



SAFE CHANGES

Social Awareness and Financial, Emotional
Connecting Headways for the Advancement
of New Generations' Electronic Safety



SAFE CHANGES TRAINING TOOLKIT

A guide for social workers on internet
safety and in conducting activities and
workshops for youth with a special focus
on Italy, Turkiye, Lebanon, Tunisia and
Algeria.

Edited by
Isabella Chiari & Alessia Pierro



Co-funded by the European Union. The views
expressed are solely those of the author(s)
and do not necessarily reflect those of the
European Union or the granting authority.
Neither the European Union nor the granting
authority can be held responsible for them.



**Co-funded by
the European Union**



SAPIENZA
UNIVERSITÀ DI ROMA





Project Coordinator
Isabella Chiari

This Safe Changes Toolbook has been developed by Sapienza University of Rome as part of the SAFE CHANGES project, with the goal of equipping youth workers, educators, and facilitators with practical tools and structured guidance to address key topics related to digital safety. The main authors are Isabella Chiari (Sapienza University) and Alessia Pierro (Amal for Education), with contributions from Emre Sönmez on cybersecurity, Fiorenza Deriu on soft skills, and collaboration from staff members of partner organizations in Türkiye, Lebanon, Tunisia, and Algeria for the development of infomaps

and the adaptation of modules to diverse local contexts.

The Toolbook offers structured chapters on cybersecurity, social risks online, internet addiction, and information trustfulness, each accompanied by real-life examples, checklists, and interactive activities. It is designed to be practical, adaptable, and rooted in participatory methods that empower young people to reflect critically on their digital lives and strengthen their digital resilience.

The project

SAFE CHANGES is a collaborative initiative designed to promote digital safety, critical thinking, and responsible online behavior among young people in Italy, Türkiye, Lebanon, Tunisia, and Algeria. These regions face growing challenges such as online harassment, disinformation, internet addiction, and unequal digital literacy. Under the coordination of Sapienza University of Rome, SAFE CHANGES addresses these challenges through a structured and participatory approach that combines education, peer engagement, and creative expression.

The project begins with the co-design of learning content and shared priorities across countries, resulting in a set of educational modules tailored to the digital realities of youth. These modules focus on key areas such as cybersecurity, social risks, internet addiction, and information trustfulness.

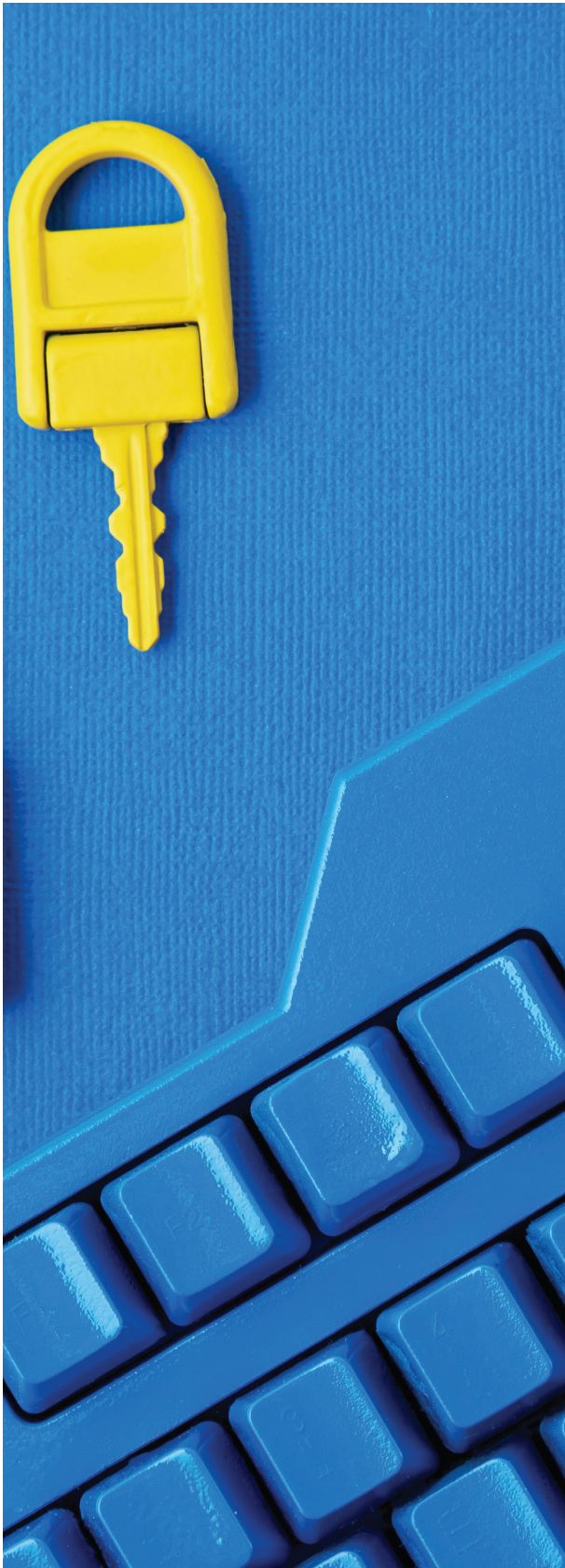
A core training program then prepares **240 youth workers**

and facilitators, who are equipped to lead local and cross-border activities. Through a series of virtual exchanges and in-person workshops, these trained facilitators engage over **960 young people aged 13–25** in interactive, youth-led sessions. Activities promote awareness, digital responsibility, and peer learning through storytelling and critical dialogue. Special attention is given to inclusion, gender sensitivity, and adapting to different social contexts.

Key deliverables of the project include:

A **Digital Safety Toolkit**, designed for facilitators working with youth; A collection of **Storytelling Modules**, created bottom-up by young participants and reflecting their lived experiences in digital spaces; A **Best Practice Guide**, capturing effective methods and lessons learned; A **series of short videos**, co-produced by young people, highlighting key messages from each topic addressed.

CONTENTS



1. MODULE: CYBERSECURITY

1. Topics in Cybersecurity

- 1.1 Personal Data Protection**
- 1.2 Phishing and scams**
- 1.3. Password Security**

2. MODULE: INTERNET ADDICTION

2. Topics in internet addiction

- 2.1. Introduction on internet addiction**
- 2.2 Developing Healthy Digital Habits**

3. MODULE: SOCIAL RISKS

- 3.1. Personal Harm and Harassment**
- 3.2. Manipulation and Deception in Digital Relationships**

4. MODULE: INFORMATION TRUSTFULNESS

- 4.1 Source credibility**
- 4.2. Misinformation and Disinformation**

5. MODULE: INFOMAPS AND VISUAL AIDS

- 5.1 Visual Aids and Infographics**
- 5.2 How to Use InfoMaps in Training Sessions**
- 5.3 Customizing Visual Aids for Your Audience**
- 5.4 How to build an evaluation test**

5. HOW TO USE THIS TOOLKIT

- 5. 1. Implementing the the toolkit**
 - 5. 1.1. Introduction: From Theory to Practice**
 - 5.1.2. Categories of Activities in the Toolkit**
 - 5.1.3. Facilitator Guidelines for Implementation**

This Safe Changes Toolkit has been developed withing the project SAFE CHANGES – Promoting Digital Safety through Youth Participation and Virtual Exchange project, co-funded under the Erasmus+ Programme– Grant Agreement No. 101112181.

Co-funded by the European Union. The views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Module 1: Cybersecurity



INTRODUCTION TO CYBERSECURITY

Objectives

Equip participants with foundational knowledge of cybersecurity essentials.

KEY CONCEPTS

Cybersecurity involves protecting internet-connected systems such as hardware, software, and data from cyber threats. This practice is crucial not only to safeguard personal and organizational data from attacks but also to ensure privacy, prevent identity theft, and protect against malware and viruses.

KEYWORDS

Cybersecurity
Phishing
Malware
Encryption
Firewalls

Every time we go online, whether to chat with friends, post on social media, play games, or do schoolwork, we are sharing information and data. That information, even when it feels private, can be seen, stored, and sometimes even stolen. Cybersecurity is about protecting our digital lives: our personal information, our accounts, and our online activities from threats and attacks.

In this module, you'll learn what cybersecurity means and why it matters for young people. You'll explore how online risks, like hacking, phishing, and data leaks, can affect your privacy, your identity, and your safety.

You'll discover simple habits that make a big difference: creating strong passwords, spotting suspicious links, setting up two-factor authentication, and knowing when something online doesn't seem right. These are skills anyone can learn, no technical background needed.

Most importantly, this module will help you feel more confident and in control of your online presence. By learning how to protect yourself and others, you become part of a safer, more respectful digital community.

The activities included in this module are designed to be flexible and adaptable. They can be tailored to different age groups and adjusted to fit the cultural and social realities of each local context. Facilitators are encouraged to adapt examples, language, and delivery methods to ensure the material resonates with the participants and supports meaningful engagement.



1. TOPICS IN CYBERSECURITY



1.1 Personal Data Protection

Personal data protection is crucial for youth navigating the digital world, as it safeguards their personal information from misuse and potential harm. Understanding how to protect personal data empowers young individuals to maintain their privacy and security online.

What is Personal Data?

Personal data refers to any information that can identify an individual, either directly or indirectly. This includes:

Direct Identifiers: Name, address, phone number, email address.

Indirect Identifiers: Date of birth, photographs, social media posts, IP addresses.

Why is Personal Data Protection Important?

Protecting personal data is essential because:

Privacy Preservation: Maintains control over personal information and who has access to it.

Prevention of Identity Theft: Reduces the risk of someone fraudulently using personal information.

Safety Assurance: Protects against stalking, harassment, and other forms of online abuse.

Approximately **79% of individuals aged 15 to 24 are internet users**, surpassing the 66% usage rate among the general population. As digital technologies become integral to various aspects of young people's lives, including education, they encounter both unique opportunities and challenges online. It's crucial to ensure that efforts to protect youth from online risks do not inadvertently restrict their access to valuable opportunities. Instead, these initiatives should aim to both safeguard and empower young individuals, enabling them to develop autonomy and resilience over time.

Research indicates that adolescents often have a limited understanding of online privacy and the implications of sharing personal information. Many young people value privacy but may trade it off for perceived benefits on social media platforms. The privacy paradox illustrates this phenomenon: while youths express concern about privacy, they frequently share significant amounts of personal information online.

The legal landscape surrounding children's data protection varies by region. In the United States, the Children's Online Privacy Protection Act (COPPA) mandates parental consent for collecting data from children under 13 years old. In contrast, the General Data Protection Regulation (GDPR) in Europe requires parental consent for children under 16. However, once adolescents reach these age thresholds, they are treated similarly to adults regarding data privacy rights.



Sharing personal data online can lead to several significant risks. One of the primary dangers is **identity theft**, where cybercriminals use personal information—such as names, addresses, and birthdates—to impersonate individuals for fraudulent activities. This can result in unauthorized financial transactions and damage to one's credit reputation.

Another concern is **financial fraud**. Sensitive data, like credit card numbers or banking details, can be exploited for unauthorized purchases or withdrawals, leading to direct financial loss. Additionally, oversharing personal information can make individuals more susceptible to **phishing attacks** and **scams**, where attackers craft convincing messages to deceive victims into revealing confidential information.

Privacy invasion is also a significant risk. Information shared on social media platforms can be accessed, collected, and misused by malicious entities, leading to unwanted exposure or harassment. For instance, sharing real-time location data or personal routines can make individuals vulnerable to **cyberstalking** or physical stalking.

Moreover, sharing personal information online can lead to **reputational damage**. Inappropriate or sensitive content shared publicly can be accessed and misused, potentially affecting personal and professional relationships. It's crucial to be mindful of the long-term implications of online posts, as they can be difficult to remove once shared.

To mitigate these risks, it's essential to be cautious about the personal information shared online and to utilize privacy settings to control access to your data. Regularly reviewing and updating these settings can help maintain control over personal information and reduce exposure to potential threats.



“ Consider Alex, a college student who enjoys sharing his daily experiences on social media. One day, he posts a photo of his new credit card to celebrate his first step into financial independence, inadvertently revealing his card number and personal details. Cybercriminals quickly exploit this information, making unauthorized purchases and causing significant financial loss for Alex. This incident highlights the importance of being cautious about sharing sensitive personal information online, as it can lead to identity theft and financial fraud. ”

“ Mia is a high school student who enjoys sharing her life on social media. Excited about her upcoming birthday, she posts a photo of her new driver's license, inadvertently revealing personal details like her full name, birthdate, and home address. A cybercriminal comes across this information and uses it to create fake identification documents. Posing as Mia, the criminal gains unauthorized access to various services, including renting apartments and purchasing items online, all under Mia's name. Unaware of these activities, Mia is later confronted with unexpected bills and legal notices for actions she didn't commit. This experience highlights the importance of safeguarding personal information online to prevent identity theft and its serious consequences. ”



✓ PERSONAL DATA PROTECTION CHECKLIST

- ☐ Avoid sharing full names, birthdates, addresses, phone numbers, school names, or other personal details in online profiles.
- ☐ Adjust privacy settings on social media platforms to control who can view your information and posts.
- ☐ Ensure that images or videos don't reveal personal information, such as school uniforms, identifiable landmarks, or sensitive documents.
- ☐ Refrain from posting your current location or daily routines, as this can expose you to potential risks.
- ☐ Never share passwords, even with close friends, and use strong, unique passwords for each account.
- ☐ Do not share personal information in response to unexpected messages or friend requests from unknown individuals.
- ☐ Consider the long-term impact of your posts. Once information is online, it can be challenging to remove.
- ☐ Stay informed about online privacy practices and regularly review the privacy policies of the platforms you use.





Activity 1: “Spot the Overshare”

KEYWORDS

Social media, privacy, oversharing, personal data, risks.

OBJECTIVES

To help participants recognize oversharing and its risks.
To foster critical thinking about online behavior and data protection.

DURATION

30–45 minutes.

PARTICIPANT AGE

13–18 years old.

MATERIALS AND TOOLS

Printed or digital mock social media profiles/posts.
Discussion prompts or checklist for analyzing oversharing risks.
Projector or screen (if presenting examples as a group).

Description of Activity:

Participants will review a set of simulated social media profiles or posts containing varying levels of personal information. Their task is to identify which posts or profiles are oversharing personal data and explain the potential risks associated with each example.

Facilitator Instructions:

Prepare mock social media profiles or posts with varying levels of personal information (e.g., a profile sharing a home address, a birthday post showing an ID card, a travel post with location tagging).

Divide participants into small groups and distribute the examples.

Ask each group to analyze the examples and discuss the potential risks of oversharing in each case.

Facilitate a group discussion to share findings and discuss safer posting habits.

Suggestions for Facilitators:

Encourage open discussion by asking questions like, “What risks do you think this person might face?”

Ensure a non-judgmental atmosphere where participants feel comfortable sharing their thoughts.
Provide concrete advice on improving privacy settings and habits based on participants’ observations.



PERSONAL DATA PROTECTION - ACTIVITIES

Activity 2: “Data Detective Simulation”

KEYWORDS

Personal data, online profiles, information security, cyber risks.

OBJECTIVES

To illustrate how personal data can be gathered from online profiles.

To teach participants strategies to protect their own information online.

DURATION

40–50 minutes.

PARTICIPANT AGE

15–24 years old.

MATERIALS AND TOOLS

Printed or digital mock profiles.
Data checklist for each participant or group.
Pens and paper for notes (group).

Description of Activity:

Participants will play the role of “data detectives,” attempting to gather as much personal information as possible from a set of mock online profiles. Afterward, they will reflect on how easily personal data can be collected and discuss strategies to protect their own information.

Facilitator Instructions:

Prepare mock online profiles with varying levels of personal information (e.g., posts sharing a name, school name, or photos with location tagging).

Give participants a checklist of personal data points to “hunt” for in the profiles (e.g., name, location, birthdate).

After the activity, lead a discussion about what was found, how it could be used maliciously, and how to avoid oversharing in the future.

Suggestions for Facilitators:

Emphasize the learning aspect, avoiding any judgment of participants’ own online behavior.

Encourage participants to think about how they can make their profiles more secure.

Offer actionable tips for improving privacy settings on popular platforms.





1. TOPICS IN CYBERSECURITY

1.2 Phishing and scams

For a safe internet experience, young people should be careful of scam messages or emails. Understanding how to protect young individuals from these threats empowers them to maintain their privacy and security online.

What is Phishing?

Phishing is a type of online scam that targets people through the delivery of emails that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. These types of emails generally ask to provide personal identifying information, which the scammer will then use to open new accounts, or invade the person's existing accounts.

Phishing - also referred to as “password harvesting fishing” - is an attempt to acquire sensitive information, such as usernames, passwords and credit card details, by pretending to be a trusted source in an email or message.

Scam messages may ask you to “update”, “validate”, or “confirm” your account information. Some phishing emails may try to scare you by threatening things like closing your account if you don't respond.

Why is it crucial to protect ourselves from phishing and scams?

1. **Financial Security:** Phishing and scams often aim to steal sensitive financial information, such as bank account details or credit card numbers. This can lead to unauthorized transactions, financial loss, or even drained savings.
2. **Identity theft prevention:** Scammers use personal information obtained through phishing to impersonate victims, leading to identity theft. This can have long-term consequences, such as fraudulent loans, damaged credit scores, and legal complications.
3. **Safeguarding privacy:** Phishing attacks often target private data, such as login credentials or personal communications. Protecting against these threats ensures your sensitive information doesn't fall into the wrong hands, preventing misuse or exploitation.

According to a [survey done by the European Commission](#), 56% of the adult population has been the victim of online fraud attacks in the last two years.

In the same report, the most common scams and frauds methods used by criminals are as follows:

1. Fraudulent lottery/prize promotions – 28%
2. Impersonation fraud – 22%
3. Fraudulent computer/internet problem – 21%
4. Promises in return for transferring/investing money – 14%
5. Requests to pay because there are problems with an account/documentation – 12%

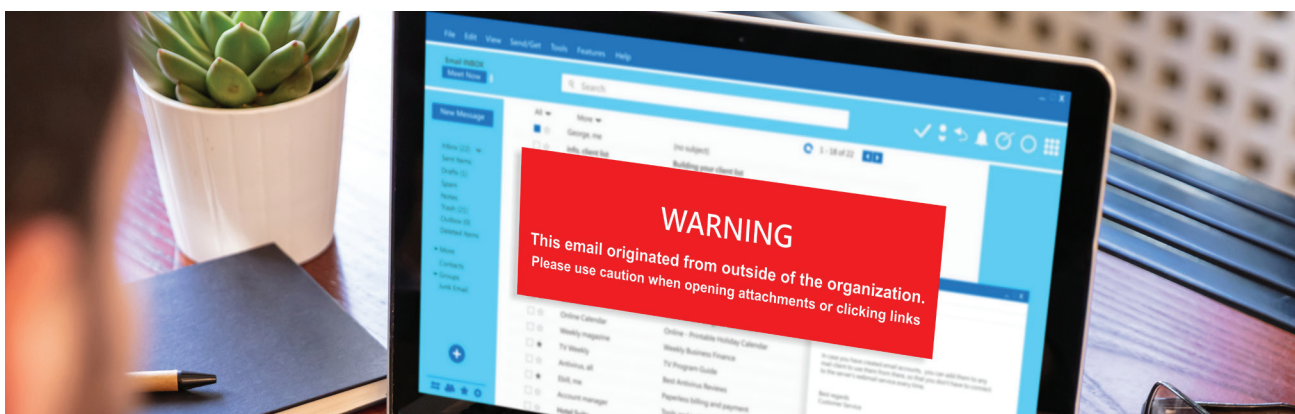


Recognition of scam emails or messages by young individuals is essential for a safe internet experience.

First, legitimate organizations have their own **email domains and email accounts**. For example, an email you receive from a bank cannot be sent through a public email domain such as @gmail.com or @hotmail.com.

The second thing you should pay attention to is the presence of **misspelling errors** in the domain name. For example, let's say the legitimate domain name of the bank we use is @safebank.com. Cybercriminals can carry out phishing attacks with misspelled domain names that resemble legitimate domain names, such as @sefebank.com or @safebenk.com.

The third point to be noted is that phishing emails generally include **a file or a website link that contains a virus**. In case the file or link is accidentally downloaded, don't worry: the antivirus programs on our electronic devices will protect you from these attacks and block them from infecting your laptop or mobile. For this reason, it is important to keep the antivirus software active and up to date.





“ When Salem checks his emails, he sees an email from his bank. The email says that his account has been hacked and that he can protect it by clicking on the attached link. Panicking, Salem clicks on the link without doing the necessary security checks and his phone gets a virus. Since he didn't use an antivirus program, the virus gets on his phone and the hacker gets all his information. When Salem checks his email later, he sees that the email is not from his bank but from his personal email address. ”

“ Merve works at a bank and uses the computer and e-mail address provided by the bank itself. The computer can access the accounts of bank customers thanks to the programs it contains. One day, an email arrives, stating that she needs to update the program and that she needs to download the file extension attached in the email immediately. When Merve looks at the domain address, she thinks it is legitimate, but she does not realize that the domain address is misspelled. She downloads the file and runs it despite her computer's warning. The file contains a remote access trojan virus. This virus, which infects the computer, allows hackers to control the computer remotely. Hackers who infiltrate the bank's system through Merve's computer seize the accounts of many bank customers. Due to this situation, the bank suffers from great financial difficulties and Merve loses her job. ”



✓ PHISHING AND SCAMS CHECKLIST

- ☐ Take time to reflect on a request for your personal information and whether the request is appropriate.
- ☐ Do not open unsolicited email from people unfamiliar to you or click on suspicious attachments, which you did not expect.
- ☐ Never supply any personal or financial information and passwords to anyone via email.
- ☐ Avoid emails that insist you act now.
- ☐ Check the sender's name, email address and whether the email domain matches the organisation that the sender claims to be from.
- ☐ Keep an eye out for spelling and grammatical mistakes.
- ☐ Protect your devices. Install anti-spam, anti-spyware and anti-virus software and make sure they are always up to date.





Activity 1: “Spot the Scam”

KEYWORDS

Phishing, scams, online security, personal data, email safety.

OBJECTIVES

To help participants recognize phishing emails and scam messages.

To develop critical thinking about email security and personal data protection.

DURATION

30–40 minutes.

PARTICIPANT AGE

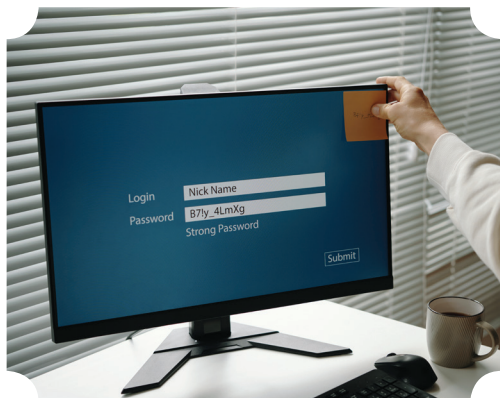
13–18 years old.

MATERIALS AND TOOLS

Printed or digital examples of phishing emails/messages.

A checklist of red flags for identifying phishing emails.

Projector or screen (if presenting examples as a group).



PHISHING AND SCAMS - ACTIVITIES

Activity 2: “Phishing Detective Simulation”

KEYWORDS

Phishing, scams, email safety, critical thinking, online security.

OBJECTIVES

To illustrate common phishing tactics and how they work.
To teach participants strategies to verify legitimate emails and messages.

DURATION

40–50 minutes.

PARTICIPANT AGE

15–24 years old.

MATERIALS AND TOOLS

Printed or digital examples of phishing emails/messages.
A phishing red flags checklist for each participant or group.
Pens and paper for notes.



Description of Activity:

Participants will act as “phishing detectives” tasked with investigating simulated scam emails or messages to uncover their tactics. Afterward, they will reflect on how scammers attempt to deceive people and how to protect themselves from such attacks.

Facilitator Instructions:

1. Prepare mock phishing emails or messages that include a variety of deceptive tactics, such as:

- ☐ Misspelled domain names (e.g., @safebenk.com).
- ☐ Requests for urgent action (e.g., “Your account will be suspended if you don’t respond in 24 hours”).
- ☐ Suspicious links or attachments.

2. Provide participants with a checklist to “hunt” for red flags, such as:

- ☐ The email domain’s authenticity.
- ☐ Spelling and grammar errors.

3. After the activity, lead a group discussion about what was found, how scammers exploit human behaviour, and how participants can protect themselves.

Suggestions for Facilitators:

Emphasize the importance of staying vigilant and skeptical of unsolicited messages.

Encourage participants to share their own experiences with suspicious emails or messages.

Offer practical advice, such as using antivirus software, checking for TLS encryption, and avoiding clicking on unknown links.



Explore how people protect themselves from phishing attacks.

Facilitators play a crucial role in stimulating meaningful discussions and encouraging participants to share personal stories or anecdotes about themselves or others they know. Begin the discussion with general, relatable questions to ease participants into the topic, such as, “**Are you aware of the importance of phishing attacks**” or “**Why should people be aware of phishing attacks?**”. The purpose of these open-ended questions is to encourage participants to join the discussion. As the discussion progresses, participants are encouraged to share their own stories through more personal questions. For example, participants are asked to describe their personal experiences by asking if they or someone close to them has ever been subjected to phishing attacks.

Participants and listeners who share their personal experiences are asked questions about their experiences, and participants are expected to make connections between what they learned in class and their personal life experiences. In addition, participants are encouraged to apply the protection methods learned during the course to their own personal experiences. They are guided through reflective questions, such as, “**What actions could you take to protect yourself from phishing attacks in similar situations?**” Participants are then tasked with applying the protection strategies they’ve learned to realistic, practical scenarios.

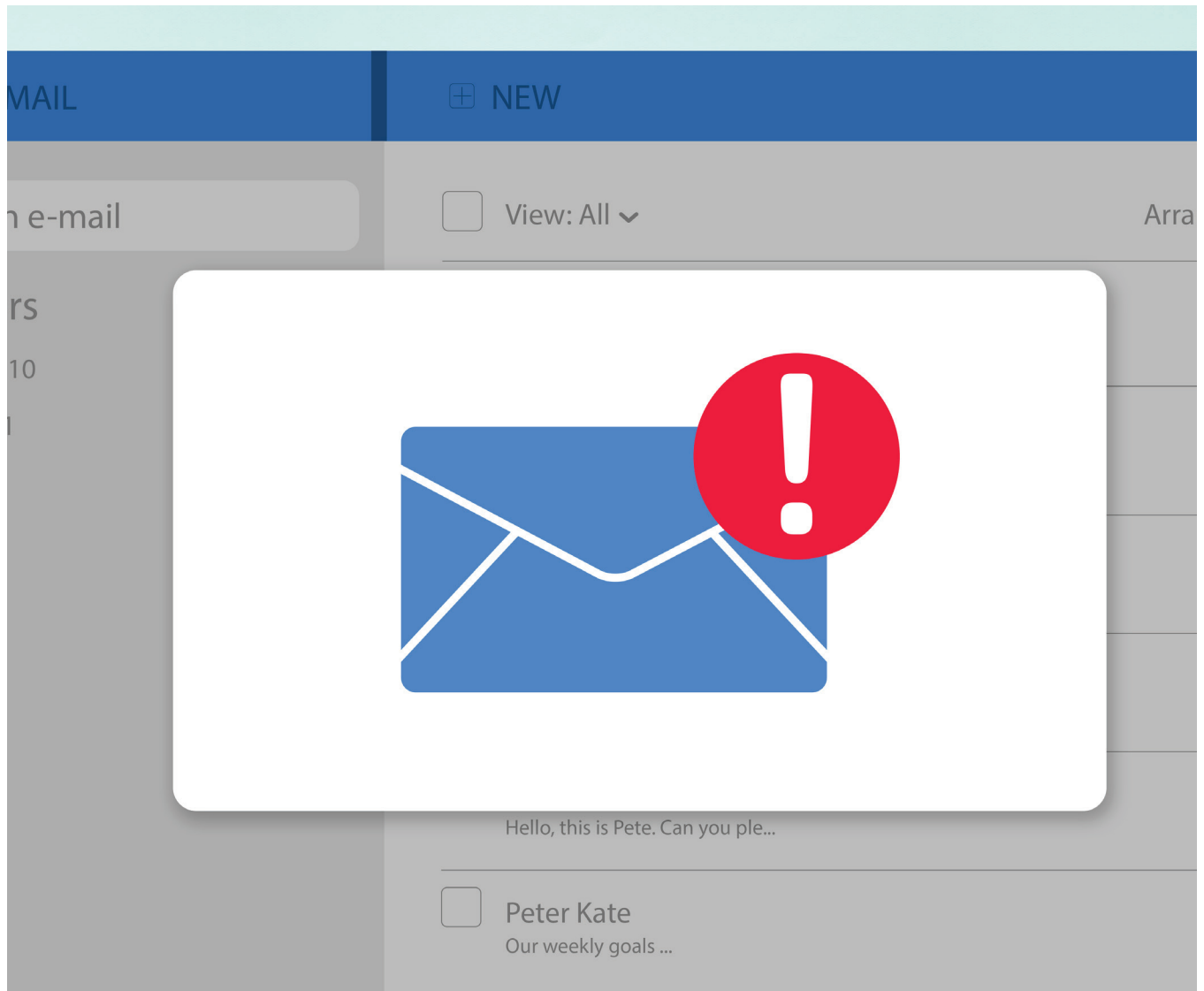
Throughout the discussion, validate participants’ contributions by actively listening, summarizing key points, and showing appreciation for their input. Avoid interrupting and gently redirect the discussion if it goes off-topic. To conclude, summarize the shared stories and insights, highlighting actionable lessons and emphasizing the importance of protecting personal data.

E-BOOKS

- ▶ Comprehensive Anti-Phishing Guide. [Download here](#) 
- ▶ The Little Book of Scams. [Download here](#) 

WEBSITES

- ▶ Phishing Scams and Fraudulent Emails. <https://www.eui.eu/ServicesAndAdmin/ComputingService/EMail/PhishingScamsAndFraudulentEMails> 
- ▶ Understanding and dealing with phishing during the COVID-19 pandemic. <https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic> 





1. TOPICS IN CYBERSECURITY

1.3. Password Security

One of the things that young people need to learn to protect themselves from the dangers of the digital world is password security. Understanding the importance of password security allows young individuals to protect their privacy and security online.

What is a password?

A password is a secret word or combination of letters, numbers, and symbols that you can use to protect your information and prove your identity when accessing something, like an account or device. If only numbers are allowed in a password, it's usually called a Personal Identification Number (PIN).

A password doesn't have to be a real word—it can be a mix of random letters, numbers, and symbols, which makes it harder for others to guess.

Not taking password security seriously may cause several problems. A [study on the state of password security in 2024](#) reveals that 30% of internet users have experienced a data breach due to a weak password.

Indeed, easily guessable passwords can make it easier for hackers to access our digital data stored online. Be aware that, no matter how strong the password is, hackers might find a way to access our information. For this reason, it is good practice to change our passwords every once in a while to better protect our privacy. [Figures](#) show that 44% of internet users rarely change their passwords, and 43% have shared a password with someone, which can lead to unauthorized access.

Why is Password security important?

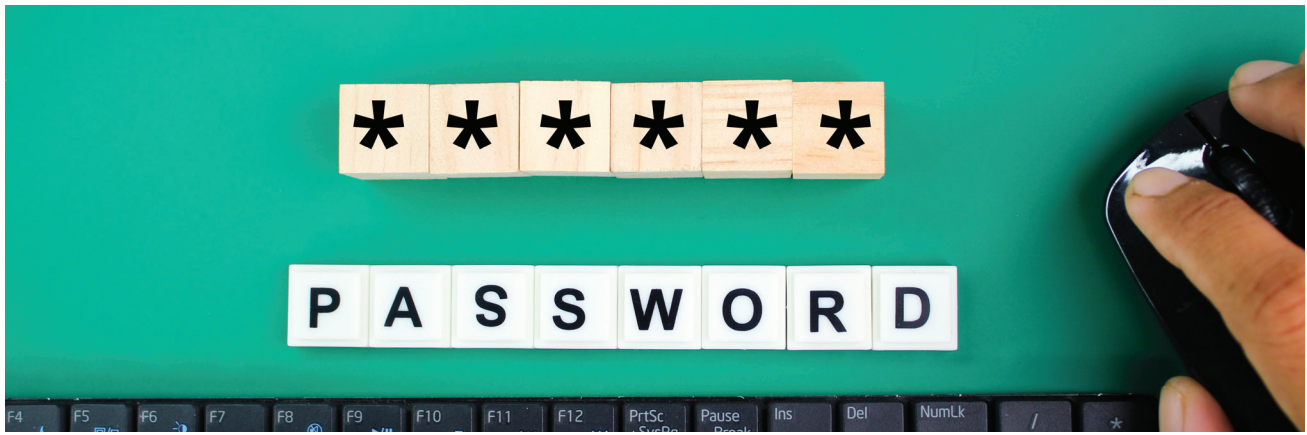
Protecting online passwords is essential to:

Safeguard Personal Data: Strong passwords significantly reduce the likelihood of unauthorized access to sensitive information, such as financial details or confidential communications.

Prevent Identity Fraud: Keeping your passwords strong helps stop hackers from pretending to be you online, protecting your personal reputation and money.

Maintain System Integrity: Good password practices contribute to the overall security of digital environments, preventing large-scale breaches and limiting the spread of malicious software.

Hackers try to get people's passwords using many methods. For example, brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. Hackers often try the most common passwords on thousands of accounts, and this may just be enough to let them break into at least some of them. Passwords leak can have different levels of gravity,



affecting a few thousands to billions of accounts like during the attack [RockYou2024](#). For this reason, protecting our account with a password that cannot be easily guessed is the first step.

According to the EU Science Hub, a strong password is essential for online security, and the principle “the longer, the better” serves as a useful rule of thumb. It is important to avoid using obvious references, such as names, significant dates, or locations, as these are easier for hackers to guess.

Randomness plays a critical role in password security since it makes it unpredictable and therefore more difficult to crack. The more you will mix letters, numbers, and special characters, the hardest the password will be to decipher. Malicious individuals often attempt to exploit systems by trying all possible combinations up to a certain length or relying on common passwords, making unpredictability an absolute necessity for effective password protection. Moreover, using the same password on different websites can harm our digital security since hackers can easily access many of your accounts with the same code. For this reason, it is important to use different passwords for each account.

However, remembering different passwords can be difficult. For this reason, software that provides password security such as lastpass and google authenticator can be used. These types of tools increase our security and help us use different passwords for different accounts. Although these measures provide us with a certain level of protection, hackers can access our passwords using more complex methods. For example, downloading a file without knowing the source or the content can expose our devices like laptops and mobile phones to viruses.

Two-Factor Authentication (2FA) is a security method that enhances protection by requiring users to verify their identity using two distinct factors before accessing an account, system, or service. These factors typically fall into three categories: something you know, such as a password or PIN; something you have, like a smartphone, hardware token, or security key; and something you are, such as biometric data like a fingerprint or facial recognition.



“ Consider Ahmet, a bit lazy when it comes to online security, who uses the same password, “Password123,” for every website. One day, a friend calls to check on him, asking if everything is alright. During the call, hackers exploit Ahmet’s weak password practices, gaining access to all his social media accounts. They impersonate Ahmet, sending messages to his friends claiming he is in trouble and urgently needs money. Unfortunately, some of his acquaintances believe the messages and send money, thinking they are helping him. Ahmet’s neglect of basic password security ends up not only compromising his accounts but also causing harm and financial loss to those around him. ”

“ Fatma uses complex passwords to secure her bank account but neglects to enable the bank’s recommended two-factor authentication. In a moment of carelessness, she downloads an email attachment she believes is from her workplace, unknowingly infecting her phone with a virus. Later, when she attempts to access her bank accounts, she discovers that all her passwords have been changed and that unauthorized cryptocurrency purchases have been made using her account. Fatma’s oversight in enabling two-factor authentication ultimately compromises her financial security. ”





Activity 1: “Password Strength Assessment”

KEYWORDS

Password strength, online security, weak passwords, strong passwords, complexity.

OBJECTIVES

To help participants identify weak passwords and understand how to create strong, secure ones.

DURATION

30–40 minutes.

PARTICIPANT AGE

13–18 years old.

MATERIALS AND TOOLS

Printed or digital lists of example passwords.
Guidelines or checklist for evaluating password strength.

Description of Activity:

Participants will review a series of mock passwords with varying levels of complexity. Their task is to evaluate the strength of each password and identify which ones are weak or strong, explaining why. They will also suggest ways to improve weak passwords.

Facilitator Instructions:

Prepare a list of mock passwords, including weak (e.g., “password123,” “john2023”), moderate (e.g., “J0hn@2023”), and strong examples (e.g., “J@hn#2023&*”). Divide participants into small groups and provide the list for review.

Ask each group to discuss the weaknesses and strengths of the passwords and suggest improvements for the weaker ones.

Facilitate a group discussion to consolidate the findings and introduce tips for creating strong passwords.

Suggestions for Facilitators:

Encourage creativity in password improvement suggestions while emphasizing randomness and length. Highlight common pitfalls, such as using personal information or common words. Share additional tools, like password managers, to support secure password practices.



PASSWORD SECURITY - ACTIVITIES

Activity 2: “2FA in Action”

KEYWORDS

Two-Factor Authentication, online security, account protection, password security.

OBJECTIVES

To show how 2FA prevents unauthorized access.
To encourage participants to enable 2FA for their online accounts.

DURATION

40–50 minutes.

PARTICIPANT AGE

15–24 years old.

MATERIALS AND TOOLS

Mock user accounts (password-only and 2FA-enabled).
Mock 2FA methods (e.g., printed codes or phone verification).

Description of Activity:

Participants will explore how Two-Factor Authentication (2FA) protects accounts by comparing scenarios with and without 2FA. They will see firsthand how 2FA adds an extra layer of security.

Facilitator Instructions:

Setup: Create two simple scenarios: one with password-only protection and one with 2FA enabled. Use mock user accounts with easy-to-guess passwords (e.g., “Password123”).

Activity Execution: Divide participants into pairs or small groups. Simulate a password breach for the password-only account (e.g., using hints like “favorite pet’s name”).

For the 2FA-protected account, introduce a second step (e.g., providing a mock verification code that only the account owner has). Let participants observe how 2FA stops unauthorized access even when the password is guessed.

Discussion: Discuss why 2FA made the second account harder to breach. Highlight how 2FA works (e.g., a code sent to a phone or email). Encourage participants to share their thoughts on how they could use 2FA in their own accounts.

Suggestions for Facilitators:

Keep the activity simple and interactive, focusing on the contrast between the two scenarios.

Explain that enabling 2FA is easy and can prevent serious risks.

Provide a quick demonstration of how to set up 2FA on a popular platform.

Offer actionable tips for improving privacy settings on popular platforms.





Explore why people should be aware of password security.

Facilitators play a crucial role in stimulating meaningful discussions and encouraging participants to share personal stories or anecdotes about themselves or others they know. Begin the discussion with general, relatable questions to ease participants into the topic, such as "What are the common ways hackers can crack people's password? or Have you ever come across a victim whose accounts were reached by hackers? These open-ended questions encourage reflection and make it easier for participants to share personal experiences or observations about others.

As the discussion progresses, try to pose deeper questions like: **"What steps should we take to ensure password security?"** or **"What are some risks you've heard of related to weak passwords?"**. To stimulate storytelling, prompt participants with scenario-based questions such as, **"Can anyone share an example of a time when someone's password's security is violated?"** and **"What happened, and what did they learn?"** or **"Have you ever seen someone use a weak password, and what advice would you give them now?"** Use follow-up questions to explore the stories further, such as, "What could have been done differently to avoid the problem?"

Throughout the discussion, validate participants' contributions by actively listening, summarizing key points, and showing appreciation for their input. Avoid interrupting and gently redirect the discussion if it veers off-topic. To conclude, summarize the shared stories and insights, highlighting actionable lessons and emphasizing the importance of password security.

E-BOOKS

▶ Protect yourself online [Download here](#) 

▶ Tips for Teens: Password Safety. [Download here](#) 

WEBSITES

▶ Password Safety: Top Ten Tips for Teens. <https://cyberbullying.org/password-safety-top-ten-tips-for-teens> 

Nick Name

B7!y_4LmXg

Strong Password

Module 2: Internet addiction



INTRODUCTION ON BALANCING YOUR DIGITAL LIFE

Objectives

Raise awareness among young people about internet addiction, its signs and consequences, and to promote healthier digital habits through critical reflection and practical strategies.

KEY CONCEPTS

Definition and forms of internet addiction, difference between intensive use and problematic use, psychological and social consequences, impact on sleep and attention, behavioral signs of addiction, emotional and psychological factors, self-regulation strategies, role of family and peers, healthy digital habits, time management tools.

KEYWORDS

Internet addiction, screen time, digital wellbeing, compulsive behavior, online habits

Today, we use the internet for almost everything—studying, working, watching videos, chatting with friends, and playing games. While the internet is full of opportunities, sometimes we end up spending more time online than we planned, and it can start to affect other parts of our lives. This module will help you explore the fine line between normal internet use and when it might become a problem.

You will learn what internet addiction means and how it is different from just using your phone or computer a lot. We will talk about how it can affect your sleep, your focus at school, and your relationships with family and friends. Sometimes, people turn to the internet to escape stress, boredom, or loneliness—without realizing that it can create more problems over time.

Throughout the activities, you will discover common signs of internet addiction, such as constantly checking your phone, feeling nervous when you're offline, or losing track of time when scrolling. These signs can be easy to miss, but once you recognize them, you can start to build better habits.

Together, we will also look at simple strategies to manage your time online in a healthier way. This includes understanding your own digital habits, finding a balance between screen time and offline activities, and supporting each other to make positive changes. This is not about giving up the internet—it's about using it wisely and making sure it doesn't control you.

You will also have access to resources to deepen your knowledge and to use simple tools that help assess the level of internet addiction—whether you are supporting others as a facilitator or reflecting on your own use as a peer leader.



2. TOPICS IN INTERNET ADDICTION



2.1. Introduction on internet addiction

Internet Addiction Disorder (IAD) refers to the compulsive or poorly controlled use of the internet that interferes with daily life, relationships, or emotional well-being. It involves excessive time spent online—whether gaming, scrolling social media, or browsing—despite negative consequences. Often compared to behavioural addictions, IAD includes symptoms like preoccupation, withdrawal, and neglect of responsibilities, and calls for awareness and strategies to promote healthier digital habits.

What are the risk factors?

Some young people may be more at risk of internet addiction than others, based on:

- ☐ Emotional or psychological factors: Feelings of loneliness, social anxiety, depression, or low self-esteem can drive people to seek comfort and escape online.
- ☐ Lack of offline engagement: When young people don't have access to offline activities, such as hobbies, sports, or face-to-face socialization, they may turn to the internet to fill the void.
- ☐ Family or social environment: Environments where internet use is unrestricted or where adults model excessive screen time may increase the likelihood of developing IAD.
- ☐ Platform design: Many websites, apps, and games are intentionally designed to keep users engaged for as long as possible through features like autoplay, endless scrolling, and reward notifications.

Why is it important to recognize internet addiction?

Uncontrolled internet use can affect a young person's health, education, and relationships resulting in a huge impact on personal wellbeing. Some key consequences include:

- 1. Physical health issues:** Extended screen time can cause sleep disturbances, headaches, eye strain (computer vision syndrome), poor posture (such as “tech neck” and spinal strain), carpal tunnel syndrome from repetitive device use, and an overall lack of physical activity.
- 2. Emotional and social effects:** IAD may lead to irritability, mood swings, and social withdrawal and isolation, leading to loneliness and weakened interpersonal skills. Excessive screen time can also strain family relationships, as youth become less engaged in family activities, causing tension, conflicts, and a sense of disconnection within the household.
- 3. Mental health struggles:** Overuse can worsen anxiety and depression, creating a cycle where online use becomes a coping mechanism rather than a healthy activity, especially when online interaction fosters comparison and dependency on virtual validation.
- 4. Sleep disturbances:** Prolonged screen use — particularly late at night — disrupts the body's circadian rhythm through blue light exposure, suppressing melatonin and contributing to irregular sleep patterns and insomnia. This cycle of poor sleep can impair focus, mood, and overall health.
- 5. Academic decline:** Excessive time online — especially on gaming or social media — can replace homework, studying, and sleep, diverting focus from academic responsibilities. This often results in missed deadlines, lower grades, reduced productivity, and overall



poor school performance.

Internet Addiction Disorder (IAD) is a growing concern in many countries, particularly among young people. As technology becomes more accessible and embedded into everyday life, understanding what drives internet overuse – and how it affects youth – has become a major focus for educators, psychologists, and researchers.

A [2021 Pew Research study](#) found that 48% of U.S. adults aged 18–29 said they are online almost constantly, compared to 42% of those aged 30–49, 22% of those 50–64, and just 8% of adults 65 and older. This highlights how younger adults are significantly more connected than older generations. Globally, according to the [Digital 2024 report](#), the average internet user globally spends approximately 6 hours and 40 minutes online each day, with the highest worldwide score registered in the age range 16–24 with 7 hours and 30 minutes.

Among internet users aged 16 to 24, social networks (96.9%) and chat and messaging apps (96.4%) are the most visited digital platforms. Other popular categories include search engines (82.6%), online shopping (72.9%), and music streaming (55.9%).

Recent studies have shown that certain psychological and environmental conditions make some adolescents more vulnerable than others. A [study by the National Institutes of Health](#) (2012) explains that individuals with symptoms of depression, anxiety, and low self-esteem are significantly more likely to develop compulsive patterns of internet use. These patterns often serve as emotional coping mechanisms. Internet platforms provide temporary relief from stress or negative emotions, but over time, they reinforce avoidance, creating a cycle of dependence. The same study found similarities between internet addiction and impulse-control disorders, including symptoms like loss of control,



withdrawal, and continued use despite knowing the negative consequences.

Globally, researchers are also noticing regional patterns. A 2024 study published in [Academia Open](#) reviewed 22 recent studies to assess internet addiction among Middle Eastern students. The findings indicate a high prevalence of internet addiction, which is significantly correlated with mental health disorders, such as anxiety and depression, and negatively impacts academic performance.

The structure of the internet itself also plays a role. Social media platforms, video-sharing apps, and online games are intentionally designed to maximize engagement. Features like endless scrolling, variable reward systems, and autoplay functions stimulate dopamine in the brain, triggering the same neural responses seen in gambling and substance addiction. This makes it particularly difficult for adolescents – whose brains are still developing self-control and decision-making skills – to regulate their use without support.

The long-term impact of internet addiction goes beyond just time spent online. Research shows that persistent overuse can affect the brain's prefrontal cortex-responsible for attention, decision-making, and emotional regulation. [MRI studies](#) reveal that heavy users show reduced grey matter in key regions, which may contribute to impulsive behavior, poor concentration, and mood instability. These neurological effects echo the patterns found in other behavioral addictions and raise concerns about the potential developmental consequences of IAD when left unaddressed.

Beyond the biological and academic effects, IAD takes a social toll. Teens with internet addiction may begin to withdraw from friends and family, preferring online interactions to face-to-face ones. This shift can impair communication skills, reduce empathy, and increase loneliness. Ironically, though they're more connected than ever, many young people report feeling isolated – driven by online comparisons, FOMO (fear of missing out), or pressure to maintain a constant presence.

Altogether, the findings point to a multifaceted problem. Internet addiction is not just about too much screen time – it's about why people are turning to the internet in the first place and what they're missing offline. The data makes it clear: without proper awareness, boundaries, and support systems, digital use can easily slip into harmful patterns. Fortunately, recognizing the risks is the first step toward preventing long-term harm and helping youth find a healthier balance in their digital lives.





“ Omar, a 17-year-old student, used to scroll through TikTok every night before bed. What started as 15 minutes turned into hours. He began sleeping less, feeling tired in class, and missing homework deadlines. When his grades dropped, his teacher asked what had changed. That conversation made Omar realize his phone habits were affecting more than just his sleep. With support, he set screen-time limits and started sleeping better – and learning better, too.”

“ Lina, 16, found comfort online during a tough year. She was always on Instagram and Discord, avoiding social events in real life. Over time, her friendships faded, and she felt more alone than ever. After missing a friend’s birthday and seeing it only online, Lina felt left out and anxious. She decided to take a break from social media and focus on reconnecting offline. Slowly, she rebuilt her confidence and felt more present with the people around her. ”

“ Ahmed loved online games. What started as a weekend hobby became daily marathons. He skipped meals, ignored family time, and once even forgot an exam. After getting in trouble at school and home, he realized his gaming had taken over. He talked to a counsellor who helped him create a routine with game-free hours. Now, Ahmed still enjoys gaming – but without letting it control his life. ”



✓ INTERNET ADDICTION CHECKLIST

- ☐ Notice changes in routine such as skipping meals, sleep, or important activities to stay online
- ☐ Watch for mood changes when not connected, including irritability, anxiety, or restlessness
- ☐ Check for secrecy, like hiding screen time or lying about how long you've been online
- ☐ Observe social withdrawal, preferring digital interactions over time with family or friends
- ☐ Pay attention to performance, such as declining grades or missed responsibilities due to internet use
- ☐ Reflect on control and whether you feel unable to cut back even when trying to limit usage
- ☐ Look for loss of interest in hobbies or activities that were once enjoyable





Activity 1: “Online or Overboard?”

KEYWORDS

Self-awareness, digital behaviour, peer discussion, critical thinking

OBJECTIVES

To help participants identify the differences between healthy internet use, overuse, and addiction.

To encourage critical thinking and open dialogue around digital habits.

To raise awareness of the impact of internet use on daily life and responsibilities.

DURATION

30–40 minutes.

PARTICIPANT AGE

13–19 years old.

MATERIALS AND TOOLS

Scenario cards/slides, coloured cards or digital voting tool, discussion prompts

Description of Activity:

Participants will be given a set of realistic online behaviour scenarios and asked to decide whether the behaviour reflects healthy use, overuse, or addiction. This activity encourages reflection and discussion on digital habits in a relatable and non-judgmental way.

Facilitator Instructions:

- ☐ Prepare 6-8 behaviour cards or slides with example scenarios (e.g., “Spends 7 hours a day gaming and skips homework,” “Uses social media 1 hour daily and puts phone away during meals”).
- ☐ Read each scenario aloud or show it on a screen.
- ☐ Ask participants to hold up coloured cards (e.g., green = healthy, yellow = overuse, red = possible addiction) or vote using a digital tool like [Mentimeter](#), [Slido](#), [Strawpoll](#), [Poll Everywhere](#), or [Jotform](#).
- ☐ Facilitate a short discussion after each scenario to explore why they made their choice.

Suggestions for Facilitators:

Use relatable, age-appropriate examples that reflect different types of internet use (e.g., gaming, social media, streaming).

Avoid labelling or judging—emphasize that this activity is about learning, not blaming.

Encourage participants to reflect on their own habits and ask, “Have I ever done something similar?”

Consider grouping participants for small peer discussions before sharing with the whole group.



INTERNET ADDICTION - ACTIVITIES

Activity 2: “My 24-Hour Digital Day”

KEYWORDS

Time awareness, self-reflection, screen-time habits, balance

OBJECTIVES

To increase participants' awareness of their daily digital habits.

To help visualize the balance (or imbalance) between online and offline activities.

To promote self-reflection as a first step toward healthier time management.

DURATION

30 minutes.

PARTICIPANT AGE

12–18 years old.

MATERIALS AND TOOLS

Printed worksheets or digital templates, colored pens or markers, optional projector for sharing examples.

Pens and paper for notes. (group).

Description of Activity:

Participants will reflect on how they spend their time in a typical day and visually map out their digital and non-digital activities. This helps raise awareness of how much of their daily life is spent online and encourages self-reflection on their digital routines.

Facilitator Instructions:

Distribute worksheets or digital templates that represent a 24-hour day (either a clock-style or timeline format).

Instruct participants to fill in the chart using different colours for digital (e.g., gaming, social media, browsing) vs. offline activities (e.g., school, meals, sports, sleep).

Once completed, invite participants to observe which parts of their day are most tech-heavy and reflect:

“Where does most of your screen time go?”

“Is anything surprising?”

“What might you want to change?”

Encourage volunteers to share their reflections with the group.

Suggestions for Facilitators:

Emphasize that this is a personal exercise – there are no “right” or “wrong” answers.

Create a comfortable atmosphere for sharing, but don't pressure anyone to discuss their chart if they prefer to keep it private.

If time allows, repeat the activity later in the program to let participants track changes in their habits.

Use this as a gentle lead-in to the next topic on prevention and healthy habits, showing how awareness is a first step toward positive change.





Explore why being aware of internet addiction symptoms is crucial for your wellbeing.

Start with general, relatable prompts to help participants ease into the discussion:

“Have you ever realized you spent more time online than you meant to?”

“What are some ways the internet helps us? What are some ways it might cause stress or problems?”

“Do you think it’s easy or hard to recognize when screen time becomes ‘too much’? Why?”

As the conversation develops, ask more reflective and thought-provoking questions:

“Why do you think people sometimes use the internet to escape their emotions or responsibilities?”

“Have you ever noticed your mood changing – feeling angry, tired, or anxious – after being online for a long time?”

“Do you think internet overuse can affect friendships or family time? How?”

“What makes it hard for people to cut down on screen time, even if they want to?”

To encourage storytelling and real-life connections, use situational prompts:

“Have you ever stayed up late online and then struggled the next day at school or work?”

“Can you think of someone (maybe a friend or yourself) who was constantly online – what were the effects?”

“Imagine you had to go a full day without the internet. What would that feel like?”

Open discussion for participants to ask questions or clarify doubts.

E-BOOKS

 Teacher’s Guide. Internet addiction [Download here](#) 

WEBSITES

 Youth Portal – Better Internet for Kids. <https://better-internet-for-kids.europa.eu/en> 

 Be Internet Awesome – Google. https://beinternetawesome.withgoogle.com/it_it 

Facilitators play a crucial role in guiding the discussion, helping participants connect the topic of internet addiction to their personal experiences and daily habits.

Start by creating a supportive and non-judgmental environment where everyone feels comfortable sharing. Encourage open dialogue by asking relatable, low-pressure questions like, **“Have you ever noticed yourself spending more time online than you planned?”** or **“Why do you think people turn to their phones when they’re stressed?”**

If the discussion drifts off-topic, guide it back by referring to the central theme, using encouraging transitions such as, **“That’s interesting – how do you think that connects to how we use the internet every day?”** Remind participants that this is not about blame or judgment, but about understanding and reflection.

To wrap up the session, invite participants to reflect on what they’ve learned by asking open-ended questions like, **“What’s one thing that stood out to you from today’s discussion?”** or **“Is there a small change you’re thinking about making after this conversation?”** These prompts allow individuals to consolidate their learning and leave the session with a sense of personal insight.





2. TOPICS IN INTERNET ADDICTION

2.2 Developing Healthy Digital Habits

As internet use becomes increasingly embedded in daily life, especially among youth, it's more important than ever to develop healthy digital habits. Prevention and mitigation strategies aim not only to reduce the risk of internet addiction but also to empower young people with the skills, awareness, and routines necessary for a balanced and mindful relationship with technology.

What are healthy digital habits?

Healthy digital habits are the choices and routines that help you use technology in a way that supports your well-being, rather than interfering with it. It's not about giving up the internet—it's about using it with intention, balance, and awareness.

Creating tech-life balance isn't about strict rules—it's about learning how to use technology in a way that adds to your life, not takes from it. Examples of what healthy digital habits include:

- ☐ **Setting Daily Screen Limits:** Try to keep non-school screen time to about 1-2 hours per day for young people and around 2-3 hours of leisure screen time per day for adults. Apps like [StayFree](#), [Screen Time](#) or [Digital Wellbeing](#) can help track and limit use.
- ☐ **Creating Tech-Free Zones:** Avoid screens during meals, in the bedroom, or during social time with friends and family.
- ☐ **Using Technology Intentionally:** Before opening an app, ask yourself: "What am I using this for?" This helps reduce mindless scrolling.
- ☐ **Taking Regular Breaks:** Follow the 20-20-20 rule: every 20 minutes, take a 20-second break to look at something 20 feet away. This helps protect your eyes and keep you focused.
- ☐ **Prioritizing Offline Activities:** Make space for non-digital hobbies—like drawing, sports, reading, or spending time outside—to stay balanced and fulfilled.
- ☐ **Being Aware of Design Traps:** Apps and websites are built to keep you hooked. [Virtual Addiction](#) highlights how features like infinite scrolling, autoplay, and "likes" are designed to trigger dopamine responses and prolong usage. Recognizing these patterns helps you stay in control of your time and how you want to spend it.

Healthy digital habits don't happen in isolation – they're much easier to build and sustain when young people feel supported by the adults around them. Parents, caregivers, teachers, and youth workers all play a vital role in guiding and reinforcing balanced digital behaviour. When support systems are consistent, caring, and informed, young people are more likely to develop a positive relationship with technology.

A 2024 study in the [Journal of Family Social Work](#) showed that when parents or caregivers set consistent expectations, stay involved, and lead by example, the risk of internet overuse drops significantly. This shows how important it is for adults to not only talk about balance



but also practice it in their daily lives.

One of the most effective ways adults can help is by introducing the “digital hygiene” concept and setting clear, age-appropriate routines around screen use. For example, households can establish “tech-free” times, such as no phones after 9 PM or no devices during family meals. In school settings, teachers might encourage breaks from screens during class or incorporate non-digital activities into the day. These boundaries reduce screen fatigue and also encourage time for face-to-face connection, rest, and reflection.

Open communication is just as important. Young people should feel safe discussing their online habits, the pressures they face on social media, or how certain digital spaces make them feel. Adults can create this space by asking non-judgmental questions like, “What’s your favorite way to relax online?” or “Have you ever felt overwhelmed by notifications or group chats?” Talking openly about digital life builds trust and allows early warning signs of overuse or distress to be recognized and addressed.

Self-assessment tools like [Young’s Internet Addiction Test](#) (IAT) can also be useful for encouraging honest reflection. Completing these together, or simply discussing the questions, can spark meaningful conversations about how time online affects emotions, relationships, and responsibilities.

Finally, adults should remember that actions speak louder than words. When young people see adults managing their own screen time responsibly – putting phones away during conversations, taking breaks from work emails, or choosing outdoor activities – they are more likely to follow that example. Healthy digital habits become part of a shared culture, not a set of rules imposed from above.



A 2012 [medical study](#) clearly shows that treating internet addiction isn't one-size-fits-all. Different people develop unhealthy digital habits for different reasons, so treatment works best when it's tailored to the individual. Some might need help managing anxiety or depression that fuels their internet use, while others benefit more from building better routines or improving family dynamics.

Cognitive Behavioral Therapy (CBT) is one of the most effective tools – it helps people recognize what triggers their behavior and replace it with healthier habits. In some cases, group therapy or family-based approaches are used to strengthen communication and support systems. For those with more severe symptoms, more structured treatment settings may be recommended.

The key is personalization: the best treatment meets the person where they are, addressing both their digital behavior and the emotional or social challenges behind it. In the end, building healthy digital habits is about creating balance, not perfection. With the right support and awareness, young people can learn to take control of their screen time and shape a relationship with technology that supports – not harms – their well-being.







“ Sarah used to check her phone the second she woke up – scrolling through messages and social media before even getting out of bed. It left her feeling rushed and distracted all day. After a school workshop on digital balance, she decided to keep her mornings screen-free until breakfast. The change was small, but it helped her start the day calmer and more focused. Now, she feels more in control of her time – and her mood. ”

“ Tarek’s family used to eat dinner with the TV on and phones at the table. They barely spoke. One day, his mom suggested a simple rule: no devices at dinner. At first, Tarek found it awkward. But soon, conversations returned. They laughed more, shared stories, and even started planning weekly game nights. That small change helped Tarek reconnect with his family – and spend less time glued to screens. ”

“ When Nour realized she was spending five hours a day on social media, she was shocked. She hadn’t noticed how much it had crept into her routine. Her counsellor introduced her to a screen-time tracking app. With it, Nour started setting daily limits and taking breaks. Within weeks, she found more time for drawing, reading, and seeing friends in person. Nour didn’t quit the internet – she just started using it on her terms. ”



✓ HEALTHY DIGITAL LIFE CHECKLIST

- ☐ Set daily limits for non-essential screen time using tracking apps like StayFree or Digital Wellbeing
- ☐ Create tech-free zones, especially during meals, in bedrooms, and during time with others
- ☐ Take regular breaks using the 20-20-20 rule to protect focus and eye health
- ☐ Prioritize offline activities such as sports, art, reading, or spending time outdoors
- ☐ Use technology intentionally by asking yourself why you're opening an app or site
- ☐ Encourage open conversations about digital life, online pressure, and personal experiences
- ☐ Use self-assessment tools like Young's Internet Addiction Test (IAT) to reflect on habits
- ☐ Model balanced screen behavior by limiting your own use and staying present in social moments





Activity 1: “Digital Habits Reflection Jar”

KEYWORDS

Reflection, screen time, emotional awareness, peer learning

OBJECTIVES

To encourage self-awareness around daily internet use.
To normalize the idea of struggling with digital balance.
To introduce simple, realistic strategies for change.

DURATION

30–40 minutes.

PARTICIPANT AGE

12–18 years old.

MATERIALS AND TOOLS

Paper slips or an online form, pens, a container or jar (physical or digital), optional whiteboard. For the online forms you can use tools like [Miro](#) and [Padlet](#).

Description of Activity:

Participants will reflect on their own digital habits by responding to thought-provoking prompts. They will anonymously place their responses into a “reflection jar” (or digital equivalent), which will be used to start a group discussion on screen-time routines, emotional responses, and balance strategies.

Facilitator Instructions:

☐ Prepare small slips of paper or a digital form with prompts like:

“One thing I do online that makes me feel good is...”

“One time I felt overwhelmed by screen time was...”

“One small habit I could try to improve my tech-life balance is...”

☐ Ask participants to write honest responses (no names) and place them in the jar or submit them online.

☐ Mix the responses and read them aloud to the group. Facilitate a calm and open discussion around the themes that emerge.

Suggestions for Facilitators:

Keep the tone supportive, not judgmental – this is about growth, not guilt.

Emphasize anonymity to help participants feel safe sharing honestly.

If time allows, invite participants to choose one positive habit they heard and try it for a week.

Use this activity as a soft entry into deeper conversations or the following checklist.



HEALTHY DIGITAL HABITS - ACTIVITIES

Activity 2: “One Day Offline Challenge”

KEYWORDS

Digital detox, mindfulness, offline, habit change

OBJECTIVES

To provide a real-life experience of digital disconnection.

To explore the benefits of offline time for focus, creativity, and mental well-being.

To help participants identify triggers for screen use and find alternatives.

DURATION

Planning: 30 minutes;

Reflection session: 30 minutes (held the day after the challenge)

PARTICIPANT AGE

13–19 years old.

MATERIALS AND TOOLS

Reflection journal/worksheet (printed or digital), pens, optional group discussion board or whiteboard

Description of Activity:

Participants will plan and later reflect on a 24-hour digital detox, focusing on replacing screen time with meaningful offline activities. The challenge encourages self-awareness and gives them a chance to experiment with healthier digital routines.

Facilitator Instructions:

Start by guiding the group in creating a personal offline plan for one day (outside school hours).

Ask participants to list activities they will do instead of using their devices – examples include reading, drawing, going for a walk, or spending time with family.

Give them a handout or digital journal page to log how they feel before, during, and after the challenge.

Schedule a follow-up session for participants to reflect and share what they noticed.

Suggestions for Facilitators:

Pairing this activity with activity 2: “My 24-Hour Digital Day”. Start with “My 24-Hour Digital Day,” then follow with this activity to deepen reflection.

Emphasize that the challenge is about trying, not succeeding perfectly – partial attempts still count.

Let participants choose their own time frame (e.g., 4 hours, an evening, or a full day).

Normalize struggle – some participants may find it hard, and that’s okay.

Use follow-up discussion to celebrate small wins and reinforce that even brief breaks from screens can have a big impact.





Help participants reflect on their own digital routines, explore the benefits of balance, and learn from each other's experiences. The aim is to normalize challenges around screen time and highlight simple ways to create better habits.

Start with light, relatable prompts to ease participants into the topic:

"What's the first thing you usually do when you wake up – does it involve a screen?"

"When do you feel most 'in control' of your screen use? When do you feel least in control?"

"What's one app or activity you could cut back on without missing much?"

As the conversation develops, ask more reflective and thought-provoking questions:

"Have you ever noticed how your mood changes depending on what you do online?"

"Why do you think it's so hard to take breaks from certain apps or games?"

"What's the difference between using the internet for fun and relying on it to escape stress?"

"Can you remember a time you felt proud of managing your screen time well?"

To encourage storytelling and real-life connections, use situational prompts:

"A student spends four hours a night on TikTok but says it helps them unwind. What might be the upside and the downside?"

"Someone tries to unplug but feels anxious or left out. How can we support people going through that?"

Open discussion for participants to ask questions or clarify doubts.

Facilitators play a crucial role in guiding the discussion, helping participants connect the topic of internet addiction to their personal experiences and daily habits. Start by creating

E-BOOKS

 Digital Fitness [Download here](#) 

 Digital Life Skills for Youth [Download here](#) 

WEBSITES

 Are You Tech Addicted? – British Council. https://learnenglishteens.britishcouncil.org/study-break/youtubers/are-you-tech-addicted?utm_source=chatgpt.com 

 UK Safer Internet Centre. https://saferinternet.org.uk/guide-and-resource/young-people/resources-for-11-19s?utm_source=chatgpt.com 

a supportive and non-judgmental environment where everyone feels comfortable sharing. Encourage open dialogue by asking relatable, low-pressure questions like, **“Do you think internet addiction is something that only affects certain people, or could it happen to anyone?”**.

If the discussion drifts off-topic, guide it back by referring to the central theme, using encouraging transitions such as, **“That’s interesting – how do you think that connects to how we develop healthy digital habits?”** Remind participants that this is not about blame or judgment, but about understanding and reflection.

To wrap up the session, invite participants to reflect on what they’ve learned by asking open-ended questions like, **“What’s one thing that stood out to you from today’s discussion?”** or **“Is there a small change you’re thinking about making after this conversation?”** These prompts allow individuals to consolidate their learning and leave the session with a sense of personal insight.



Module 3: Social risks



INTRODUCTION SOCIAL RISKS AND COMMUNICATION

Objectives

Equip young people with the awareness, knowledge, and strategies needed to recognize, prevent, and respond to harmful social interactions in digital spaces.

KEY CONCEPTS

Social risks include harmful online behaviors such as cyberbullying, grooming, and harassment. They can cause emotional, psychological, and physical harm. Manipulation, deception, and exposure to harmful content are common forms. Anonymity and lack of accountability increase risk. Empathy, digital boundaries, and support systems help prevent and address online harm.

KEYWORDS

Cyberbullying, grooming, online harassment, digital manipulation, harmful content

The internet gives us amazing ways to connect with others, share our thoughts, and learn new things. But not all online interactions are positive or safe. Sometimes, people use digital spaces to hurt, trick, or take advantage of others. These situations are called social risks—and they can be just as serious as problems we face in the real world.

In this module, we'll look at some of the most common social risks young people face online. These include cyberbullying (when someone uses the internet to harass or threaten others), grooming (when someone tries to gain trust in order to exploit you), online harassment, and other forms of manipulation or emotional harm. These experiences can be confusing, upsetting, and even dangerous—so it's important to know what they look like.

Social risks can happen on any platform—social media, games, group chats, or messaging apps. They often start out seeming harmless or even friendly. That's why learning to recognize red flags is key. This module will help you understand the warning signs and give you tools to stay in control of your digital life.

You'll also explore how online harm affects people emotionally and socially. Feeling anxious, isolated, or ashamed is a common reaction—but you're not alone. Talking about it and asking for help is a sign of strength, not weakness.

Finally, you'll learn what to do if you—or someone you know—is experiencing one of these risks. Whether it's blocking someone, saving messages, reporting abuse, or simply talking to a trusted adult, there are steps you can take.

This module is here to help you stay informed, stay safe, and support others. The more we talk about social risks, the better we can protect ourselves and create a kinder, more respectful online world.





3. TOPICS IN SOCIAL RISKS

3.1. Personal Harm and Harassment

The rise of digital communication has opened powerful avenues for learning and connection, but it has also brought new forms of harm. “Personal harm and harassment” in digital spaces refers to behaviors where individuals – often young people – are targeted, intimidated, or exploited emotionally or socially through online interactions. These actions can leave lasting effects on self-esteem, mental health, and even physical safety.

What are the risks?

Young people may face different types of personal harm online, including:

- ☐ **Cyberbullying and Online Harassment:** This includes spreading hurtful rumors, sending threatening messages, or sharing personal information or photos without consent. The harassment may be public (such as in comments) or private (via direct messages or through hate groups), but the impact is often deep and long-lasting.
- ☐ **Sexual Harassment and Revenge Porn:** Unwanted messages of a sexual nature, persistent advances, or sharing intimate images without consent can result in feelings of shame, isolation, and trauma. Girls and LGBTQ+ youth are particularly vulnerable. Revenge porn often involves former partners sharing content to humiliate or manipulate.
- ☐ **Trolling:** Online trolls aim to provoke or humiliate others through offensive comments or personal attacks. While some may treat it as “just a joke,” repeated trolling can escalate into serious emotional harm, especially when it targets someone’s appearance, identity, or beliefs.
- ☐ **Doxxing:** When someone’s personal data – like their address or school – is published online to shame or intimidate them, the threat becomes real and immediate. Victims may face harassment not only online but in their everyday lives.
- ☐ **Cyberstalking:** Some individuals are repeatedly followed, monitored, or messaged online in ways that create fear or distress. This often includes unwanted messages, impersonation, or use of location data to control or threaten.

Why is it important to recognize personal harm and harassment online?

Online abuse can be just as damaging as in-person aggression, and sometimes even harder to escape. Its consequences include:

- ☐ **Mental Health Issues:** Victims often experience anxiety, depression, and stress. In severe cases, this can lead to suicidal thoughts or behaviors.
- ☐ **Academic Disruption:** Cyberbullying and online harassment affect focus, attendance, and school performance.
- ☐ **Social Withdrawal:** Victims may isolate themselves, avoiding both online and offline interactions, which increases loneliness.
- ☐ **Long-term Trauma:** Persistent harassment can leave psychological scars, damaging self-esteem and affecting future relationships.
- ☐ **Real-life Safety Risks:** Tactics like doxxing or stalking can lead to physical danger and



fear for personal safety.

The rapid development of digital platforms has led to a parallel increase in negative social behaviors online. According to a 2016 [NIH study](#), the anonymity, immediacy, and wide reach of online communication often reduce accountability, enabling users – especially adolescents – to engage in harmful conduct more freely. This environment can fuel behaviors such as cyberbullying, social exclusion, and even cyber-racism.

The UNICEF's [State of the World's Children 2024 Report](#) reveals that over 36% of young people worldwide have experienced some form of online harm, with significant overlap between digital abuse and symptoms of anxiety, depression, and social withdrawal.

In line with this, a 2024 report by the [Australian Institute of Criminology](#) found that nearly 75% of dating app users have experienced some form of sexual violence, including harassment and stalking. The risks extend beyond dating platforms – according to a [Girlguiding UK survey](#), one in three girls aged 11 to 21 has received unsolicited sexual images, and one in five has been cyberstalked. Alarming trends continue: the [UK Revenge Porn Helpline](#) reported a 106% increase in cases in 2023, handling nearly 19,000 incidents.

Cyberbullying represents another widespread and deeply harmful issue for young people across the globe. In the United States, a [2023 National Survey](#) found that approximately 55% of students aged 13 to 17 reported experiencing cyberbullying at some point in their lives. Similarly, a [2022 study](#) in the UK revealed that 39% of children aged 8 to 17 had encountered bullying – online or offline – with 84% facing it through digital devices and 61% in person. The emotional toll is significant: [research](#) shows that over 50% of teens report feeling angry after being cyberbullied, about 33% feel hurt, and nearly 15% feel scared. Importantly, two-thirds of these teens say cyberbullying affects their ability to



learn and feel safe at school, and they are four times more likely to engage in self-harm or suicidal behavior. The platforms most associated with cyberbullying include YouTube (79%), Snapchat (69%), TikTok (64%), and Facebook (49%).

For young users, whose emotional and social identities are still developing, these interactions can be particularly damaging. The repeated exposure to digital harassment can cause deep psychological wounds and foster a sense of social isolation. The emotional detachment common in online spaces may also desensitize aggressors, reinforcing a cycle of abuse where harmful behavior is minimized or normalized.

Moreover, the digital space can create echo chambers where abusive language or discriminatory behavior goes unchallenged – or even encouraged – by peer groups. When personal harm online is dismissed as “harmless fun” or a “normal part of being online,” victims are less likely to report incidents, and perpetrators face little consequence. As the line between virtual and real-world interactions continues to blur, the emotional effects of online harassment become just as real and damaging as those experienced in face-to-face encounters.

Prevention requires a combination of education, technical tools, and community support. [UNICEF](#) emphasizes teaching empathy and digital respect early on to stop cyberbullying before it starts. [Further studies](#) recommend blocking aggressors, saving evidence, and reporting incidents through trusted adults or school systems. Additionally, [UNITAD](#) advises protecting personal data, adjusting privacy settings, and using secure passwords to avoid becoming a target. Together, these strategies help build safer, more respectful digital spaces for all.





“ Maya, 15, started receiving cruel comments on her TikTok videos from anonymous users. The insults grew worse and classmates joined in. Feeling humiliated, she stopped posting and avoided school. With help from a teacher, Maya reported the abuse, got support, and learned how to manage privacy settings to protect herself online. ”

“ After a breakup, Sam discovered that a private photo shared in confidence had been posted on a messaging group. He felt betrayed and deeply anxious. With the support of a school counselor and legal advice, the image was taken down and the perpetrator faced consequences. Sam’s story highlighted the need for consent and legal awareness. ”

“ Leila, a young climate activist, posted a video sharing her views on environmental issues. Soon after, trolls flooded her inbox with hate, and someone published her address online. Terrified, she alerted the platform and the police. Thanks to quick action, the posts were removed, and Leila received emotional support and safety advice. ”



✓ PERSONAL HARM CHECKLIST

- ☐ Think before posting and avoid sharing content that could hurt or embarrass someone
- ☐ Use privacy settings to control who can see your posts and personal information
- ☐ Block and report users who harass, threaten, or make you feel unsafe
- ☐ Save evidence of online abuse such as screenshots or message logs
- ☐ Avoid responding to trolls to reduce conflict and emotional impact
- ☐ Talk to a trusted adult if you feel targeted or uncomfortable online
- ☐ Check your digital footprint regularly and remove outdated or revealing content
- ☐ Protect your personal data such as your location, school, and contact details
- ☐ Know your rights and understand local laws and platform policies around online harassment



Activity 1: “Stop, Block, Speak”

KEYWORDS

Digital safety, cyberbullying, peer support, online harassment, empathy

OBJECTIVES

To help participants recognize forms of online harassment and harmful behavior
To practice safe, effective responses to digital aggression
To foster empathy and build peer support strategies
To promote confidence in reporting and seeking help

DURATION

30–45 minutes.

PARTICIPANT AGE

13–18 years old.

MATERIALS AND TOOLS

Scenario cards/slides, discussion prompts, optional props for role play

Description of Activity:

Participants will explore a set of real-life digital conflict or harassment scenarios and work together to decide how to respond safely. This activity builds empathy, encourages safe habits, and empowers young people to act when faced with online harm.

Facilitator Instructions:

- ☐ Prepare 4-6 scenario cards or slides with realistic examples (e.g., “Someone shares your private photo in a group chat,” “A classmate creates a fake account to mock you”).
- ☐ Read each scenario aloud or present it on a screen.
- ☐ Ask participants to discuss in small groups:
 - What’s happening?
 - What’s harmful about this situation?
 - What could the targeted person do?
 - How could a friend or bystander help?
- ☐ Invite each group to share a short role-play or summary of their response.
- ☐ Lead a class discussion to compare ideas and reinforce best practices.

Suggestions for Facilitators:

Choose diverse, age-appropriate examples covering different platforms and types of harm
Emphasize open dialogue and make it clear there are no “perfect” answers – what matters is thinking through safe responses
Encourage participants to reflect on similar situations they’ve seen or experienced
Create a supportive environment where students feel safe discussing sensitive topics



PERSONAL HARM - ACTIVITIES

Activity 2: “Safe or Sketchy?”

KEYWORDS

Digital boundaries, online safety, red flags, self-protection, respectful behavior

OBJECTIVES

To help participants identify online behaviors that may cross personal boundaries
To encourage critical thinking about digital interactions
To strengthen decision-making and awareness of potential red flags
To promote safer, more respectful online behavior

DURATION

30-40 minutes.

PARTICIPANT AGE

13-19 years old.

MATERIALS AND TOOLS

Scenario slides/cards, colored cards or digital voting tool, whiteboard or shared screen.

Description of Activity:

Participants will evaluate a variety of online behaviors or interactions and decide whether they feel “safe,” “risky,” or “harmful.” This activity encourages reflection on digital boundaries, online safety, and respectful behavior in virtual spaces.

Facilitator Instructions:

- ☐ Prepare 6-8 example scenarios (e.g., “A stranger sends a friend request with no mutual contacts,” “A friend shares your photo without asking,” “You’re asked to move a chat from a game to a private messaging app”).
- ☐ Read each scenario aloud or show it on a screen.
- ☐ Ask participants to raise colored cards (green = safe, yellow = risky, red = harmful) or use a digital poll.
- ☐ After each vote, invite brief group discussion:

What made this feel unsafe or okay?

What would you do in this situation?
- ☐ Record common concerns and suggestions on a board or shared screen.

Suggestions for Facilitators:

Use examples that reflect real-world experiences, especially from social media, gaming, and group chats

Make the activity interactive and non-judgmental – there are often gray areas worth exploring

Invite personal reflection: “Has something like this happened to you or someone you know?”

Summarize with practical safety tips based on group input





Explore why recognizing and responding to online harassment is essential for digital well-being.

Start with general, relatable prompts to ease into the topic:

“Have you ever seen or heard someone being treated badly online?”

“Why do you think people act differently behind a screen than in person?”

“What kinds of online comments or messages make you feel uncomfortable?”

As the conversation develops, ask more reflective and thought-provoking questions:

“Why do you think some people don’t report online bullying or harassment when it happens to them?”

“What impact do you think harmful messages or public shaming online can have on someone’s confidence or mental health?”

“Do you think being a ‘bystander’ in these situations makes a difference? Why or why not?”

“How does seeing this kind of behavior online affect how you act or feel on social media?”

To encourage storytelling and real-life connections, use situational prompts:

“Have you or someone you know ever been targeted or made fun of online? What happened?”

“Can you think of a time when someone stood up for someone else online? What did they do, and what was the result?”

“Imagine someone posted your personal photo or information without your permission – how would that make you feel, and what would you do?”

E-BOOKS

 Exploration of Cyberbullying. Comic Book [Download here](#) 

WEBSITES

 StopBullying.gov. <https://www.stopbullying.gov> 

 Cyberbullying – National Children’s Alliance. <https://www.nationalchildrensalliance.org/cyberbullying/> 

Facilitator Tips:

Allow time for everyone to reflect and speak – especially those who might not share right away.

Encourage participants to support each other and listen without judgment.

Take note of recurring themes or concerns, and validate participants' experiences.

Gently guide the conversation back if it veers off-topic, and provide support if any sensitive issues arise.

Facilitators play a crucial role in guiding the conversation and helping participants connect the topic of online harassment to their personal experiences and digital lives. Begin by creating a supportive, non-judgmental space where everyone feels safe to speak.

Encourage open dialogue with simple, relatable questions like **“Have you ever seen someone being bullied or harassed online? What did you think or do?”** or **“Why do you think people sometimes say things online they wouldn’t say face-to-face?”**

As questions come up, validate each contribution and gently guide the group to reflect more deeply on what respectful digital behavior looks like. If the discussion drifts, bring it back with bridging phrases like **“That’s a great point – how do you think that connects to the idea of online respect or safety?”** or **“Interesting – does anyone else want to add how they’d respond in a similar situation?”**

Remind participants that this session is not about blame or shame, but about learning, support, and making better choices online.

To wrap up, invite personal reflection with open-ended prompts such as **“What’s one thing you’ll remember from today’s discussion?”** or **“Is there something small you could do to help make digital spaces more respectful or safe?”**.

These reflections help participants leave with a clearer understanding of the topic—and a sense of personal agency in how they engage online.



3. TOPICS IN SOCIAL RISKS



3.2. Manipulation and Deception in Digital Relationships

Manipulation and deception in digital relationships are often subtle, but their impact can be deep and long-lasting. Predators and scammers may use emotional tactics to manipulate individuals, particularly young people who are still learning to navigate online spaces and form healthy relationships. These deceptive behaviors can lead to emotional distress, financial loss, or exposure to harmful situations.

What are the risks?

Young people are increasingly vulnerable to online relationships that are not what they seem. These deceptive interactions can assume different forms. Key risks include:

- ☐ **Grooming:** Grooming is when someone builds a relationship to manipulate or exploit a young person, often for abuse. It starts with trust-building but can lead to requests for personal information, explicit photos, or even physical meetings.
- ☐ **Romance Scams:** Scammers create fake romantic connections to gain trust and then manipulate victims into sending money or gifts. These scams prey on feelings of loneliness, leaving victims both financially and emotionally hurt.
- ☐ **Sextortion:** Sextortion occurs when someone threatens to share explicit images or messages unless their demands are met, often for money or more content. This can lead to feelings of shame, fear, and isolation.
- ☐ **Catfishing:** Catfishing involves using a fake identity to deceive someone into a relationship. The goal is often manipulation or exploitation, and the discovery of the deception can lead to emotional distress.
- ☐ **Exposure to Inappropriate Content:** Young people may be exposed to graphic or inappropriate content, either intentionally or through manipulative behavior. This can cause trauma, confusion, and a distorted understanding of healthy relationships.

Why is it important to recognize manipulation and deception online?

Recognizing the red flags linked to all these different forms of manipulatory online behaviours is vital for safeguarding young people's emotional and psychological health. The consequences of not recognizing these risks can be severe including:

- ☐ **Emotional Distress:** Victims often experience anxiety, shame, or confusion, which can lead to long-term mental health issues like depression and trust issues.
- ☐ **Manipulation and Exploitation:** Failure to identify these risks can lead to young people being manipulated into dangerous or exploitative situations, including financial loss or personal harm.
- ☐ **Social Isolation:** Victims may withdraw from their real-world relationships, fearing embarrassment or humiliation, which deepens feelings of loneliness and isolation.
- ☐ **Trauma and Trust Issues:** Experiencing these manipulative behaviors can leave lasting emotional scars, damaging a young person's ability to trust others or engage in healthy relationships.



☐ **Safety Concerns:** Some scams and grooming attempts can escalate into physical meetings, posing threat to physical safety and well-being.

Young people today often rely on digital spaces for connection, support, and even intimacy. However, these environments are also breeding grounds for manipulation and exploitation. The deceptive nature of these interactions – whether through fake identities, emotional blackmail, or the sharing of harmful content – makes them especially difficult to identify in the early stages.

Besides enhanced connectivity, the internet allows users to navigate spaces anonymously, without having to prove their real identity. This **anonymity**—combined with a lack of awareness about existing risks, peer pressure that may encourage risky online behaviors, and psychological drivers such as emotional distress or curiosity – increases the likelihood of encountering an online predator.

Predators and manipulators build trust with young individuals over time, often with the intent of exploiting or abusing them. For example, in the early stages, grooming may appear harmless, with perpetrators providing emotional support and validation, making the victim feel special. However, this slow and calculated process can eventually lead to requests for inappropriate content or in-person meetings.

In [2023 report](#) from the Federal Trade Commission, in the USA victims of romance scams lost over \$1.14 billion in just one year, with the majority of cases starting on social media or dating apps. Though adults are frequent targets, young people are particularly at risk due to their developing emotional awareness and increased screen time. According to a [2024 UNICEF analysis](#), one in five adolescents has received unwanted sexual messages or images online, often from strangers posing as peers or romantic interests.



Manipulative tactics don't always appear aggressive or threatening – they often begin with compliments, shared interests, and a false sense of security. For example, catfishing often involves the use of AI-generated photos and deepfake technology to create convincing fake profiles. A [2025 study by the Australian Institute of Criminology](#) found that 11% of adolescents experienced sextortion, often before age 16. In 40% of cases, perpetrators used digitally altered content, highlighting the growing risk of tech-enabled exploitation.

Exposure to inappropriate content, especially when framed as part of an emotional or romantic connection, can be equally harmful. Youth may be manipulated into viewing or engaging with graphic materials, leading to trauma or desensitization. As the line between emotional connection and **digital manipulation** blurs, it becomes more difficult for young users to identify when boundaries are being crossed.

What makes these threats especially dangerous is the shame and fear they often provoke. Victims may feel responsible, embarrassed, or fearful of judgment, which prevents them from speaking up or seeking help. This **silence** enables perpetrators to continue their behavior unchecked. In many cases, the manipulation only becomes clear in hindsight – after significant emotional, psychological, or even financial harm has occurred.

Digital deception also undermines trust – not just in others, but in the online world itself. Victims may feel betrayed or unsure of whom to believe, leading to withdrawal from both digital and real-life social spaces. As highlighted in a 2022 Review in [Frontiers in Psychology](#), the emotional aftermath of online manipulation can mirror that of in-person abuse, with long-term impacts on self-esteem, relationship-building, and emotional resilience.

Recognizing manipulation is essential for prevention. But more importantly, young people need access to supportive environments where they can safely share concerns and learn to recognize red flags. Education about emotional boundaries, critical thinking about digital personas, and understanding online consent are all key components of resilience. Prevention also includes parental awareness, platform regulation, and peer support.

Creating safer digital spaces requires not only technology, but trust – between young people and the adults, educators, and peers who support them. When youth feel empowered to speak up and ask questions, the cycle of manipulation can be disrupted, and healthy, respectful digital relationships can thrive.





“Hana, 15, began chatting with someone who followed her on social media. He was friendly, seemed her age, and complimented her often. Over time, their chats turned flirty. Trusting him, Hana sent a private photo. A day later, he demanded more – and threatened to share the first one if she didn’t send them. Hana panicked and considered staying silent out of fear and shame. But she remembered a school workshop about online safety and confided in her older sister. Together, they contacted a support line and reported the account. The photo was never shared. Hana learned that no one has the right to use fear or shame as control, and asking for help isn’t weakness – it’s power..”

“Omar, 13, loved playing online games and was thrilled when an older player started messaging him regularly. They played together often, and the person even gifted him in-game items. Over time, the messages became more personal – asking Omar to keep secrets and move their chat to a private app. The older player shared stories to gain Omar’s sympathy and trust, then began asking for photos and tried to arrange a meetup. Omar felt confused and uncomfortable. Instead of replying, he told his school counselor, who took it seriously. The adult was reported and blocked. Omar was relieved to learn he wasn’t to blame, and that grooming often starts with kindness that turns into control.”

“Layla, 14, was part of a group chat with classmates where they usually shared memes and funny videos. One afternoon, someone posted a link saying, “This is so crazy – watch till the end!” Curious, Layla clicked. What she saw was violent and disturbing, nothing like what she expected. She felt sick, confused, and couldn’t stop thinking about it afterward. At first, she was embarrassed to tell anyone, but after a restless night, she talked to her older cousin. He reassured her it wasn’t her fault and helped her report the group. Layla learned to trust her instincts and now thinks twice before clicking unfamiliar links – even if they come from people she knows.”

✓ PERSONAL HARM CHECKLIST

- ☐ Trust your instincts if someone moves too fast or makes you feel uncomfortable early on
- ☐ Avoid sharing personal information like your address, school, or intimate photos with people you don't know offline
- ☐ Verify identities by asking for proof or video chatting if you're unsure who someone really is
- ☐ Be cautious if someone is overly complimentary or gives you too much attention too quickly
- ☐ Set boundaries and stick to them, especially when someone asks for personal or explicit content
- ☐ Report and block anyone who pressures you or threatens you if you don't comply with their demands
- ☐ Refuse to engage with inappropriate or graphic content, even if someone insists or pressures you
- ☐ Talk to a trusted adult if you feel unsafe or someone asks you to keep your conversations secret
- ☐ Avoid meeting in person with anyone you've only interacted with online
- ☐ Save evidence of harmful messages or content in case you need to report the situation





Activity 1: “Recognizing Grooming Tactics”

KEYWORDS

Grooming, manipulation, online predators, digital safety, red flags, self-protection

OBJECTIVES

To help participants identify the early warning signs of online grooming.

To raise awareness about the psychological tactics used by predators.

To encourage self-protection and critical thinking in digital relationships.

To empower young people to seek help if they recognize grooming behaviors.

DURATION

30–40 minutes.

PARTICIPANT AGE

13–19 years old.

MATERIALS AND TOOLS

Scenario slides/cards or digital polling tool

Colored cards (green, yellow, red) or digital voting tool

Whiteboard or shared screen

Description of Activity:

Participants will explore various online grooming tactics used by predators to manipulate and exploit young people. By reviewing scenarios and discussing red flags, they will gain a deeper understanding of how grooming begins and how to protect themselves.

Facilitator Instructions:

☐ Prepare 6-8 example scenarios that demonstrate grooming behavior (e.g., “A new online friend starts complimenting you frequently and seems overly concerned about your feelings,” “Someone you met online begins to share personal problems and asks for advice,” “An online acquaintance invites you to meet in person or share photos without a clear reason”).

☐ Read each scenario aloud or display them on a screen.

☐ Ask participants to vote using colored cards (green = harmless, yellow = suspicious, red = grooming) or use a digital voting tool.

☐ After each vote, facilitate a group discussion by asking:

What makes this situation feel like grooming?

What are the first signs of grooming in this scenario?

How would you protect yourself or someone else in this situation?

☐ Record the group’s thoughts and safety tips on a whiteboard or shared screen.

Suggestions for Facilitators:

Focus on the psychological tactics often used by groomers to build trust and manipulate young people. Encourage participants to ask questions and share concerns

Discuss the importance of reporting suspicious behavior to a trusted adult or authority figure.

DIGITAL RELATIONSHIPS - ACTIVITIES

Activity 2: “Digital Boundaries Bingo”

KEYWORDS

Digital boundaries, online safety, behavior reinforcement, healthy habits, commitment

OBJECTIVES

To motivate participants to actively practice healthy and safe online behaviors.
To raise awareness of important digital safety habits.
To encourage accountability for personal online safety and responsibility.

DURATION

20-30 minutes.

PARTICIPANT AGE

13-19 years old.

MATERIALS AND TOOLS

Digital bingo cards (using Google Sheets, Canva, or an online bingo tool)
Video conferencing platform (Zoom, Teams, etc.)
Chat for discussion

Description of Activity:

This bingo-style game encourages participants to identify and commit to healthy digital behaviors by marking off behaviors they’ve already practiced or plan to practice.

Facilitator Instructions:

☐ Prepare Prepare Bingo Cards: Create digital bingo cards with different digital safety behaviors, such as:

“Set your social media profiles to private” / “Block someone who makes you feel uncomfortable” / “Report a suspicious online interaction” / “Talk to an adult about an online situation” / “Avoid sharing personal details with strangers online” / “Use two-factor authentication on your accounts” / “Only accept friend requests from people you know” / “Limit the amount of personal info in your bio” / “Review your privacy settings regularly”

You can create these bingo cards using tools like Google Sheets, Canva..

☐ Start the Game: Share the bingo card link with the participants via a meeting chat (Zoom, Teams, etc.) or send it as a shared document.

Participants can either mark the boxes digitally (if using an online bingo tool) or keep track on their devices.

☐ Show to Play: The facilitator will read out one of the digital safety behaviors or scenarios from the bingo list (e.g., “Set your social media profiles to private”). Participants will check if that behavior is something they’ve already practiced or if they commit to trying it in the next week. If they can mark it off, they do so.

After each behavior, ask participants to reflect briefly about why that behavior is important to them and how it helps them stay safe online.

Winning: The first person (or team) to get a full line (vertical, horizontal, or diagonal) on their bingo card wins. After the game, give a few minutes to discuss.





Explore why recognizing and responding to manipulation and deception online is essential for digital well-being.

Start with general, relatable prompts to ease into the topic:

“Have you ever received a message from someone you didn’t know but who seemed really friendly or interested in you?”

“What makes someone seem trustworthy online?”

“Have you ever seen a fake profile or felt unsure if someone online was who they said they were?”

As the conversation develops, ask more reflective and thought-provoking questions:

“Why do you think some people pretend to be someone else online?”

“What might make a person fall for a scam or manipulation without realizing it?”

“What are some warning signs that an online relationship might not be healthy or real?”

“How do you think it feels to find out you’ve been tricked or used by someone you trusted online?”

To encourage storytelling and real-life connections, use situational prompts:

“Have you or someone you know ever been contacted by someone online who turned out to be fake or had bad intentions?”

“Can you think of a time when someone realized they were being manipulated – how did they react, and what happened next?”

“Imagine someone online asks you for personal photos or money after weeks of chatting – how would you respond? What would raise red flags?”

E-BOOKS

 Blocking and reporting [Download here](#) 

WEBSITES

 Cyberbullying Behaviour and Catfishing Activities for all ages. <https://www.antibullyingpro.com/support-and-advice-articles/cyberbullying-behaviour-and-catfishing-how-can-we-recognise-if-someone-is-fake-online>



 Klicksafe – Catfishing, Cybergrooming, Sextortion. <https://www.klicksafe.eu/en/news/catfishing-cybergrooming-sex-tortion-worauf-achten-bei-online-kontakten> 

 UNHCR – Safe Online for Children. <https://help.unhcr.org/slovakia/safe-online/children/> 

Facilitator Tips:

Allow everyone time to speak – some might need more time to reflect.

Reassure participants that there's no judgment and that many people have experienced online deception.

Gently validate concerns and bring in real-life safety strategies if needed.

Keep the tone supportive and focused on learning, not blame.

☐ Open discussion for participants to ask questions or clarify doubts.

Facilitators should guide this session with empathy and openness. Create a space where questions are welcomed and no concern is too small. You might begin with:

“Is there anything you’ve always wondered about online scams or grooming but weren’t sure who to ask?”

“Have you ever felt unsure about someone you were talking to online and didn’t know what to do?”

☐ As questions come in:

☐ Listen actively and thank them for speaking up.

☐ Use the questions to open group reflection:

“That’s a great question – has anyone else ever felt that way?”

“Let’s think about what someone could do if they were in that situation.”

☐ Bring the group back on track with gentle guidance:

“That’s interesting – how does that connect to trusting someone online?”

“Thanks for sharing – does anyone want to add how they might handle it differently?”

Wrap up with reflection prompts:

“What’s one thing you learned today that surprised you?”

“Is there something you’ll do differently next time you meet someone online?”

“How can we support each other to stay safe in digital relationships?”



Module 4: Information Trustfulness

INTRODUCTION TO INFORMATION TRUSTFULNESS



Objectives

To develop young people's ability to recognize, question, and share truthful information in digital environments, while protecting themselves and others from disinformation.

KEY CONCEPTS

Information trustfulness refers to how accurate, reliable, and credible information is. It involves assessing the quality and integrity of content based on its source, supporting evidence, consistency, and lack of bias or manipulation. Trustworthy information is essential for making informed decisions, communicating effectively, and protecting ourselves and society from disinformation and manipulation.

KEYWORDS

Source Credibility, Reliability, Evidence-based, Disinformation, Bias, Fact-checking

Every day, we are surrounded by information—on social media, in messages from friends, on websites, videos, and news platforms. But not all the information we see is accurate or trustworthy. Some of it is incomplete, misleading, or even purposely false. That's why learning how to recognize truthful information has become an essential skill for young people navigating the digital world.

Information trustfulness means knowing how to tell whether what we read or hear is reliable, accurate, and fair. It involves asking questions like: Who is sharing this? Why are they sharing it? Is there evidence to support it? Trustworthy information comes from sources that are open, balanced, and based on facts—not on emotions or manipulation.

In this module, you'll explore what makes information credible and how to spot warning signs of misinformation and disinformation. You'll also learn how to check sources, identify bias, and use fact-checking tools. These skills are important not only for protecting yourself, but also for helping your community stay informed and make good decisions.

By the end of this module, you will be better equipped to think critically, ask the right questions, and become someone others can count on for sharing honest and responsible content. Being able to recognize and promote trustworthy information is a key part of being a responsible digital citizen.



4. TOPICS IN INFORMATION TRUSTFULNESS



4.1 Source credibility

Information trustfulness refer to the degree to which information can be considered accurate, reliable, and credible. It is an assessment of the quality and integrity of information based on various factors, such as its source, consistency, evidence supporting it, and the absence of bias or manipulation. The importance of information trustfulness lies in its fundamental role in ensuring that individuals, organizations, and societies can make informed, accurate, and fair decisions. Reliable information is not only the backbone for efficient communication, governance, and innovation but also protects us against the negative effects of disinformation and manipulation.

In an age where information is abundant but often unreliable, assessing source credibility has become critical for youth actively engaging with online information sources in order to establish whether the information they are reading or listening to is trustworthy, accurate, and deserving of adoption.

Even though information and sources are interconnected, they mean different things. Information is the message or details you hear, read, or see, like a news story, a post, or a fact someone tells you. The source is where that information comes from, for example a person, an organization, or a social media platform.

What is Source Credibility?

- ☐ Source credibility refers to the perceived trustworthiness and expertise of the origin of an information. This includes:
- ☐ Expertise (Knowledge and Skills): How much does the person or source know about the topic? A credible source should have the right qualifications or experience in the area they are talking about.
- ☐ Trustworthiness (Honesty): How honest and fair is the source? A trustworthy source shares information openly, without trying to push a personal agenda (like making money or promoting politics)
- ☐ Reputation (Track Record): How reliable has the source been in the past? If they have consistently shared accurate and useful information, they are more likely to be trusted.

Why is Source Credibility Important?

Ensuring source credibility is essential for:

Making Good Choices (Informed Decision-Making): Credible sources give accurate and reliable information that helps people make sound decisions in critical areas like health, work, or government.

Stopping False Information (Preventing Misinformation): Ensuring source credibility reduces the spread of false or misleading information, protecting young people and communities from the potential negative outcomes which may arise from believing something untrue.

Building Confidence (Building Trust): Honest and reliable sources help build trust between people, organizations, and the public, resulting in much more positive relationships and communication.

Studies on the topic of source trustfulness have revealed significant differences in trust levels around the world. A global study on trust in the news media conducted by the [Global Data Platform Statista](#) (2024), shows that Scandinavians emerged as the most trusting, with Finland leading at 69%. This contrasts sharply with other regions like Italy (34%), Turkey (35%). People trust news differently based on the source, with radio and TV trusted more, but distrust is rising across all ages due to fake news and division. According to another study led by the [Arab Barometer](#) in 2019, trust in media for information also varies significantly across MENA and nearby countries, with Lebanon showing a relatively high trust rate at 67%. In contrast, Algeria (47%) and Tunisia (44%) exhibit lower trust levels. These variations suggest differing degrees of confidence in traditional media and social media as a source of trustworthy information, influenced by factors like media freedom, state control, and access to alternative sources.

The spread of fake news and the divisive nature of political events have made it difficult for people - especially young people but also older generations - to rely on the mass media for accurate information. A study by three [MIT researchers](#) (2018) found that false news spreads much faster and wider than true news. According to Sinan Aral, a professor at MIT and co-author of the study, false information travels farther, faster, and reaches more people in all types of topics - often by a huge margin compared to the truth.

We receive an enormous amount of information of different kinds and in different ways. Think about where you get information daily. You might hear it from podcasts, the radio, or even voice assistants like Siri. You see it in YouTube videos, TikTok, or TV shows. You read it in Instagram captions, websites, or texts. Information comes to us in many ways - listen, watch, or read!

We can recognize a trustworthy source thanks to several important factors. First, information is more trustworthy if it comes from authors with real qualifications, like degrees or experience. For example, research written by experts is more reliable than opinions from people without a background in the subject. The reputation of the institution also matters - well-known organizations like universities or respected news outlets are usually more trusted than lesser-known ones. Transparency is key too. Trustworthy sources clearly explain how they got their information, while hidden motives or undisclosed funding can raise doubts.

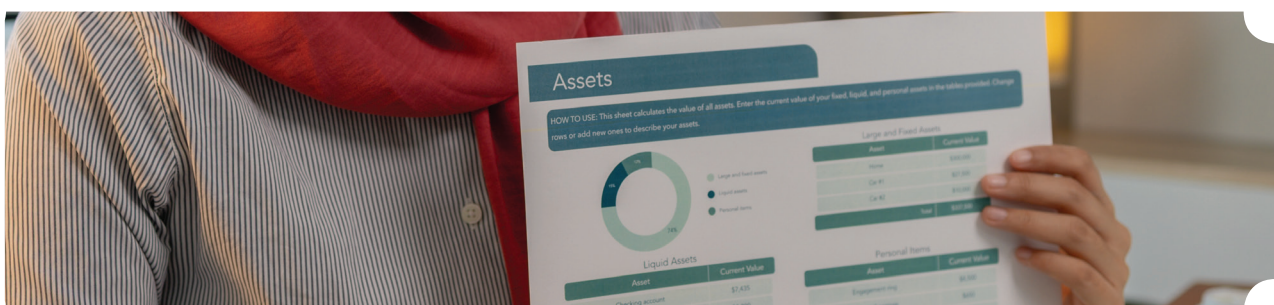
Moreover, a reliable source has to be consistent, do not continuously change its claims, and up-to-date over time. Imagine looking up medical advice for handling an allergy and finding two articles on a website, one from 2015 and another from 2016, each suggesting a different method.



“ Consider Emma, a college student who felt unwell and searched online for remedies. She found a flashy blog suggesting a "miracle detox drink," but something felt off. Instead, she consulted a government health website and found evidence-based advice from medical experts. Following their guidance, Emma recovered quickly. Later, she discovered the blog had no medical backing and spread dangerous misinformation. Emma realized the importance of trusting credible sources with verified expertise, which not only protected her health but also reinforced her ability to make informed decisions. ”

“ Sophia is a high-school student preparing for her final school project. Sophia relied on a blog with vague claims to gather information. When her teacher returned the paper, pointing out the sources were unreliable, she felt frustrated. Determined to improve, Sophia replaced the blog with peer-reviewed articles and reputable websites. Her hard work paid off with a better grade, and she realized how using trustworthy sources not only strengthened her arguments but also made her work more credible and impactful. ”

“ Take Andrea, an enthusiast of new investment opportunities who wanted to invest in stocks and cryptocurrency after reading a viral social media and Reddit post claiming a small tech company would skyrocket. Excited, he almost bought shares but decided to double-check. He visited reputable financial news sites and found no credible evidence supporting the claim. Instead, experts warned of potential fraud surrounding the company. David avoided a costly mistake and realized how trusting unverified sources could have put his savings at risk. By relying on credible, evidence-based information, he made smarter investment decisions. ”



✓ SOURCE CREDIBILITY CHECKLIST

- ☐ Check Credentials and confirm that the author or organization has the qualifications and experience relevant to the topic.
- ☐ Verify through multiple sources and cross-check the information with other reliable sources to ensure accuracy.
- ☐ Examine transparency and look for clear citations, references, and disclosures about funding or affiliations.
- ☐ Assess reputation and rely on sources with a proven history of accuracy and trustworthiness.
- ☐ Beware of red flags and avoid sources that use sensationalism, emotional appeals, or vague claims without evidence.
- ☐ Distinguish fact from opinion and separate factual information from personal opinions or commentary.
- ☐ Use fact-checking tools and verify claims using platforms like [AFP](#), [Reuters](#), [Snopes](#), [FactCheck.org](#), or [PolitiFact](#).





Activity 1: “Truth or Trap: Evaluating Source Credibility”

KEYWORDS

Trustworthy sources, misinformation, credibility, source evaluation, fact-checking, bias detection

OBJECTIVES

To teach participants how to identify reliable and unreliable sources of information.

To encourage critical thinking about the credibility of media and online content.

To help participants develop skills to navigate misinformation.

DURATION

30–45 minutes.

PARTICIPANT AGE

15–24 years old.

MATERIALS AND TOOLS

Printed or digital mixed information sources.

Discussion prompts or checklist for analyzing source credibility.

Projector or screen (if presenting examples as a group).

Description of Activity:

Participants will practice evaluating various information sources to distinguish between trustworthy and unreliable ones. They will be presented with examples of news articles, social media posts, and websites, and must analyze them for credibility based on their sources, content, and presentation.

Facilitator Instructions:

- ☐ Prepare a set of mixed information sources: One reliable news article; One unreliable news article (e.g., misinformation or bias); A social media post (both good and bad examples); A reputable website and a questionable website.
- ☐ Show each example to the group without revealing its credibility.
- ☐ Divide participants in discussion groups.
- ☐ Ask participants to evaluate each source using a set of questions: Who is the source? Is there evidence or references? Is the tone neutral or biased? Does the source have a reputation for reliability?
- ☐ Facilitate a group discussion to share findings and the techniques used to spot reliable resources.
- ☐ Reveal the credibility of each source.

Suggestions for Facilitators:

Encourage open discussion by asking questions like, **“Were you surprised by discovering which information was actually true?”**

Ensure a non-judgmental atmosphere where participants feel comfortable sharing their thoughts. Provide concrete feedback based on participants' tactics deployed to recognize source credibility.

Groups present their analysis and compare across articles.

SOURCE CREDIBILITY - ACTIVITIES

Activity 2: “Guess the Credible Source” (Guess Who? Game)”

KEYWORDS

Source evaluation, critical questioning, game-based learning, fact-checking

OBJECTIVES

To practice asking strategic questions about source credibility.

To reinforce understanding of key credibility indicators (expertise, transparency, reputation, bias).

To encourage playful learning and collaboration.

DURATION

30–40 minutes.

PARTICIPANT AGE

12–16 years old.

MATERIALS AND TOOLS

Prepared “source cards” (physical cards, slides, or digital cards).

Example list of questions participants can ask.

Scoreboard or tally sheet (optional for competitive play). group).

Description of Activity:

Participants will play a source credibility guessing game modeled after Guess Who? style gameplay. Each participant or team will try to identify which information source is credible by asking yes/no questions about the source’s characteristics (expertise, transparency, bias, etc.). The goal is to encourage strategic questioning and critical thinking about what makes a source trustworthy.

Facilitator Instructions:

☐ Prepare a set of source cards (physical or digital), each with a short description but no label of whether it is trustworthy or not. Examples: Peer-reviewed scientific journal; Influencer on TikTok; Government health website; Personal blog with no author info; Reputable international newspaper; Sponsored content post; Anonymous Reddit post; NGO report; Satirical news website.

☐ One participant (or team) selects a secret source card without revealing it.

☐ The other players take turns asking YES/NO questions to guess which source it is. Example questions:

Does this source have a named author? Is this source peer-reviewed? Is this source known for neutrality? Is it likely this source has an agenda? Is this source affiliated with a government or university?

☐ After gathering clues, the players make a final guess.

☐ Once revealed, the group discusses whether the source was credible or not, and why.

Suggestions for Facilitators:

Before starting, review what makes a source credible. Model one round first so participants understand how to ask effective YES/NO questions. Use a mix of easy and tricky source examples to challenge participants. Optionally, add a competitive element: teams can score points for correct guesses.



Explore what practical consequences can lead to trusting an unreliable source.

Facilitators play a crucial role in stimulating meaningful discussions and encouraging participants to share personal stories or anecdotes about themselves or others they know. Begin the discussion with general, relatable questions to ease participants into the topic, such as, **“Why is it important to assess the credibility of a source before accepting information?”** or **“Have you ever come across a situation where trusting an unreliable information led to a problem?”** These open-ended questions encourage reflection and make it easier for participants to share personal experiences or observations about others.

As the discussion progresses, try to pose deeper questions like: **“Why do you think some people tend to trust information on social media without cross-checking?”** or **“Do you think traditional media (like TV and newspapers) are more trustworthy than social media? Why or why not?”** or **“Do you think people feel pressured to believe or share popular opinions even if they are not fully convinced by their credibility?”**. To stimulate storytelling, prompt participants with scenario-based questions such as, **“Have you ever felt overwhelmed by trying to figure out what’s real and what’s not online?”** or **“Have you ever seen someone spread a fake news from a sketchy source, and what advice would you give them now?”** Use follow-up questions to explore the stories further, such as, “What consequences did it cause?”.

Throughout the discussion, validate participants’ contributions by actively listening, summarizing key points, and showing appreciation for their input. Avoid interrupting and gently redirect the discussion if it veers off-topic. To conclude, summarize the shared stories and insights, highlighting actionable lessons and emphasizing the importance of ensuring source credibility.

E-BOOKS

- ▶ Fact Checking Manual. [Download here](#) 
- ▶ Fact Checking 101. [Download here](#) 
- ▶ Web Literacy for Student Fact-Checkers [Download here](#) 

WEBSITES

- ▶ BBC Evidence Toolkit for youth. <https://www.bbc.co.uk/teach/young-reporter/articles/z6v3hcw> 
- ▶ Digital Civics Toolkit <https://www.digitalcivicstoolkit.org/investigate> 



4. TOPICS IN INFORMATION TRUSTFULNESS



4.2. Misinformation and Disinformation

Misinformation, disinformation and bias are pervasive issues in today's digital landscape. This chapter focuses on information, that is the message or details you hear, read, or see, and how to recognize unreliable information by looking at its language and message.

What are Misinformation and Disinformation?

Disinformation is a complex challenge, as different types of content can cause varying levels of harm to those who encounter it. False and misleading information comes in many forms. Therefore, understanding the differences can help young people navigate it. A study led by [OECD](#) (2022) have divided misleading content into 5 different types of untruths online:

☐ **Disinformation:** False or misleading content made on purpose to trick, manipulate, or harm others, often for money or power. Examples include fake news, deepfakes, and hoaxes. Fake news is false information presented as real news to mislead people. A deepfake is a manipulated video or audio made using AI to make someone appear to say or do something they didn't. A hoax is a fake story or claim spread to deceive or trick others.

☐ **Misinformation:** False content shared accidentally, without knowing it's wrong. People don't create it but unknowingly spread it.

☐ **Contextual Deception:** Real information twisted or shown out of context to mislead, like mismatched headlines or leaving out key facts.

☐ **Propaganda:** Content, often by governments or organizations, designed to influence opinions and emotions instead of sharing balanced facts. It mixes truth and lies and often plays on feelings.

☐ **Satire:** Funny or exaggerated content that critiques society or politics. While meant as a joke, it can be misunderstood and shared as real.

Bias also plays an important role when it comes to the way we perceive information.

What is Bias?

Bias is when we have an unfair preference for or against something or someone. It affects how we think and can lead us to believe false information. Our beliefs are shaped by many things, like how we were raised or what we've learned. Often, we only believe information that agrees with what we already think, especially if it makes us feel strong emotions like fear or anger.

On social media, we see more of what we like or agree with, creating a "bubble" around us. Bias can also make us trust certain sources, like public figures, even if what they say isn't true, making it easier for false information to spread.

Why is Recognizing Untruths Online and Bias important?

Recognizing untruths online and bias is essential for:

- Promoting Critical Thinking (Evaluating Information Carefully): Being aware of bias and objectivity helps young people think more critically about the information they receive and develop more accurate views on important topics.
- Understanding the World (Increasing Context Comprehension): Approaching information with a critical ear and an open mind helps to make sense of the facts young people see, hear or read everyday, and therefore of the reality they live in.
- Fostering Trust and Accountability (Building Confidence in Sources): Recognizing bias or misinformation allows to hold media and institutions accountable, making sure they share information honestly and fairly.

In the digital age, false news poses a growing risk as the internet becomes a primary source of information for many. Even when not internally trusted, social media remains a major driver of fake news dissemination. Younger audiences are particularly vulnerable due to their higher usage of these platforms. This issue gained attention during the COVID-19 pandemic, where fake health claims spread rapidly.

A 2019 [Ipsos survey](#) showed that 86% of people online have come across fake news, and 67% of it was linked to Facebook. Fake news is seen as a global epidemic, worsening political discourse and internet distrust. Social media platforms, governments, and online trolls are blamed for its spread. Efforts to counter it, like account removal and education, are widely supported, though there's no clear agreement on who should regulate fake news.

Misinformation is everywhere, often dressed up with fake credentials or misleading content. Social media makes it worse by creating echo chambers, where people share unverified information that matches their beliefs. For example, on Facebook, you join a group about fitness and start seeing only posts about extreme diets, making you believe they're the best way to stay healthy, while ignoring other, more balanced advice.

Algorithms often promote exciting or sensational content, even if it's not accurate. Imagine opening Instagram and seeing a viral video of a famous celebrity saying something shocking; the video has dramatic captions but no proof. Even though the video was a deepfake created thanks to AI, many people shared it making many others believe it was indeed true.

An additional challenge in the media is that the line between facts and opinions is sometimes unclear, making it harder to judge credibility. Stopping fake news needs a multifaceted approach aiming at teaching young people how to think critically about the information they see and share.



“ Sophie came across a viral tweet claiming her favorite actor had been arrested for a serious crime. Shocked, she clicked on the hashtag, which was trending with thousands of tweets discussing the alleged incident. Without thinking twice, Sophie shared the news with her followers. Hours later, the actor released a statement affirming the story was entirely fake, a prank started by an anonymous account. Sophie felt embarrassed and realized how quickly false stories can spread and harm someone’s reputation, even if they’re untrue. ”

“ Mark shared a dramatic photo online showing a river turned bright red, claiming pollution had caused a disaster in their city. His friends were outraged and quickly reposted it, sparking concern across social media. Later that evening, someone traced the image back to an old news article—turns out, the photo was taken years ago in another country. Embarrassed, Mark realized he should have fact-checked before sharing. He learned that spreading misleading content, even unintentionally, can cause unnecessary fear and confusion.”

FACT
FAKE

✓ PASSWORD SECURITY CHECKLIST

- ☐ Verify the author's qualifications and background.
- ☐ Cross-check information across multiple reliable sources.
- ☐ Look for supporting evidence (studies, reports, or data).
- ☐ Use fact-checking websites like Snopes, FactCheck.org, or PolitiFact.
- ☐ Ask yourself if the story is trying to provoke any strong emotions like fear, anger, excitement.
- ☐ Pause before reacting or sharing to take time to evaluate and avoid echo chambers.
- ☐ Check if the date of the article is recent.
- ☐ Read beyond the headline to understand if the context matches the article.
- ☐ Check if memes, photos, or videos are being presented out of context.
- ☐ Follow resources on media literacy to improve your ability to spot fake news.





Activity 1: “Fake News Detection Challenge”

KEYWORDS

Fake News, Media Literacy, Fact-Checking, Emotional Manipulation, Critical Analysis

OBJECTIVES

To develop critical thinking skills for identifying bias and untruths in online information.

To promote the use of fact-checking tools for making informed decisions before sharing content.

DURATION

30–45 minutes.

PARTICIPANT AGE

12–18 years old.

MATERIALS AND TOOLS

Printed or digital mixed information sources.

Discussion prompts or checklist for analyzing source credibility.

Access to fact-checking websites (e.g., AFP, Reuters, Snopes, FactCheck.org, PolitiFact)

Projector or screen (if presenting examples as a group).

Description of Activity:

In this challenge, participants will work in teams to evaluate a set of news articles or social media posts. They will analyze each piece for signs of misinformation, such as untrustworthy sources, emotional language, or lack of supporting evidence. After analyzing the content, participants will decide whether the information is real or misleading and justify their decision. If the information is misleading, participants must identify whether it represents disinformation, misinformation, contextual deception (such as fake news, deepfakes, or hoaxes), propaganda, satire, or bias.

Facilitator Instructions:

- ☐ Choose a mix of news articles, social media posts, and headlines, including both authentic and misleading examples (e.g., sensational headlines, emotional language, fake photos, biased sources, personal agendas). Introduce fact-checking tools like Snopes, FactCheck.org, or PolitiFact.
- ☐ Divide participants into discussion groups and have them evaluate each example using the following guiding questions:
 - ☐ About the Source: Who is the source (individual, organization, platform)? Is the source known for accuracy and reliability? Are the author’s credentials or background provided?
 - ☐ About the Content: Is the information backed by evidence, references, or data? Are claims verifiable through other credible sources? Is the tone neutral or emotional? Are any facts missing, distorted, or taken out of context? Are images or videos manipulated (e.g., deepfakes, misleading visuals)?
 - ☐ About the Intent: What’s the likely goal (inform, entertain, persuade, provoke, manipulate)? Is there an agenda or bias? Does it use clickbait, fear, outrage, or humor?
- ☐ Final Judgment: Is the content trustworthy or misleading? Why?

MIS- DIS-INFORMATION - ACTIVITIES

Activity 2: “Compare the Coverage”

KEYWORDS

Media bias, perspective analysis, cross-source comparison, balanced reporting

OBJECTIVES

To develop an understanding of media bias and framing.

To promote the habit of comparing sources before trusting content.

DURATION

45–60 minutes.

PARTICIPANT AGE

15–24 years old.

MATERIALS AND TOOLS

Articles on the same event from different sources.

Analysis worksheet.

Description of Activity:

Participants will examine how different news outlets cover the same event and compare for bias, tone, and credibility of different sources.

Facilitator Instructions:

☐ Select a major news event and provide 3–4 articles from different outlets (mainstream, niche, biased, balanced).

☐ Participants work in groups to analyze:

Who wrote the article?

What is the tone of the coverage?

What facts are included or omitted?

What perspectives are presented?

Is the article trustworthy? Why or why not?

☐ Groups present their analysis and compare across articles.

Suggestions for Facilitators:

Keep the activity simple and interactive, focusing on the contrast between the two scenarios.

Explain that enabling 2FA is easy and can prevent serious risks.

Provide a quick demonstration of how to set up 2FA on a popular platform.

Offer actionable tips for improving privacy settings on popular platforms.





Facilitators play a crucial role in stimulating meaningful discussions and encouraging participants to share personal stories or anecdotes about themselves or others they know. Begin the discussion with general, relatable questions to ease participants into the topic, such as, **“Can you think of any recent examples of fake news that you or someone you know has encountered?”** or **“Do you think social media makes it easier for fake news to spread? Why or why not?”** These open-ended questions encourage reflection and make it easier for participants to share personal experiences or observations about others.

As the discussion progresses, try to pose deeper questions like: **“How might fake news contribute to spreading fear, anger, or division in a group, community or country?”**, **“What are some risks you’ve heard of related to believing fake news?”**, **“What makes people believe fake news, even when it’s obviously false?”** or **“Do you think fake news is always intentional? Can people share false information without meaning to? How can this happen?”**. Use follow-up questions to explore the stories further, such as, **“What role do you think each of us plays in stopping the spread of fake news?”**.

Throughout the discussion, validate participants’ contributions by actively listening, summarizing key points, and showing appreciation for their input. Avoid interrupting and gently redirect the discussion if it veers off-topic. To conclude, summarize the shared stories and insights, highlighting actionable lessons and emphasizing the importance of protecting personal data.

E-BOOKS

- ▶ Manual for School Teachers against Fake News [Download here](#) 
- ▶ Peer to Peer in Youth Information [Download here](#) 

WEBSITES

- ▶ POECD Going Digital Toolkit Policy Note on Disentangling untruths online <https://goingdigital.oecd.org> 



Module 5: InfoMaps and Visual Aids

INTRODUCTION TO INFORMATION TRUSTFULNESS



Objectives

To enhance young people's ability to interpret, question, and discuss digital trends and safety challenges using visual tools such as InfoMaps and infographics.

KEY CONCEPTS

InfoMaps are visual learning tools that organize complex digital information in a way that is easy to interpret and explore. They help youth identify patterns, compare data across regions, and engage with abstract or data-heavy topics like cybersecurity, digital access, or e-governance. InfoMaps support inclusive, visual learning and make it easier for participants to connect global trends with local realities.

KEYWORDS

InfoMaps, digital indicators, visual learning, cybersecurity index, e-government, digital trends

InfoMaps are powerful visual tools that make complex digital topics more understandable, especially for youth. They **visually represent data, patterns, and relationships across regions or indicators**—allowing participants to grasp big-picture dynamics in a concrete and engaging way. By turning statistics and indexes into accessible images, InfoMaps help bridge the gap between global trends and local realities.

In the context of internet safety and digital inclusion, InfoMaps serve as excellent starting points for discussion and reflection. They support visual learning and make it easier to identify disparities, question assumptions, and stimulate critical thinking.

In this Toolkit, you'll find InfoMaps Maps that illustrate several key digital concepts:

Global Cybersecurity Index (GCI): Compares countries' readiness to protect against cyber threats by evaluating legal frameworks, technology, capacity-building, and international cooperation.

E-Government Development Index (EGDI): Measures how well countries use digital technology to deliver public services, considering online services, telecommunications infrastructure, and human capital.

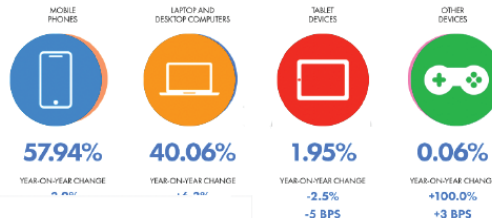
Internet Usage Trends (from DataReportal 2024 & 2025): Country-specific and regional data on digital access, screen time, social media usage, and mobile connections. These maps make visible the diverse digital habits and infrastructure realities among youth globally and locally.

Mapping the Digital Landscape: Data & Trends

GLOBAL OVERVIEW

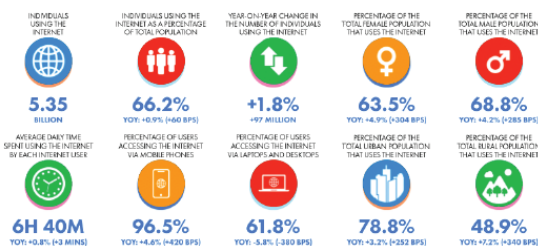
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO VISITORS ACCESSING EACH KIND OF DEVICE



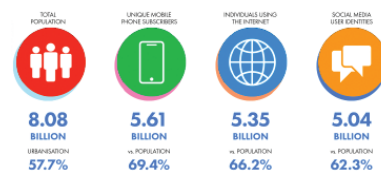
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



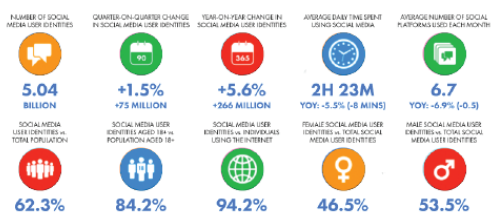
ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES



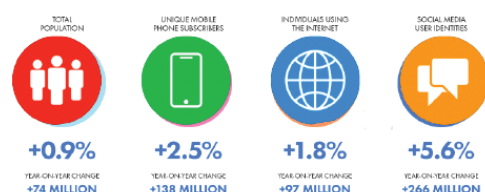
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER ENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



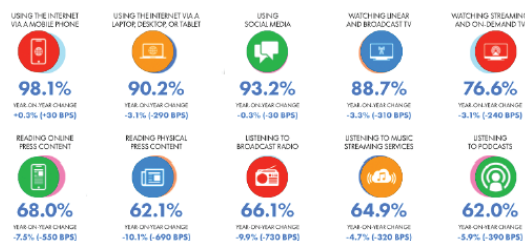
DIGITAL GROWTH

CHANGE IN THE USE OF CONNECTED DEVICES AND SERVICES OVER TIME



MEDIA USE

THE PERCENTAGE OF INTERNET USERS AGED 18 TO 64 WHO CONSUME EACH MEDIA TYPE



Source: Data Reportal. [2024]. Digital 2024: Global Overview.

5. INFOMAPS AND VISUAL AIDS



How to use Infomaps

5.1 Visual Aids and Infographics

InfoMaps are not meant to be interpreted passively—they are designed to be used interactively during training. For example:

Use Case. When discussing cybersecurity in Türkiye, facilitators can show the country's GCI ranking alongside others. This can prompt questions like: “What does this ranking tell us?” or “How do we experience digital threats in our daily lives compared to what this map shows?”

Visual aids—such as infographics, diagrams, timelines, and posters—play a crucial role in making abstract or dense information more accessible, especially for youth. These tools support visual learning by organizing content in a clear, appealing, and memorable format. When thoughtfully designed and used during workshops, they enhance understanding, promote engagement, and support inclusion across different levels of literacy, language, and learning style.

Why Use Them in Digital Safety Education?

InfoMaps simplify complexity. Infographics break down challenging concepts like cybersecurity threats, digital footprints, or disinformation into clear visuals that are easier to grasp.

Visuals grab attention and hold it, making them particularly useful for maintaining interest in long sessions or online formats. InfoMaps support inclusion. For multilingual, neurodiverse, or less confident readers, visual aids offer an alternative entry point into the topic. They reduce reliance on heavy text and support comprehension through imagery, color coding, and structure.

They also create shared understanding. In intercultural or intergenerational settings, where words may not fully translate, visuals can offer a universal language that supports connection and empathy. They are particularly useful in the context of Virtual exchanges by enabling facilitators and participants to start from data for comparing differences and similarities in different countries.

Effective Visual Aids for Internet Safety Topics

A **timeline of digital milestones** can serve as a compelling visual journey through the evolution of internet use. It may include key moments such as the invention of the smartphone, the rise of major social platforms, the implementation of GDPR, or high-profile data leaks. This type of visual helps youth situate themselves within the broader digital transformation and reflect on how quickly the online landscape has changed

around them.

Infographics that **compare safe and unsafe online behaviors** are particularly useful for younger audiences. These visuals place good practices and risky habits side by side—for example, using two-factor authentication versus sharing passwords with friends. Such graphics are practical, culturally adaptable, and make excellent discussion starters for group reflection on everyday choices in digital life.

A **screen time breakdown chart**, whether as a pie chart or bar graph, offers a clear picture of how time is typically spent online. Showing the average daily time dedicated to activities like social media, gaming, streaming, or studying encourages participants to think critically about digital balance, routine, and attention management. This type of visual is especially helpful for sparking conversations about habits.

Posters highlighting **digital rights and responsibilities** can help reinforce foundational knowledge. These might include rights such as privacy, freedom of expression, and informed consent, presented alongside key behaviors that show respect for oneself and others online. These visuals support digital citizenship and give young people language to talk about their place in the digital world.

Finally, **data flow diagrams** can illustrate how personal information travels online. They can show what platforms collect, where that data goes, and how it might be used. These visuals raise awareness about surveillance, targeted advertising, and the importance of informed digital choices. They are excellent tools for introducing concepts related to digital ethics and citizenship.

5.2 How to Use InfoMaps in Training Sessions

Integrating InfoMaps into youth sessions turns passive learning into active exploration. Here's how you can do it effectively.

- ☐ Start with curiosity: Ask questions like, “Where do you think your country ranks in digital safety?” before revealing the InfoMap.
- ☐ Print or project InfoMaps: Use them as backdrops during discussions or small-group work.
- ☐ Pair with reflective activities: Like “My 24-Hour Digital Day” or “Cybersecurity Score Challenge”, which invite youth to relate their own habits to the map data.
- ☐ Use as storytelling tools: Invite youth to interpret the map – “What do you think this says about your country’s internet culture?”

Suggested Activities:

- ☐ Country comparison debates (“Which country is the safest online?”)
- ☐ Mapping one’s personal digital footprint and linking it to local infrastructure
- ☐ Poster creation based on EGD or internet access statistics



5.3 Customizing Visual Aids for Your Audience

The effectiveness of any visual aid depends on how well it speaks to the specific group you're working with. Youth across countries, age groups, and tech-literacy levels will engage differently.

What areas to consider to customize your visual aids:

Language

Adapt your visuals to the audience's language skills. Use simple, clear terms and avoid jargon. For example, replace “two-factor authentication” with “extra password step” for younger or less technical groups. In multilingual settings, provide key terms in both the local language and English (e.g., “cybersecurity / sicurezza informatica”). Where possible, include visual cues (icons, images) alongside text to aid comprehension.

Cultural Relevance

Incorporate local examples, platforms, and cultural references to make InfoMaps and visual aids more relatable. For instance, in North Africa or the Middle East, you might include Anghami or Telegram when mapping social media use, rather than assuming TikTok, Instagram, or Facebook are most popular. In a European session, reference GDPR when discussing data privacy. This helps participants see themselves in the content.

Age Appropriateness

For younger ages (12–14), prioritize highly visual, personal, and interactive activities:

- ☐ Use My Digital Footprint Map or The Global You, which encourage reflection on familiar apps and behaviors.
- ☐ Replace complex terms with icons or emojis (eg lock for security, world for global apps).
- ☐ Use colorful, playful visuals rather than text-heavy slides.
- ☐ For older teens (15+) and young adults:
- ☐ Introduce data comparisons and global rankings (Cybersecurity Score Challenge or E-Gov Explorer).
- ☐ Encourage critical reflection through open-ended questions: How does your country's cybersecurity readiness impact you?
- ☐ Include infographics with clear charts and percentages to stimulate discussion.

Interactivity

Always design visual aids to invite participation: Use editable posters where participants can add stickers or comments (e.g., “Which apps do you trust most?”).

Provide worksheet versions of InfoMaps for small groups to annotate.

Turn key visuals into puzzles or matching games. For example, match icons of common online risks with prevention tips, or match services to their country's EGDI score.

Toolkit Tip: Use editable slides or PDFs so you can adapt visual materials to different sessions or countries.

A well-customized visual aid not only conveys information – it also sparks dialogue and co-creation. Build in moments where participants can actively shape or respond to the visual content.

5.4 How to build an evaluation test

An evaluation test helps facilitators understand what participants have learned, and what may need reinforcement. For youth workshops, it's important to keep assessments light, clear, and engaging, never stressful. Your test should reflect the tone of the session: participatory, inclusive, and age-appropriate.

Multiple-Choice Example (for ages 13–25):

Which of the following is the most secure behavior when using public Wi-Fi at a café?

- A. Checking social media, but avoiding any personal messages
- B. Logging into your email only if it's urgent
- C. Using a VPN and avoiding entering any sensitive login information
- D. Using your mobile hotspot instead of Wi-Fi

This question requires more than recognition; it asks participants to weigh options and apply layered knowledge (e.g., risk management, digital habits, and tool use like VPNs).

True or False Example (with embedded reasoning):

True or False: A platform with a high number of users worldwide is automatically more secure than a local platform.

(False)

Follow-up discussion: Popularity does not guarantee strong data protection or responsible governance. Participants must consider privacy policies, legal frameworks, and local data regulations.

Scenario-Based Multiple Choice (for critical thinking):

You're applying for a scholarship online. The website looks professional, but it asks for your ID number, home address, school transcript, and parents' income—all on the first page. What do you do?

- A. Fill it out quickly to increase your chances
- B. Check the web address and search for reviews or official links
- C. Share it with your friends so they can apply too
- D. Screenshot the form and post it online to ask if it's real



Activity 1: “My Digital Footprint Map”

KEYWORDS

Digital identity, privacy, footprint, awareness.

OBJECTIVES

Build awareness of personal data exposure.
Promote digital responsibility and privacy awareness.

DURATION

30–40 minutes.

PARTICIPANT AGE

12–16 years old.

MATERIALS AND TOOLS

Templates, colored pens, stickers, projector.

Description of Activity:

Participants create a visual representation of their digital presence, mapping out the platforms, apps, and websites they engage with. The goal is to raise awareness about how much personal information is shared and where.

Facilitator Instructions:

☐ Provide a blank “digital world map” template (e.g., cloud shapes, website icons, devices).

☐ Ask participants to write or draw each platform/app they use in a bubble.

For each, they note:

- How often they use it
- What kind of data they share
- Who can see it (public/private)

☐ Compare the app usage from groups’ results with the data on InfoMaps to reflect on trends on app usage on country-level and world wide.

☐ Reflect as a group:

“Which platform do you trust the most? Why?”

“What surprised you about your map?”

“How could you reduce unnecessary sharing?”

Suggestions for Facilitators:

Start by showing a simple example of a digital footprint map to guide participants. Encourage them to include apps or platforms they use daily, weekly, or occasionally, and note what they share and who sees it. Allow creativity, participants can draw, write, or use symbols. Remind the group that sharing is voluntary and there are no wrong answers. After completing the maps, have participants compare their usage with the InfoMaps and discuss similarities or differences. Use reflection questions to close the activity and spark discussion on digital habits and privacy.

Activity 2: “Cybersecurity Score Challenge”

KEYWORDS

Cybersecurity, digital hygiene, personal safety, global index.

OBJECTIVES

Encourage good cybersecurity habits.

Connect personal habits to national/global issues.

DURATION

25–35 minutes.

PARTICIPANT AGE

14–24 years old.

MATERIALS AND TOOLS

Score sheets, country GCI summaries, slides.

Description of Activity:

Using simplified elements from the Global Cybersecurity Index (GCI), participants evaluate their personal cybersecurity practices and compare them with country-level efforts.

Facilitator Instructions:

☐ Present a simple version of the GCI categories:

- Password strength
- Use of 2FA (Two-Factor Authentication)
- Device protection (updates/antivirus)
- Recognizing phishing
- Use of public Wi-Fi

☐ Let participants self-assess and total their scores.

Show GCI results for different countries and compare.

☐ Discussion:

“How secure is your digital life compared to your country’s readiness?”

“What can you improve?”

Suggestions for Facilitators:

Begin by clearly explaining each **GCI category** in simple terms and offer examples to help participants reflect honestly on their habits. Emphasize that this is a self-assessment, not a test, and encourage honest answers. After the scoring, project or hand out selected GCI results from relevant countries. Invite participants to **compare their scores with national scores** and discuss gaps or similarities. Keep the tone light and empowering, focusing on what can be improved rather than what is lacking. Use this moment to introduce small, practical tips participants can start applying immediately.



Activity 3: “Digital Doctors”

KEYWORDS

Digital divide, global comparison, equity, e-government.

OBJECTIVES

Raise awareness of digital inequality.
Foster empathy and global thinking.

DURATION

40–50 minutes.

PARTICIPANT AGE

14–19 years old.

MATERIALS AND TOOLS

Country fact sheets, poster materials, markers.

Description of Activity:

Explore the differences in internet access and digital public services between countries featured in the InfoMap (e.g., Italy vs. Tunisia).

Facilitator Instructions:

- ☐ Divide participants into country teams (Italy, Algeria, Lebanon, etc.).
- ☐ Give each team a profile with key data (EGDI score, internet usage %, youth access).
- ☐ Teams create a visual “Country Profile Poster” highlighting:
 - Digital strengths
 - Weaknesses or barriers
 - Youth opportunities (e.g., jobs, education access)
- ☐ Reflect:

“How does your country’s digital infrastructure impact your daily life?”

“What could improve access for everyone?”

Suggestions for Facilitators:

Start by introducing the concept of digital inequality using a real-world example or a question like, “Do you think everyone in your country has the same online opportunities?” Assign country teams thoughtfully to ensure diversity in discussion. Encourage each team to think like “digital doctors,” diagnosing their country’s strengths and gaps using the provided data. Support groups as they work on their posters, helping them connect the statistics to real-life experiences. During the reflection, prompt participants to consider how digital access affects education, jobs, and participation in society. Emphasize that the goal is not to rank countries but to understand different realities and imagine solutions.

Activity 4: “The Global You”

KEYWORDS

Global tech, platform geography, digital culture

OBJECTIVES

To raise awareness of digital globalization.

To encourage critical thinking about digital sovereignty and cultural influence.

DURATION

30–40 minutes.

PARTICIPANT AGE

13–18 years old.

MATERIALS AND TOOLS

Blank world maps, platform origin sheets, pens

Description of Activity:

Participants map their favorite digital platforms and apps to their country of origin, then reflect on digital globalization.

Facilitator Instructions:

- ☐ Hand out blank world maps.
- ☐ Ask participants to list 5–10 digital platforms they use daily and locate their headquarters on the map (e.g., TikTok – China, WhatsApp – USA).
- ☐ Prompt discussion:
 - “How global is your digital life?”
 - “Do you use any local apps?”
 - “What’s the impact of using mostly foreign platforms?”

Suggestions for Facilitators:

Begin by asking participants what apps or platforms they could not live without to spark curiosity. Then explain that many of the tools we use daily come from different parts of the world. Provide examples to help participants locate headquarters on the map if needed. Encourage participants to work in pairs or small groups to support each other in identifying origins.

During the discussion, guide participants to think beyond geography and reflect on cultural influence, language, and digital dependence. Ask if they’ve ever used a local platform and why global ones tend to dominate. Keep the atmosphere open and reflective, encouraging curiosity rather than criticism.



Activity 5: “E-Gov Explorer: Public Services Online”

KEYWORDS

E-government, digital inclusion, civic tech, comparative analysis

OBJECTIVES

To understand how digital government affects real life.
To build critical thinking and civic engagement.

DURATION

45–60 minutes.

PARTICIPANT AGE

16–24 years old.

MATERIALS AND TOOLS

EGDI InfoMaps, country cards, poster/chart templates

Description of Activity:

Using the E-Government Development Index (EGDI), participants compare how different governments use digital tools to serve their citizens.

Facilitator Instructions:

- ☐ Present EGDI scores via a map (global or regional).
- ☐ Assign teams a country and provide an EGDI breakdown (online services, infrastructure, human capital).
- ☐ Teams investigate:
 - What services are offered online?
 - What challenges remain?
 - How does it affect youth (e.g., digital ID, job search)?
- ☐ Groups present as if pitching improvements to a digital ministry.

Suggestions for Facilitators:

Start by briefly explaining what e-government means and why it matters in everyday life, especially for young people accessing services like education, healthcare, or job applications. When assigning countries, ensure a balance between high and low EGDI scores to encourage comparative thinking. Encourage each team to think critically: what works, what doesn't, and what would make a difference for young users. As teams prepare their pitches, remind them to be creative but realistic, thinking like advisors to a digital ministry. During presentations, prompt the audience to ask questions or offer feedback. This not only fosters engagement but also encourages youth to see themselves as future contributors to digital policy and public innovation.

Activity 6: “Digital Policy Lab”

KEYWORDS

Digital strategy, policy design, governance, cybersecurity, digital equity

OBJECTIVES

To promote systems thinking and real-world policy engagement.

To build digital literacy, strategic planning, and presentation skills.

DURATION

50–60 minutes.

PARTICIPANT AGE

18–25 years old.

MATERIALS AND TOOLS

Country InfoMap data sets, policy brief template, pens or

Description of Activity:

Participants take on the role of policy advisors and draft a national digital strategy based on the InfoMap data (GCI, EGD, and usage trends). They assess their assigned country’s current status and recommend targeted actions to improve digital inclusion, cybersecurity, and e-government services.

Facilitator Instructions:

- ☐ Assign each team a country from the InfoMaps (e.g., Türkiye, Lebanon, Tunisia, Algeria, Italy).
- ☐ Provide them with data on cybersecurity scores, internet usage, and EGD components.
- ☐ Teams identify key weaknesses and set three policy priorities, such as improving public access, enhancing digital skills training, or regulating data use.
- ☐ Each group presents their plan as a five-minute policy pitch, followed by a short Q&A with peers.

Suggestions for Facilitators:

Start by framing the activity with a real-world context: explain how governments use national digital strategies to shape internet access, public services, and cybersecurity readiness. Encourage teams to take a realistic approach, focusing on actionable priorities based on the InfoMap data. Offer guiding prompts such as “What does this country need most: infrastructure, education, or regulation?” and “How would you prioritize limited resources?”

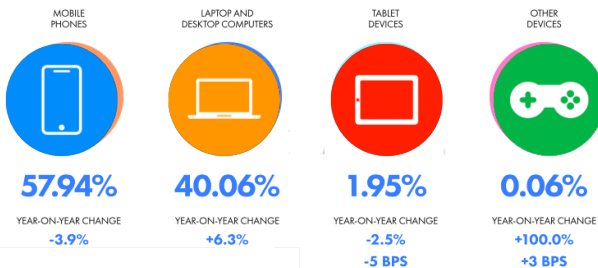
During presentations, moderate a brief Q&A, asking participants to challenge each other respectfully. Emphasize that the goal is not perfection but practicing critical analysis and connecting data to decision-making. Encourage creative, inclusive, and locally informed solutions.

Mapping the Digital Landscape: Data & Trends

GLOBAL OVERVIEW

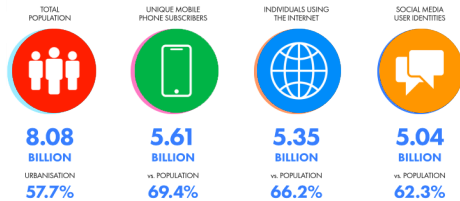
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



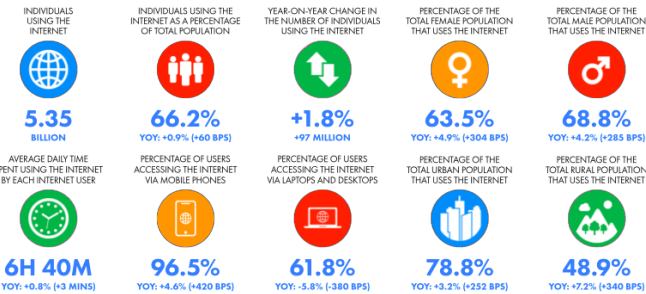
ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES



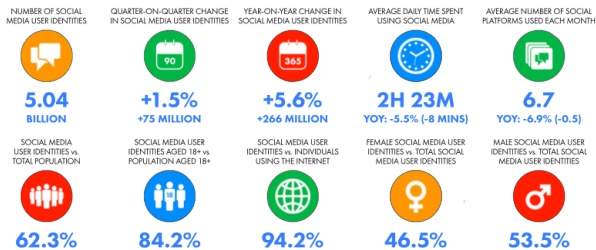
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



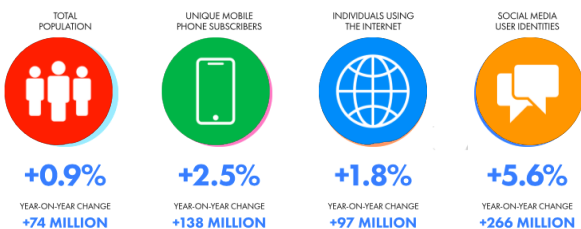
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



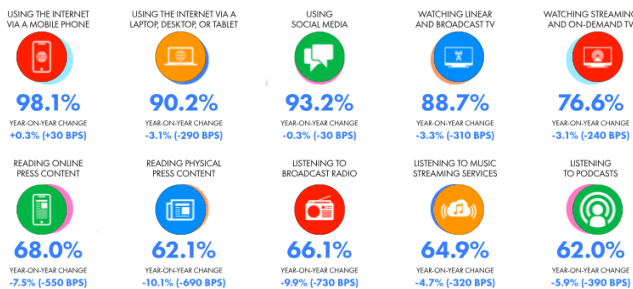
DIGITAL GROWTH

CHANGE IN THE USE OF CONNECTED DEVICES AND SERVICES OVER TIME



MEDIA USE

THE PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO CONSUME EACH MEDIA TYPE

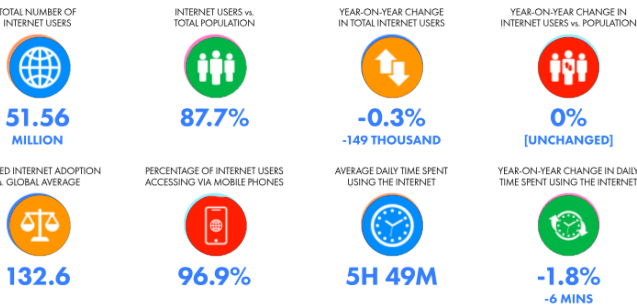


Mapping the Digital Landscape: Data & Trends

ITALY

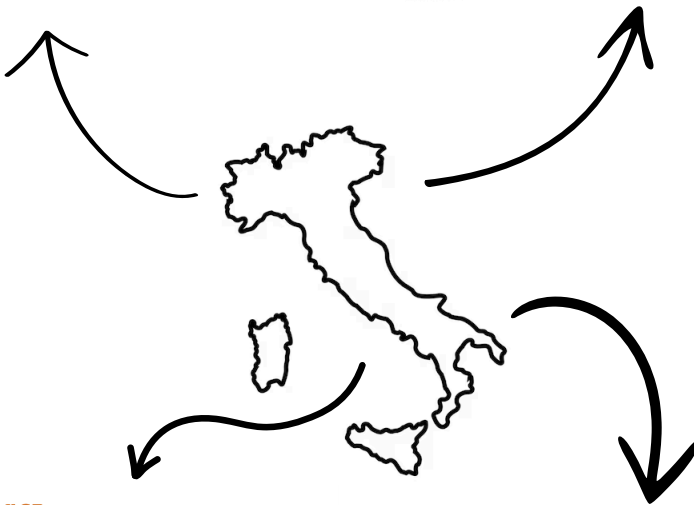
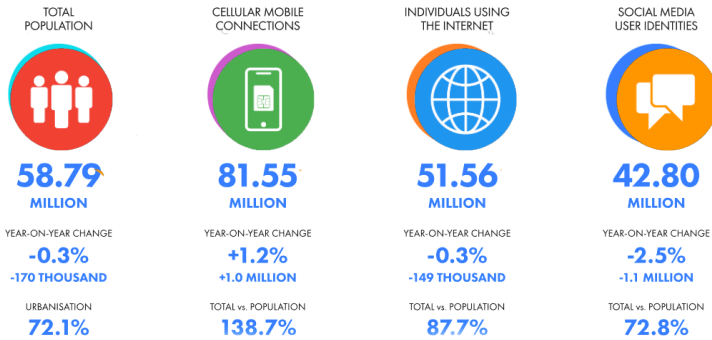
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



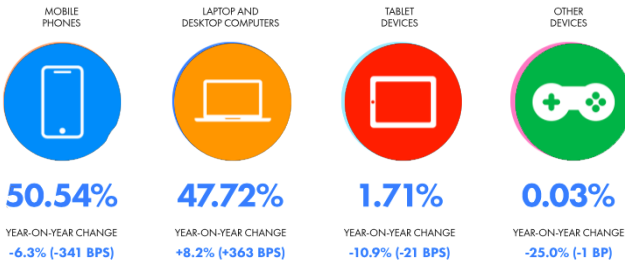
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.



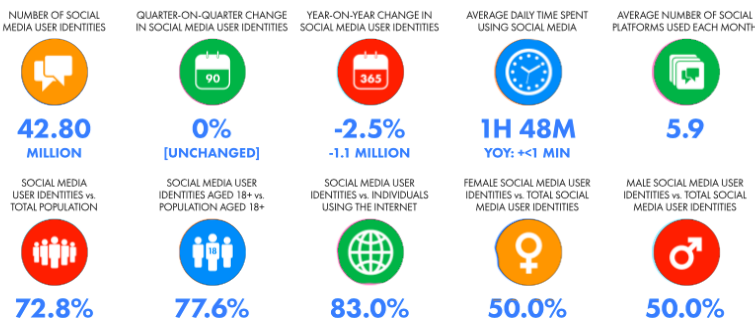
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



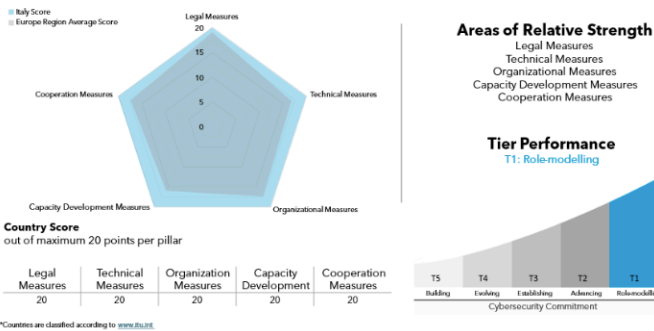
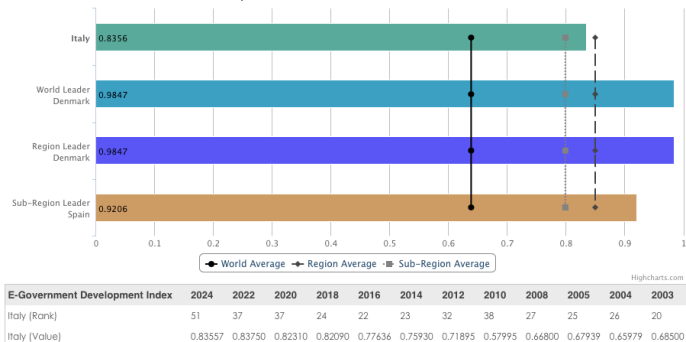
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



Source: Data Report, (2024), Digital 2024: Italia.

E- Government Development Index 2024

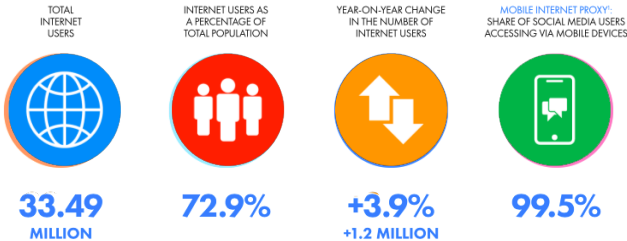


Mapping the Digital Landscape: Data & Trends

ALGERIA

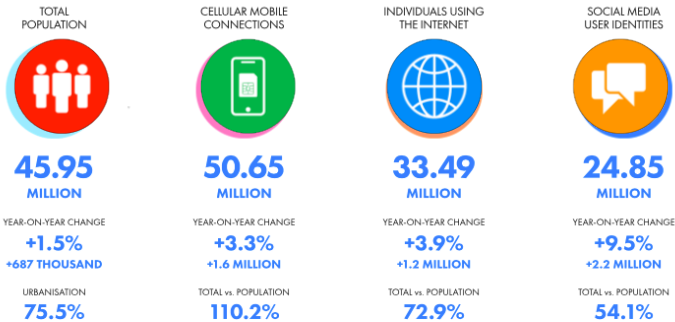
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



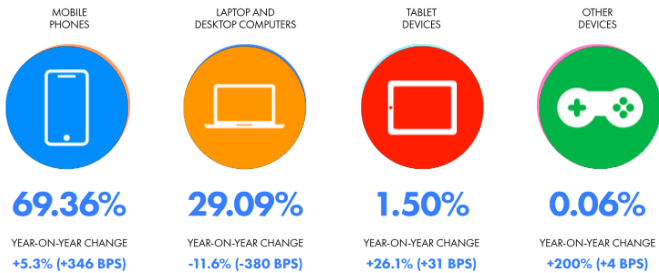
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.



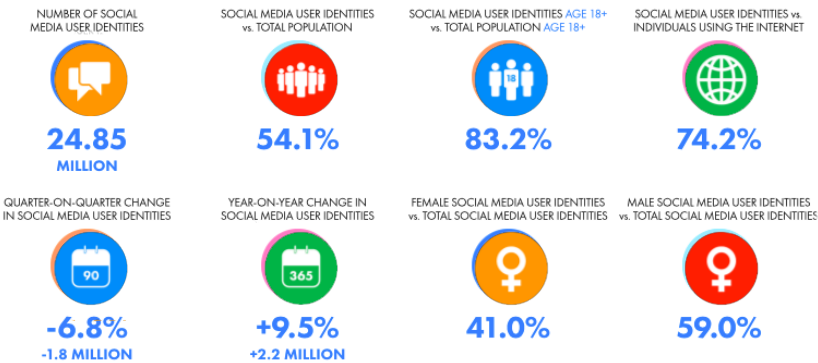
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



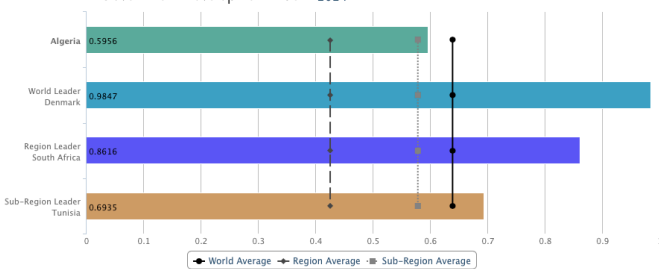
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



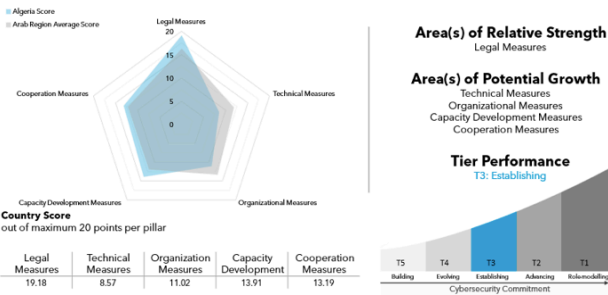
Source: Data Reportal, (2024), Digital 2024: Algeria.

E-Government Development Index 2024



E-Government Development Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Algeria (Rank)	116	112	120	130	150	136	132	131	121	123	118	91
Algeria (Value)	0.59556	0.56110	0.51730	0.42270	0.29991	0.31064	0.36077	0.31810	0.35150	0.32423	0.32476	0.36993

Source: United Nations (UN), (2024), E-Government Knowledge Database.



*Countries are classified according to www.itu.int

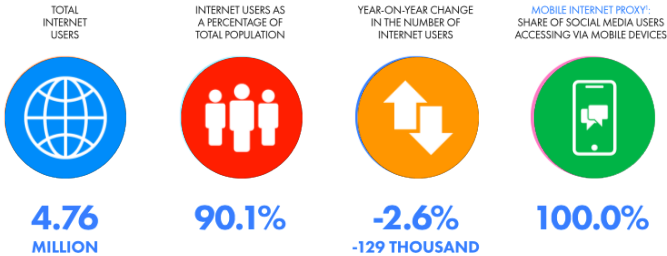
Source: International Telecommunication Union (ITU), (2024), Global Cybersecurity Index

Mapping the Digital Landscape: Data & Trends

LEBANON

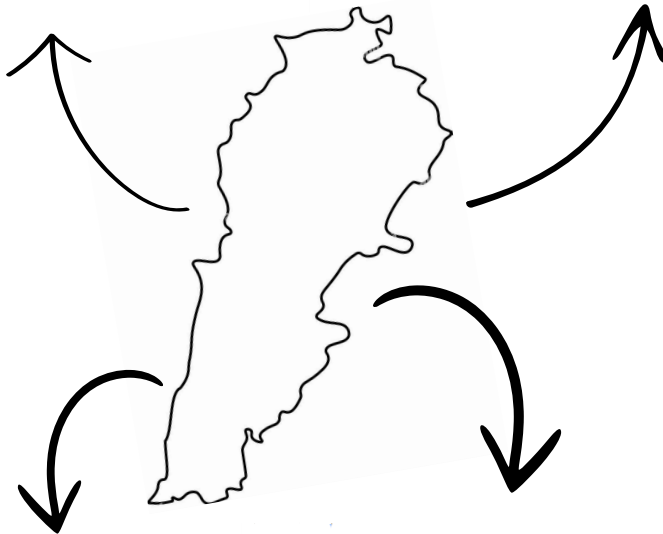
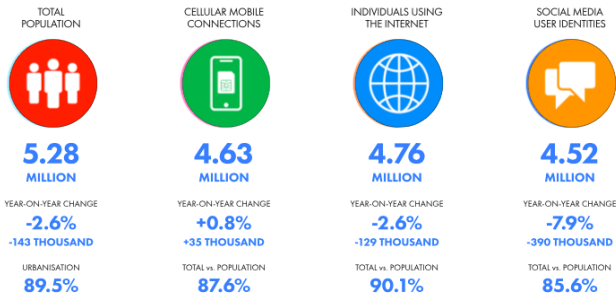
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



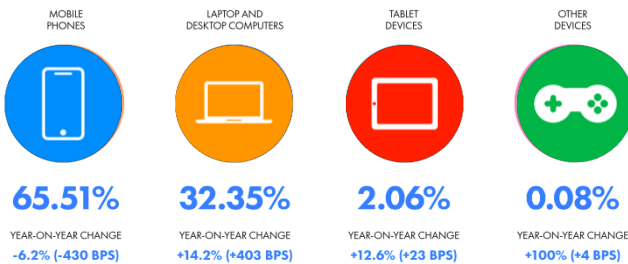
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPAREABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.



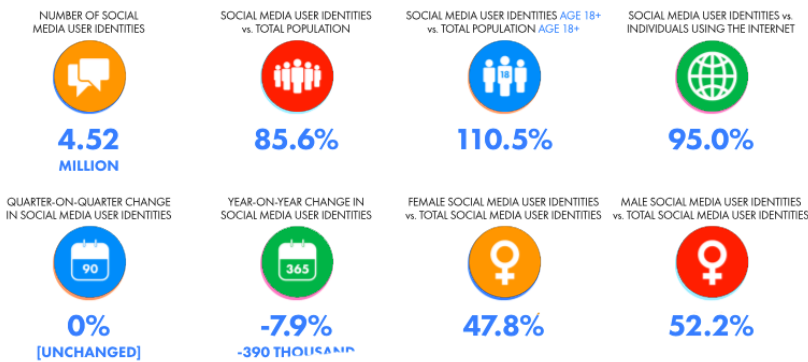
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



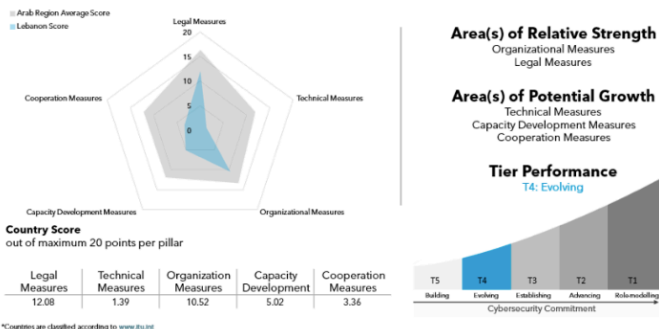
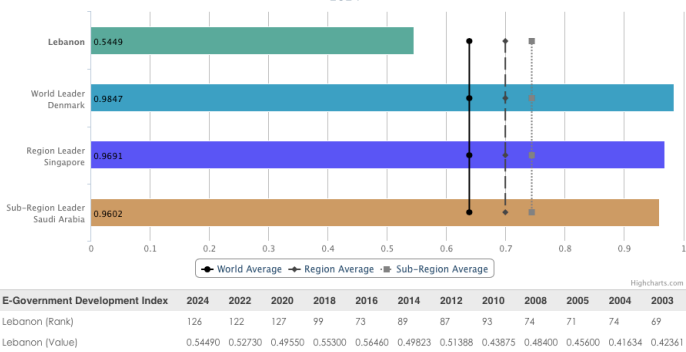
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



Source: Data Reportal, (2024), Digital 2024: Lebanon.

E-Government Development Index 2024

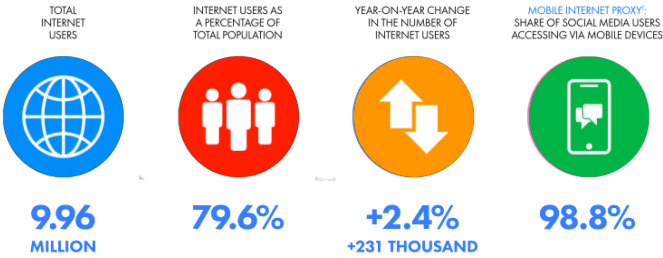


Mapping the Digital Landscape: Data & Trends

TUNISIA

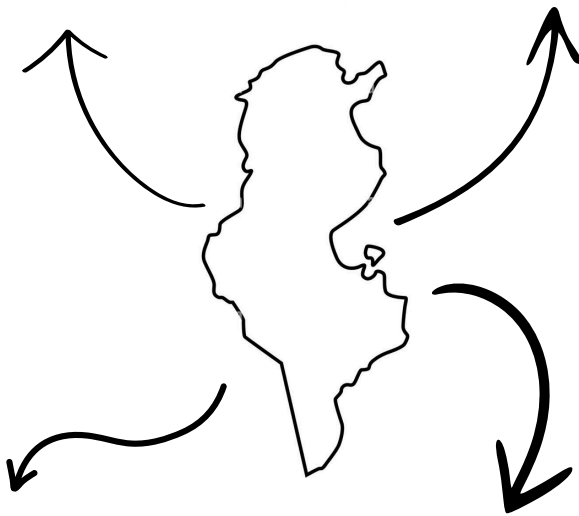
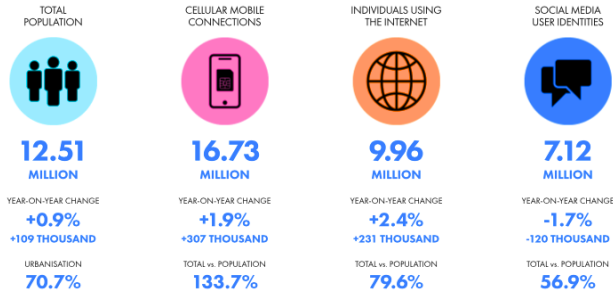
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



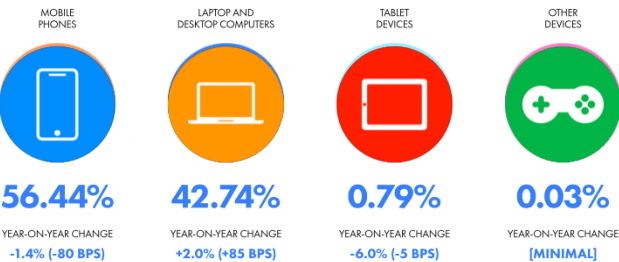
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT DIFFERENCES TO SOURCE DATA AGAIN THAT TUNISIA'S UNIDENTIFIED AND NOT COHERENT WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.



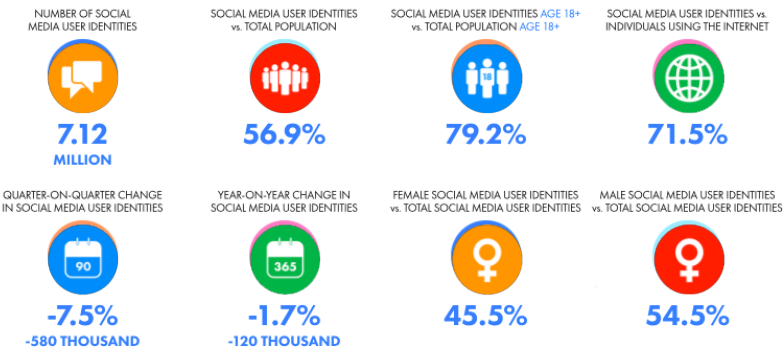
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



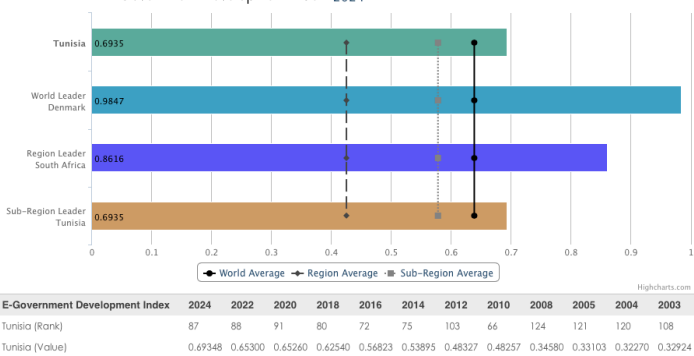
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE [NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS]

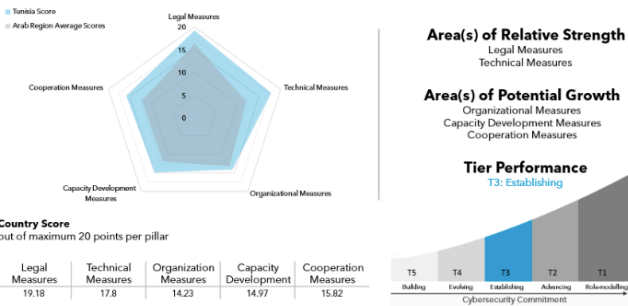


Source: Data Reportal, (2024), Digital 2024: Tunisia.

E-Government Development Index 2024



Source: United Nations (UN), (2024), E-Government Knowledge Database.



*Countries are classified according to www.itu.int

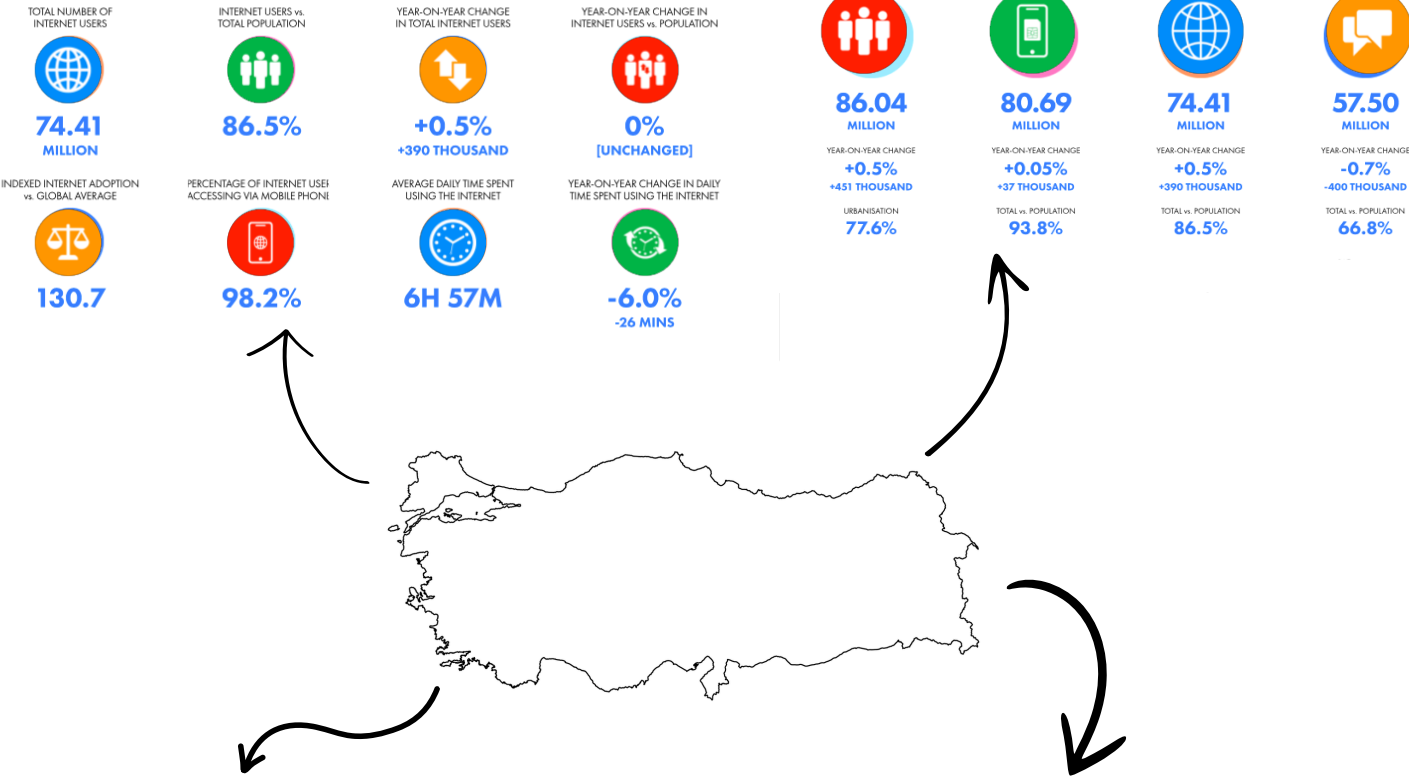
Source: International Telecommunication Union (ITU), (2024), Global Cybersecurity Index

Mapping the Digital Landscape: Data & Trends

TÜRKİYE

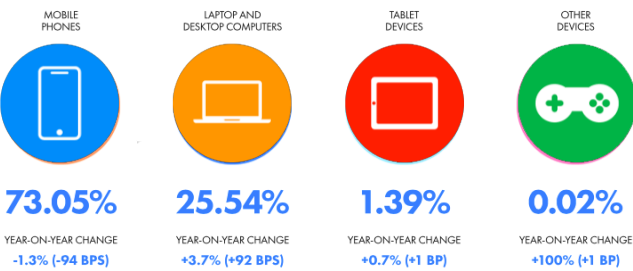
OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



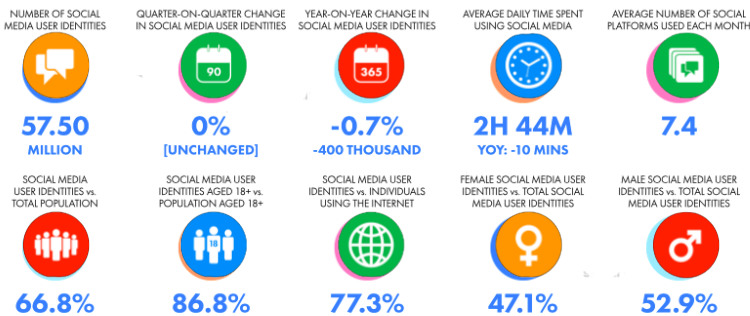
SHARE OF WEB TRAFFIC BY DEVICE

PERCENTAGE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS RUNNING ON EACH KIND OF DEVICE



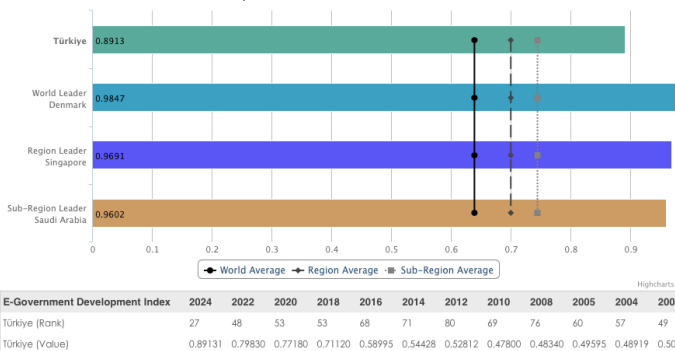
OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)

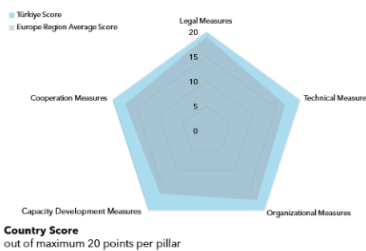


Source: Data Reportal, (2024), Digital 2024: Türkiye.

E- Government Development Index 2024



Source: United Nations (UN), (2024), E-Government Knowledge Database.



*Countries are classified according to www.itu.int

Source: International Telecommunication Union (ITU), (2024), Global Cybersecurity Index

5. HOW TO USE THIS TOOLKIT



ACTIVITIES AND EXERCISES

Objectives

To help facilitators create inclusive and interactive learning experiences using the Toolbook. To equip youth workers with strategies to engage young people in digital safety and promote critical, responsible online behavior.

KEY CONCEPTS

This chapter focuses on how to implement and adapt the Toolbook's activities in ways that promote accurate understanding, meaningful participation, and safe exploration of digital life. At its core, this approach is based on principles of participatory, context-sensitive, and experience-driven learning. Activities are structured to develop digital skills and interpersonal and critical thinking capacities.

KEYWORDS

Experiential learning, peer-to-peer education, facilitation, adaptation, inclusion, digital resilience

Every day, we are surrounded by information—on social media, in messages from friends, on websites, videos, and news platforms. But not all the information we see is accurate or trustworthy. Some of it is incomplete, misleading, or even purposely false. That's why learning how to recognize truthful information has become an essential skill for young people navigating the digital world.

Information trustfulness means knowing how to tell whether what we read or hear is reliable, accurate, and fair. It involves asking questions like: Who is sharing this? Why are they sharing it? Is there evidence to support it? Trustworthy information comes from sources that are open, balanced, and based on facts—not on emotions or manipulation.

In this module, you'll explore what makes information credible and how to spot warning signs of misinformation and disinformation. You'll also learn how to check sources, identify bias, and use fact-checking tools. These skills are important not only for protecting yourself, but also for helping your community stay informed and make good decisions.

By the end of this module, you will be better equipped to think critically, ask the right questions, and become someone others can count on for sharing honest and responsible content. Being able to recognize and promote trustworthy information is a key part of being a responsible digital citizen.



5.1. IMPLEMENTING THE TOOLBOOK



5.1.1. Introduction: From Theory to Practice

In today's digital world, knowing how to navigate the internet safely is not just reaching the right information, but it is strongly connected to developing the ability to think critically, respond wisely, and act with confidence and awareness. This transformation requires more than reading facts or listening to lectures. Young people need opportunities to explore real-life scenarios, reflect on their own behaviors, and engage with others in meaningful conversations about digital safety. That's where experiential learning comes in, particularly through bottom-up, participative approaches and peer-to-peer learning that value the voices, experiences, and active contributions of young people themselves.

The activities and exercises proposed in this Toolbook are designed to support facilitators, educators, and youth workers in turning theory into practice. By using methods that involve discussion, collaboration, creativity, and hands-on interaction, these tools help participants internalize concepts and build practical digital skills. When young people are actively engaged, they are more likely to connect what they learn to their own lives, and to remember and apply it.

A key part of this approach is the role of the facilitator. Facilitators are not just instructors, they are guides who create the conditions for safe, inclusive, and dynamic learning spaces. Their task is to encourage openness, ensure that all participants feel heard and respected, and adapt the activities to meet the needs of different age groups and cultural contexts. The ability to hold space for dialogue, curiosity, and shared learning is at the heart of effective digital safety education.

Ultimately, the aim of these activities is to empower young people. Through experiential learning, they can develop essential outcomes such as digital resilience, critical thinking, and safer online behavior. This chapter offers practical guidance on how to implement and adapt these activities to meet the needs of diverse youth groups, helping them move from digital vulnerability to digital empowerment.

5.1.2. Categories of Activities in the Toolbook

Icebreakers & Group Discussions

Icebreakers are short, playful, and engaging activities that help participants relax and feel part of the group. They are especially useful at the beginning of a workshop to reduce anxiety, break down social barriers, and set a positive tone. Icebreakers should be inclusive, culturally sensitive, and tailored to the age and background of participants. Ideally placed at the very start of a session, they help foster trust and open the door to active participation. Icebreakers are often suitable for adults as well as younger participants and need not be intellectually challenging. They also serve to build cohesion in the group and let participants familiarize with each other.

Group discussions invite participants to reflect on their experiences, express opinions, and listen to others in a safe environment. They are best used after an initial icebreaker or to introduce or conclude key concepts. Use open-ended questions to stimulate dialogue, and organize small groups or circles to ensure equal participation. Facilitators should moderate gently, set clear ground rules for respect, and encourage peer-to-peer learning and bottom-up contributions. It's important to be attentive to group dynamics: facilitators may need to step in if one voice dominates or if discussions drift off-topic. Ensure all participants feel heard and supported, and adapt the pace or topic when needed. These discussions support critical thinking and allow deeper exploration of sensitive topics in a collaborative and participative way.

Role-Playing & Case Studies

Simulating real-world online scenarios helps youth step into different roles and explore consequences of digital choices. These formats promote empathy, decision-making, and critical analysis. Facilitators should keep scenarios realistic, assign roles carefully, and allow time for post-activity reflection. These activities work especially well after initial trust has been established in the group, often in the middle or second half of a workshop. They encourage deeper engagement and are highly effective in participative approaches where peer-to-peer learning and co-construction of meaning are central. Practical uses include enacting cyberbullying cases, fake news analysis, or privacy dilemmas. Provide clear instructions, allow preparation time, and lead structured reflection to unpack lessons. Adjust complexity depending on participants' age and digital experience to ensure relevance and accessibility.

Interactive & Collaborative Activities

These activities promote hands-on learning, teamwork, and creativity. Through games, simulations, collaborative challenges, or group problem-solving, participants build digital resilience and communication skills while actively engaging with the content. These activities play a different role from group discussions or case studies, as they emphasize doing rather than discussing or observing. They are especially useful after a concept has been introduced, allowing participants to test and apply knowledge in a more dynamic format. Practical uses include creating infographics on digital rights, designing posters on safe online habits, or completing digital escape rooms that explore cybersecurity threats. Use varied formats—physical, digital, creative—and ensure instructions are clear and age-appropriate. These activities are particularly important in participative approaches, where co-construction of knowledge and peer exchange are central. They should be scheduled after group trust has been built, often in the middle of workshops when energy levels are high. Facilitators should circulate and guide groups without dominating, encouraging reflection and teamwork throughout the process.

Guided Debriefing

Reflection is essential to cement learning. Debriefing activities help participants process emotions, evaluate what they learned, and connect insights to real-life behavior. These activities play a unique role compared to previous ones, as they are not about learning new content, but about integrating and internalizing what has already been explored. They are best placed at the end of key sessions or at the close of the workshop day, when participants have completed a significant exercise or discussed complex issues.



Facilitators should ask open-ended questions, validate emotions, and highlight key takeaways and strategies for applying them beyond the session. For example, after a role-play on online harassment, facilitators might ask: “What did you feel in your role?” or “How would you act differently in real life?” Managing this stage requires sensitivity and listening skills. Facilitators should watch for emotional fatigue or discomfort and ensure the space remains respectful and supportive. Guided debriefing reinforces learning, strengthens group cohesion, and gives participants the tools to bring insights from the workshop into their daily digital behavior.

5.1.3. Facilitator Guidelines for Implementation

Working with youth on digital safety requires more than just delivering content. Facilitators play a key role in shaping how participants engage with the material, with each other, and with their own digital behaviors. These guidelines are designed to help facilitators implement the activities from this Toolbook in inclusive, engaging, and adaptable ways. Whether you are working with young people in schools, community centers, or online settings, these strategies support effective learning and meaningful participation.

Start every session with an activity that breaks the ice and sets a positive tone. **Icebreakers** are essential for helping participants feel comfortable, particularly in mixed or unfamiliar groups. Introduce clear and simple ground rules for participation, such as active listening, no interrupting, and the right to pass on questions. Use body language, tone, and openness to model trust and respect. Facilitators should also be transparent about the goals of the session, giving young people a sense of ownership over the learning process.

Young people relate best to **scenarios** that reflect their daily lives. Ground activities in examples that resonate with their experiences, like social media dilemmas, messaging apps, or gaming environments. Avoid overly abstract language. Instead, use concrete examples (e.g., “Have you ever seen a fake giveaway on Instagram?”) to spark discussion. When appropriate, bring in short videos, screenshots, or news stories to illustrate concepts. Real-life examples help bridge the gap between theory and practice and allow participants to see the relevance of the topic.

Facilitators must ensure that **all participants feel valued and included**. Monitor group dynamics carefully. Some participants may be shy or unsure, while others may dominate conversations. Use techniques like round-robin sharing, small group discussions, or written reflections to make space for quieter voices. Encourage active listening and model this behavior. Acknowledge every contribution with respect, and if necessary, gently redirect dominant participants to allow others to speak. Diversity of voices enriches the learning environment and supports peer-to-peer discovery.

No workshop goes exactly according to plan. Youth energy, attention span, group chemistry, or unexpected challenges may require real-time adjustments. Be prepared to rearrange activities,

shorten or lengthen discussions, or shift the format (e.g., from plenary to small group). Pay attention to signals from the group. Are they bored, restless, confused, or energized? Use **energizers** or short breaks if needed. Flexibility is key to maintaining engagement and ensuring that learning is responsive to the group's needs.

Encourage youth to **share** their own digital experiences, both positive and negative. Peer learning is a powerful method that fosters trust, reduces feelings of isolation, and supports critical thinking. Design activities where participants can co-create content. For example, developing digital charters, solving online dilemmas together, or storytelling exercises. Highlight that participants are experts in their own digital lives, and that their experiences are valuable contributions to group learning.

© An **energizer** activity is a short, engaging exercise designed to boost energy, re-focus attention, and create a more dynamic group atmosphere during a workshop or training. Typically lasting between 2 and 10 minutes, energizers are especially useful after breaks, during long sessions, or when participants show signs of fatigue or disengagement. They often involve movement, creativity, humor, or light competition, and are meant to re-activate participants' minds and bodies, improve mood, and strengthen group cohesion. Energizers should be inclusive, simple, and adapted to the group's age, cultural background, and comfort level.

Building a space where young people feel safe to express themselves is essential. Reinforce that there are no wrong answers when exploring digital safety. Emphasize that making mistakes or changing opinions is part of the learning journey. **Use inclusive language and be sensitive to cultural, gender, and social differences within the group.** Address inappropriate comments or exclusionary behavior immediately and respectfully. Include confidentiality agreements when appropriate, especially when dealing with sensitive or personal topics.

Young people have different levels of digital literacy, maturity, and cultural context. This Toolkit offers **flexible structures** that facilitators should adjust as needed. For younger participants or those with less online experience, simplify tasks and provide more guidance. For older or more digitally savvy youth, introduce complexity and critical thinking challenges. When possible, adapt case studies or role-playing exercises to reflect local examples or common platforms used in the community. Using local references makes the learning more concrete and relevant.

After each activity, make time to reflect. Ask **open-ended questions** such as: "What surprised you in this activity?" or "How could you use this idea in your own life?" Help participants connect the session to their behavior, habits, and digital environment. This step transforms surface-level knowledge into deeper understanding and long-term change. Provide take-home materials or small challenges (e.g., "Try turning off notifications for one day") that extend the learning beyond the workshop.

Remember that your role is not to be the expert in every topic, but to guide the group's exploration in a supportive, honest, and responsive way. Facilitation is about listening, adapting, and fostering growth—not about having all the answers. Use this Toolkit as a flexible guide, and trust the group's curiosity and creativity to lead to meaningful learning.



SAFE CHANGES

Social Awareness and Financial, Emotional
Connecting Headways for the Advancement
of New Generations' Electronic Safety



Co-funded by the European Union. The views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



**Co-funded by
the European Union**



SAPIENZA
UNIVERSITÀ DI ROMA

