



Co-funded by
the European Union

MODULE 09

MEDIA LITERACY AND ONLINE SAFETY

DIGITAL RURAL EUROPEAN ART
AND MEMORY



Project partners



Project DREAM
Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122



Co-funded by
the European Union

Project information:

DREAM - Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122

Funded by the European Union. However, the views and positions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or SAAIC. Neither the European Union nor the granting authority can be held responsible for them.



How to use this E-book

You can read this material before, during or after the session. Each section introduces a concept and connects it with a practical activity. The activities are designed for beginner adult learners. They do not require advanced technical knowledge. The goal is to build habits: pause before sharing, check sources, protect accounts, review privacy and ask for help when needed.

The module also includes a Learn by Playing section. This is not an appendix: it is a practical part of the module where learners apply the theory through short decision-making challenges inspired by real media literacy and cybersecurity quizzes.

At the end of the module, learners complete an integrated activity: they analyse a piece of online content, check its reliability and prepare a short online safety plan.



Sagrada Família, Spain

MODULE INFORMATION

 Module number 09	 Level Beginner
 Topic Safety online and media literacy	 Format Hybrid learning
 Duration 3 hours	 Main output Online Safety Plan

About this module

This ebook accompanies DREAM Module 9, dedicated to media literacy and online safety. Its purpose is to help learners use digital media with greater awareness, protect themselves online and make better decisions when reading, sharing or publishing information.

Media literacy is not only about detecting fake news. It includes understanding who created a message, why it was created, how it reaches us, what evidence supports it, what emotions it activates and what risks appear when we share it.

Online safety is connected to this. A person who can evaluate information also needs to protect accounts, recognise scams, manage privacy, respond to harmful behaviour and know where to ask for help.

For DREAM, this module supports digital participation, cultural work and community projects. Learners may use online platforms to share local stories, images, videos, models or educational resources. They need to do this critically, safely and respectfully.



Learning Objectives

- Understand what media literacy and online safety mean in everyday digital life.
- Distinguish between fact, opinion, interpretation, advertising and manipulation.
- Evaluate online sources using basic credibility checks.
- Recognise misinformation, disinformation, clickbait and emotional manipulation.
- Understand how algorithms, influencers and social platforms can shape what people see.
- Apply basic fact-checking habits before sharing information.
- Protect accounts using strong passwords, password managers and multi-factor authentication.
- Recognise common online risks such as phishing, smishing, fake shops, impersonation and scams.
- Use resources such as INCIBE and Have I Been Pwned to improve online safety.
- Practise media literacy and online safety through gamified challenges with scenarios, choices, feedback and reflection.
- Prepare a simple personal or project-level online safety checklist.

Index

1. What is media literacy	3
2. Why media literacy matters for DREAM	5
3. Fact, opinion, interpretation and advertising	7
4. How online information reaches us	9
5. Misinformation, disinformation and manipulation	11
6. Source evaluation and fact-checking habits.....	12
7. Images, videos and AI-generated content.....	14
8. Privacy, digital footprint and personal data	16
9. Online safety basics: accounts, passwords and devices.....	18
10. INCIBE recommendations and trusted help resources	20
11. Have I Been Pwned and data breach checks.....	21
12. Shared file safety: Telegram, direct downloads and compressed archives.....	23
13. Online scams, phishing and social engineering	26
14. Cyberbullying, hate speech and respectful participation	28
15. Safe publishing for community and heritage projects	30
16. Learn by Playing: Media Literacy and Cyber Safety Challenges.....	32
17. Final activity	34
18. Digital Wellbeing Tip	36
19. Basic glossary	37
20. Module closing.....	38
Bibliography	39

1. What is media literacy

Media literacy is the ability to access, understand, evaluate, create and share media messages responsibly. It applies to news, social media posts, videos, images, podcasts, search results, advertising, websites and AI-generated content. A media literate person does not believe everything immediately but also does not reject everything automatically. The skill is to ask better questions: who made this, what evidence is given, what is missing, who benefits and what should I check before sharing?

Media literacy also includes understanding that media messages are constructed. A headline, photograph, music choice, editing style or thumbnail can influence how we feel about a topic before we read the details.



Key Concepts

Media literacy: the ability to access, understand, evaluate, create and share media content critically and responsibly.

Source: the person, organisation, publication, website or other origin from which information or media content comes.

Message: the main idea, information or impression that a piece of media communicates to its audience.

Evidence: information used to support a statement or claim, such as facts, data, documents, photographs, expert knowledge or other verifiable material.

Audience: the people a media message is intended to reach or is likely to reach.

Purpose: the reason why a media message was created, for example to inform, explain, persuade, entertain, promote something or encourage people to act.



Practical Task

Choose one online post and answer:

- who created it?
- what is it trying to make you think or do?
- what evidence does it provide?

Mini tip: Do not only ask whether a message is true; ask how it is trying to affect you.

2. Why media literacy matters for DREAM

DREAM learners may use digital tools to document local heritage, publish project results, share training materials or participate in online communities. These activities require trust and responsibility. When a community project publishes content online, it becomes part of the information environment. A wrong image credit, an exaggerated claim, a misleading statistic or an unsafe publication can damage credibility.

Media literacy helps learners become better participants, not only better consumers. They learn to search, compare, interpret, create and share with care.

For cultural and heritage work, media literacy also protects context. A story, object or image should not be removed from its meaning or used in a way that confuses the audience.



Key Concepts

Digital participation: Taking part in digital spaces by contributing information, ideas, knowledge or content, rather than only receiving information.

Community memory: The stories, photographs, experiences, traditions and knowledge through which a community remembers and understands its past.

Credibility: The degree to which information or content can be considered trustworthy. Credibility is strengthened by accuracy, reliable sources, correct attribution and transparency about uncertainty.

Context: The background information needed to understand something correctly, such as who created it, where and when it comes from, what it represents and why it matters.

Responsible publishing: Checking content before sharing it and considering accuracy, sources, permissions, privacy, attribution and possible effects on the people or community involved.



Practical Task

List three types of content a DREAM project could publish online and one risk for each.

Mini tip: A good digital project is not only visible; it is trustworthy.

3. Fact, opinion, interpretation and advertising

A fact can be checked against evidence. An opinion expresses a point of view. An interpretation explains what something may mean. Advertising tries to persuade people to buy, click, subscribe or support something. Online content often mixes these categories. A video may include facts, personal opinions, sponsored products and emotional storytelling. A social media post may look like information but actually work as promotion. Learners should practise separating the claim from the emotion. If a message says that something is shocking, urgent or obvious, the reader should still ask what evidence supports it.



Key Concepts

Fact: A statement that can be checked and supported by reliable evidence.

Opinion: A personal view, belief or judgement. An opinion may be informed by facts, but it cannot be proven in the same way as a factual claim.

Interpretation: An explanation of what information, an event, image or source may mean. Different people may interpret the same material differently, so the reasoning and evidence behind an interpretation should be clear.

Advertising: Content created to promote a product, service, organisation or activity and encourage people to take a particular action, such as buying, visiting or registering.

Sponsored content: Content that has been paid for or otherwise supported by a company or organisation. It should be clearly identified so that audiences can distinguish it from independent editorial or informational content.

Evidence: Information used to support or verify a claim, such as an official document, photograph, dataset, record, expert source or other reliable material.



Practical Task

Mark three sentences from an online article as fact, opinion, interpretation or advertising.

Mini tip: Before reacting, identify what kind of message you are reading.

4. How online information reaches us

People do not see online information randomly. Search engines, social networks, video platforms and recommendation systems decide what appears first, what is repeated and what seems popular. **Algorithms** can be useful because they help filter huge amounts of content. But they can also create narrow information habits, repeat similar viewpoints and reward emotional or extreme content.

Influencers, online communities and platform design also shape attention. Likes, shares, comments, notifications and trending sections can make content feel important even when it is not reliable.



Key Concepts

Algorithm: A set of rules or calculations that a digital system uses to process information and decide what content or results to show.

Recommendation: Content suggested to a user based on signals such as previous activity, interests, popularity or platform rules.

Feed: The continuously updated stream of posts, videos, news or other content shown on a platform.

Influencer: A person who has built an audience online and can shape what followers notice, discuss, trust or buy.

Platform design: The way a digital platform is structured, including its buttons, notifications, layout and features, which can influence how people behave and what they see.

Attention: The limited mental focus people give to information. Many digital platforms are designed to attract and hold attention for as long as possible.



Practical Task

Compare the first results for the same topic on two platforms. Are they similar or different?

Mini tip: What you see online is selected, not neutral.

5. Misinformation, disinformation and manipulation

Misinformation is false or inaccurate information shared without necessarily intending harm. **Disinformation** is false or misleading information created or spread deliberately to deceive.

Manipulation can use real facts in a misleading way. A post may use an old image, remove context, exaggerate a statistic, use a false expert or present a single example as if it proved a general rule.

Clickbait uses curiosity, fear or anger to make people click. Emotional manipulation is powerful because people often share before checking when content confirms what they already feel.



Practical Task

Find a headline that uses strong emotion. Rewrite it in a neutral way.

Mini tip: Strong emotion is a signal to slow down, not to share faster.

Learn by playing: after this section, try Challenge 3, Fake News Lab, in *Section 16*. It turns misinformation techniques into a short decision-making activity.

6. Source evaluation and fact-checking habits

A basic source check starts with simple questions: who published this, when, where, with what evidence and with what purpose? If the source is unclear, the information should be treated carefully. **Cross-checking** means comparing the claim with other reliable sources. Official institutions, recognised media, academic sources, specialised organisations and fact-checking bodies can help, but they should still be read critically.

Fact-checking is not only for journalists. A learner can practise small habits: read beyond the headline, check the date, search the same claim elsewhere, inspect the URL, look for the original source and avoid sharing screenshots without context.



Key Concepts

Source: The person, organisation, document, website or other material from which information comes.

Credibility: The degree to which a source or piece of information can be considered trustworthy based on factors such as expertise, transparency, accuracy and evidence.

Evidence: Information that supports or helps verify a claim, such as documents, data, photographs, records, research or other reliable sources.

Cross-checking: Comparing the same claim or information with other independent sources to see whether they confirm, contradict or add context to it.

Original source: The earliest or primary source from which information, an image, quotation, statistic or claim comes, rather than a later repost, summary or copy.

Fact-checking: The process of checking whether a claim is accurate by examining evidence, identifying the original source and comparing reliable information.

Mini tip: If you cannot find where a claim comes from, do not help it travel.

Learn by playing: after this section, try Challenge 3, Fake News Lab, in *Section 16*, and use the source-checking habits before choosing an answer.

7. Images, videos and AI-generated content

Images and videos feel convincing because they look direct. However, they can be edited, taken out of context, staged, generated by AI or reused from another event. A useful habit is **reverse searching** an image, checking whether the same photo appeared earlier, looking for visual inconsistencies and asking whether the image source is reliable.

AI-generated content creates new challenges. Text, images, voices and videos can imitate real people or realistic events. The answer is not panic, but verification: check context, source, evidence and whether trusted sources report the same event.



Key Concepts

Edited image: A picture that has been changed after it was taken or created.

Context: The information around an image or message that helps us understand what it really shows or means.

Reverse search: A way to search the internet using an image instead of words, to see where else the image appears.

Deepfake: A fake or altered image, video or audio made with AI so that it can look or sound real.

AI-generated content: Text, images, video or audio created partly or fully by artificial intelligence.

Verification: Checking whether information, an image or a claim is real, accurate and trustworthy.



Practical Task

Compare two images of the same topic and identify what context each one gives or hides.

Mini tip: A realistic image is not the same as reliable evidence.

Learn by playing: after this section, try Challenge 2, Real or AI?, in *Section 16*. The challenge asks learners to inspect images and videos before trusting them.

8. Privacy, digital footprint and personal data

Privacy means controlling personal information and understanding who can see, store, use or share it. A **digital footprint** is the trail left by accounts, posts, photos, comments, searches, location data and shared files.

You should avoid publishing sensitive information such as identity documents, passwords, private addresses, personal phone numbers, health information or images of other people without permission. Privacy settings matter, but they are not magic. A private post can still be copied. A deleted post may have been saved. A shared folder may be forwarded. Safe behaviour is stronger than relying only on settings.



Key Concepts

Privacy: Having control over who can see or use information about you.

Personal data: Information that can identify you, such as your name, email address, phone number or photo.

Digital footprint: The information and traces you leave behind when you use websites, apps or online services.

Consent: Giving clear permission for something to happen, for example for your photo or personal information to be shared.

Visibility: Who can see your profile, posts, photos or other information online.

Settings: Options in an app or website that let you control things such as privacy, notifications and who can see your content.



Practical Task

Review a sample social media profile and identify three pieces of information that should not be public.

Mini tip: Share as if the content could travel further than you expect.

9. Online safety basics: accounts, passwords and devices

Many online safety problems start with accounts. A weak password, reused password or unprotected email account can give attackers access to other services. Good basic habits include using long unique passwords, storing them in a password manager, enabling multi-factor authentication, updating devices, locking screens and avoiding unknown downloads.

Backups also matter. If a device is lost, damaged or infected, backups can protect important files. For community or project work, backups should be organised and understandable, not improvised at the last minute.



Key Concepts

Password manager: A tool that stores your passwords securely so you do not have to remember them all.

Multi-factor authentication: An extra security step that asks for more than just a password, for example a code sent to your phone.

Update: A newer version of software that can fix problems, improve security or add features.

Backup: A saved copy of important files that you can use if the original files are lost or damaged.

Device security: The steps you take to protect your phone, tablet or computer from unwanted access, loss or harmful software.



Practical Task

Create a personal account safety checklist without writing any real password.

Mini tip: The email account is often the master key; protect it first.

10. INCIBE recommendations and trusted help resources

INCIBE, the Spanish National Cybersecurity Institute, is a useful reference for online safety in Spain. It provides guidance, educational resources and a cybersecurity help line for citizens, professionals and organisations.

INCIBE materials for citizens cover practical topics such as safe browsing, secure connections, basic settings, antivirus, firewalls, updates, user accounts, backups, encryption, passwords, malware, online fraud, phishing, smishing, vishing, privacy, mobile devices and artificial intelligence. INCIBE is valuable because it translates cybersecurity into everyday actions. The goal is not to become a technical expert, but to know what to do when receiving a suspicious message, protecting an account, shopping online or configuring a device.

A simple INCIBE-inspired checklist can include:

- update devices
- use unique passwords
- activate multi-factor authentication
- make backups
- check links before clicking
- avoid sharing verification codes
- review privacy settings and ask for help when something feels wrong



Practical Task

Use the INCIBE topic list to choose three online risks and write one prevention action for each.

Mini tip: Good online safety includes knowing where to ask for reliable help.

11. Have I Been Pwned and data breach checks

Have I Been Pwned is a service that allows users to check whether an email address appears in known data breaches. It can also be used to understand why password reuse is dangerous. A **data breach** means that information from a service has been exposed. This may include email addresses, usernames, passwords, phone numbers or other account data. If a password is reused across accounts, one breach can affect many services.

Learners should use Have I Been Pwned carefully. They can check an email address, but they should not type real current passwords into random websites. For passwords, they should use trusted password managers or known safe checking tools and follow official guidance. If an email appears in a breach, the response should be calm and practical: change reused passwords, make each password unique, enable multi-factor authentication, check account activity and be alert to phishing messages.



Key Concepts

Data breach: A security incident in which private or personal information is accessed or exposed without permission.

Exposed email: An email address that has appeared in leaked or stolen data and may be known to attackers.

Password reuse: Using the same password for more than one account.

Credential stuffing: An attack in which stolen email addresses and passwords are automatically tried on other websites to see if they also work there.

Account recovery: The process of getting access to your account again if you forget your password or lose access.



Practical Task

Simulate a breach response plan. What would you do if your email appeared in a breach?

Mini tip: A breach warning is not the end of safety; it is a signal to clean up your accounts.

12. Shared file safety: Telegram, direct downloads and compressed archives

Many risks arrive through files shared outside official channels: Telegram groups, unknown cloud folders, direct download links, forums, cracked software pages or shortened URLs. These routes can be legally questionable and technically risky.

The safest recommendation is to avoid downloading files from sources of doubtful legality or unclear origin. Pirated software, cracked tools, unknown installers and password-protected archives are common ways to distribute malware.

Before opening a downloaded file, learners should ask basic questions:

Who sent it?

Was I expecting it?

Does the source have a reputation?

Is the file legal to use? Does the filename match the content?

Is the extension suspicious?

Is it asking me to disable antivirus or enable macros?

Compressed files such as ZIP, RAR or 7Z should not be opened blindly. First, check the source, scan the archive with antivirus, inspect the file list without extracting if possible, and avoid archives that contain executable files such as .exe, .scr, .bat, .cmd, .msi, .apk or suspicious shortcut files.

If a file is important but uncertain, use safer analysis steps: check the URL before downloading, scan the file with updated antivirus, compare hashes if the official source provides them, and consider multi-engine scanning services such as VirusTotal for public non-private files or URLs. Do not upload private or sensitive files to public scanning services.

Documents can also be dangerous. Office files with macros, PDFs from unknown sources, fake invoices and compressed folders with hidden executables are common attack

methods. A safe habit is to open documents in protected view, avoid enabling macros, and use official sources whenever possible.

For learning environments, the rule should be simple: use official websites, trusted repositories and legal sources. If a platform or file asks learners to bypass payment, disable protection, install unknown tools or ignore warnings, it is not appropriate for training.



Key Concepts

Compressed archive: A file that contains one or more files packed together, usually to make them easier to store or send. ZIP is a common example.

Executable file: A file that can start a program or installation when opened, such as an .exe file.

Malware: Harmful software that can damage a device, steal information or access it without permission.

Hash: A digital value that can be used to check whether a file has been changed.

Antivirus: Software that helps find, block and remove harmful software.

Direct download: Downloading a file directly from a website to your device.

Cracked software: Software that has been illegally changed to avoid paying for it or to remove licence restrictions. It can also contain harmful software.

Protected View: A safety mode that opens some downloaded documents with editing disabled until you decide that the file is safe.



Practical Task

Inspect a sample download scenario and decide whether to open, delete, scan, verify with the sender or download again from an official source.

Mini tip: If a file comes from a doubtful place and asks you to trust it quickly, do the opposite: slow down and verify.

Learn by playing: after this section, try Challenge 4, Safe Download Mission, in *Section 16*. It practises decisions about Telegram files, direct downloads and compressed archives.

13. Online scams, phishing and social engineering

Phishing is a trick that tries to make people reveal information or click a dangerous link. Smishing uses SMS or messaging apps. Vishing uses phone calls. Social engineering uses trust, urgency or fear to influence behaviour.

Common warning signs include urgent deadlines, threats, prizes, unexpected attachments, requests for verification codes, strange payment instructions, shortened links and messages that pressure people to act quickly.

The safest response is to pause. Do not use the link in the message. Go directly to the official website or app, contact the organisation through a known channel and never share passwords or authentication codes.



Key Concepts

Phishing: A fake message or website designed to trick you into giving away personal information, passwords or money.

Smishing: Phishing carried out through text messages or messaging apps.

Vishing: Phishing carried out through a phone call or voice message.

Scam: A dishonest attempt to trick someone, usually to steal money, information or access to an account.

Social engineering: Manipulating people into doing something unsafe, for example sharing a password or opening a harmful link.

Verification code: A temporary code used to confirm your identity when signing in or making a sensitive change to an account.



Practical Task

Analyse three suspicious messages and highlight the warning signs.

Mini tip: Urgency is one of the most common tools of online fraud.

Learn by playing: after this section, try Challenge 1, Spot the Phish, in *Section 16*. It follows the same logic as interactive phishing quizzes: inspect, decide and learn from feedback.

14. Cyberbullying, hate speech and respectful participation

Online safety is not only technical. It also includes how people treat each other. Cyberbullying, harassment, hate speech and humiliation can seriously affect wellbeing and participation. Respectful participation means disagreeing without attacking, avoiding public shaming, not sharing private images, reporting abusive behaviour and supporting people who are targeted.

In learning or community projects, groups should agree basic rules before publishing or discussing online: who can comment, who moderates, what is not acceptable and how problems will be handled.



Key Concepts

Cyberbullying: Using digital tools to repeatedly hurt, embarrass or threaten another person.

Harassment: Unwanted behaviour that makes someone feel threatened, uncomfortable or unsafe.

Hate speech: Content that attacks or encourages hatred against people because of characteristics such as their origin, religion, gender or identity.

Moderation: The process of checking online content and behaviour and applying community rules.

Reporting: Using a platform's tools to alert it about harmful, abusive or inappropriate content or behaviour.

Wellbeing: Feeling safe, balanced and comfortable when using digital technologies.



Practical Task

Write five community rules for a safe online project space.

Mini tip: A safe digital space needs rules, moderation and care.

15. Safe publishing for community and heritage projects

When publishing community or heritage content, learners should think about consent, context and privacy. A photo of a person, a private location or a community story may require permission before being shared. Safe publishing also means checking media rights, giving attribution, avoiding misleading captions and protecting vulnerable people or sensitive cultural information.

Before publishing, a project team can use a short review: Is the source clear? Is the licence clear? Are people shown with consent? Does the content reveal private data? Could the story be misunderstood without context?



Key Concepts

Consent: Clear permission from a person before using or sharing their image, story, voice or personal information.

Attribution: Giving credit to the person or source that created or provided the content.

Context: The background information that helps people understand a story, image, object or tradition correctly.

Community safety: Making sure that published content does not put people, places or communities at unnecessary risk.

Heritage sensitivity: Treating cultural heritage with care and respect, especially when it involves personal memories, traditions, sacred places or sensitive community information.

Publishing review: A final check before sharing content to make sure it is accurate, respectful, properly credited and safe to publish.



Practical Task

Review a draft post about a local heritage object and identify what should be checked before publication.

Mini tip: Publishing responsibly protects both the audience and the community represented.

16. Learn by Playing: Media Literacy and Cyber Safety Challenges

This section turns media literacy and online safety concepts into short decision-making challenges. Learners practise spotting phishing, AI-generated content, misinformation and unsafe files through realistic scenarios with instant feedback.

The aim is practice-based learning. Learners do not only read advice; they make choices, compare signals, receive explanations and reflect on what they would do in real life.

Suggested scoring: each challenge includes 3 to 5 scenarios. Learners receive 1 point for each good decision and 1 extra point when they can explain the warning sign or verification step. At the end, they can receive a simple badge: Careful Checker, Source Detective, AI Image Spotter or Cyber Safety Guardian.

Challenge 1: Spot the Phish. Learners inspect emails, SMS messages, direct messages or Telegram-style messages. They look at the sender, link, tone, urgency, attachment, request for codes and whether the message asks them to use an unsafe channel. Inspiration: Google/Jigsaw Phishing Quiz (<https://phishingquiz.withgoogle.com/>). Example decision: click the link, ignore it, report it, or go directly to the official website.

Challenge 2: Real or AI? Learners analyse images, short videos or screenshots and decide whether the content is real, AI-generated, edited or missing context. They look for visual inconsistencies, strange hands or text, unnatural reflections, lack of source, old images reused as new events and whether trusted sources confirm the claim. Inspiration: Detect Fakes by Northwestern University (<https://detectfakes.kellogg.northwestern.edu/>), Deepfakes Tracker digital literacy games (<https://deepfakestracker.org/digital-literacy-games/>), Real or AI (<https://whichoneisreal.com/real-or-ai/>) and Sightengine AI or Not (<https://sightengine.com/ai-or-not>).

Challenge 3: Fake News Lab. Learners review headlines, posts or short articles and identify emotional manipulation, weak evidence, false authority, clickbait, missing context, conspiracy framing or misleading statistics. Inspiration: Bad News Game (<https://www.getbadnews.com/>), Inoculation Science games (<https://inoculation.science/inoculation-games/>), NewsFeed Defenders and ABC Fake News Game. Example decision: share, save for later, check another source, rewrite neutrally or reject as unreliable.

Challenge 4: Safe Download Mission. Learners receive realistic file-sharing situations: a ZIP in a Telegram group, a direct download link, a password-protected RAR, a cracked installer, a PDF invoice, a shortcut hidden inside an archive or a file from an unknown cloud folder. They decide whether to open, delete, scan, verify with the sender, check the URL, compare a hash or download from an official source.



Reflection

Which warning sign did you almost miss, and what habit will help you notice it next time?

Mini tip: A good challenge should feel like a real decision, not a memory test.

17. Final activity

The final activity combines media literacy and online safety. Learners choose a piece of online content related to culture, technology, local news or community life and analyse it before deciding whether it should be shared.

Analysis sheet

Title or topic	
Platform	
Creator	
Date	
Main claim	
Evidence	
Emotional language	
Source check	
Second source	
Possible missing context	
Final decision	

Safety sheet

Personal data involved	
Privacy risks	
Scam warning signs	
Account safety actions	
File-download risks	
Could INCIBE guidance help?	
Would <i>Have I Been Pwned</i> be useful for checking breach exposure?	

Mini tip: The best online safety tool is a pause before action.

18. Digital Wellbeing Tip



Digital Wellbeing Tip

Make Your Screen More Comfortable

A screen that is too bright, text that is too small or an uncomfortable sitting position can make digital activities more tiring than they need to be.

Try this: Adjust the screen brightness, increase the text size if necessary and place the device where you can use it comfortably. Change your position or stretch if you have been sitting for a long time.

Reflection question: Is there one small change that could make using your phone or computer more comfortable?

19. Basic glossary

Algorithm: system that selects or ranks content according to rules and data.

Cyberbullying: repeated harmful behaviour carried out through digital tools.

Data breach: exposure of account or personal data from a service.

Digital footprint: trail of information a person leaves online.

Disinformation: false or misleading information shared deliberately to deceive.

Fact-checking: process of checking a claim against evidence and reliable sources.

Hash: digital fingerprint used to compare whether a file matches an expected version.

Have I Been Pwned: service used to check whether an email appears in known data breaches.

INCIBE: Spanish National Cybersecurity Institute, a trusted cybersecurity reference and help resource.

Media literacy: ability to access, understand, evaluate, create and share media responsibly.

Misinformation: false or inaccurate information that may be shared without intent to harm.

Multi-factor authentication: account protection that requires an additional verification step.

Phishing: fraudulent message designed to steal information or make users click dangerous links.

RAR/ZIP/7Z: compressed archive formats that can contain one or many files.

Privacy: control and protection of personal information.

Source: person, organisation or platform that publishes information.

20. Module closing

Media literacy and online safety are everyday skills. They help people participate online without being passive, careless or easily manipulated. The module has shown that reliable digital participation requires both critical thinking and practical protection. Learners should check information, protect accounts, respect others and publish with care.

After this module, learners should be able to pause before sharing, evaluate a source, recognise common risks, use trusted help resources, practise through short challenges and create a simple safety checklist for personal or project use.

Mini tip: Think critically, act safely and share responsibly.

Bibliography

European Commission. (2026, June 22). *Media literacy*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/media-literacy>

European Commission. (2026, June 23). *Tackling online disinformation*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

Grizzle, A., Wilson, C., & Gordon, D. (Eds.). (2021). *Media and information literate citizens: Think critically, click wisely!* UNESCO. <https://www.unesco.org/en/articles/media-and-information-literate-citizens>

Instituto Nacional de Ciberseguridad. (n.d.). *Ciudadanía*. Retrieved August 28, 2026, from <https://www.incibe.es/ciudadania>

Richardson, J., & Milovidov, E. (2022). *Digital citizenship education handbook: Being online, well-being online, rights online* (2022 ed.). Council of Europe Publishing. [Council of Europe publication](#)