possibly even email back with a question – but that might just get a scammer to persist, so likely not engaging is fine.
- Decision: Respond with requests for verification (like "Can we schedule a phone call? Can you send official contract?"), or decide to ignore? If convinced it's fake, maybe no reply or a polite decline, and possibly report the email as phishing. If uncertain, proceed with extreme caution and without sending personal docs until sure – but generally, this scenario is a known scam pattern.



- What do you do with the attachment? (Ideally don't open it – could be malware. Or open in a secure way – sandbox or phone – but better to avoid.)
- Reflection: Discuss how greed/excitement (easy high pay) and maybe flattery (“we found you, you’re chosen”) could cloud judgment. What cognitive tricks did the scammers use? (Pressure by saying act fast to secure position, appeal to financial need.) How does verifying and taking time protect you from identity theft in this case?

(Feel free to create additional cases, e.g., a phishing website scenario, a malware-infected USB found, a sextortion attempt, etc., depending on what threats you want to practice. Be mindful of the group’s maturity and comfort.)

This document was developed with contributions from the project team. Some sections of the text were reviewed and edited with the support of artificial intelligence (AI)-based tools, in order to improve clarity and coherence. Final responsibility for the content lies with the authors.



EM&M

EMotional intelligence & cybersecurity
environMents in youth education

Partnership:

Asociatia De Dezvoltare Economico-Sociala (**ADES**) - Coordinator, Romania

KAINOTOMIA & SIA EE - Partner, Greece

LABC S.R.L. - Partner, Italy

STOWARZYSZENIE CENTRUM WSPIERANIA EDUKACJI I
PRZEDSIĘBIORCZOŚCI (**CWEP**) - Partner, Poland

E&D KNOWLEDGE CONSULTING, LDA - Partner, Portugal

"**PRAMMER**" Wissens Stadtinstitut Zur Sozialforschung Verein Zur Förderung
Der Partizipativen, Mediativen Und Sozialen Entwicklung Und Die Vermittlung
Von Künstlerischen, Sportlichen, Gesundheitlichen, Kulturellen,
Wirtschaftlichen, Wissenschaftlichen - Partner, Austria



**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 National Agency for Community Programmes in the Field of Education and Vocational Training (ANPCDEFP). Neither the European Union nor the ANPCDEFP can be held responsible for them.

Project Reference Number: 2024-2-RO01-KA220-YOU-000293190



EM&M

EMotional intelligence & cybersecurity
environMents in youth education



KAINOTOMIA
κέντρο διά βίου μάθησης



LABC



Centrum Wspierania
Edukacji
i Przedsiębiorczości



E&D Knowledge
Consulting

PRAMMER



© 2026. This work is openly licensed via [CC BY-NC-ND](https://creativecommons.org/licenses/by-nc-sa/4.0/)



Co-funded by
the European Union