Co-funded by the European Union

ESAFETY WOMEN

TOOLKIT



NUMBER: 2024-1-LT02-KA210-YOU-000243179
DATES: 01/10/2024 - 31/03/2026

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Table of Content

Main aim & Objectives 3

Activites & Results 4

Partners 5

Facts about GBV online and offline 7

Empowering safety online 10

Modules 12

Conclusion 65

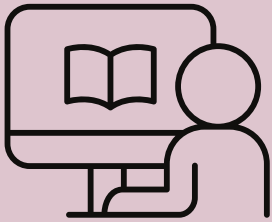
Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Title: eSAFETTY WOMEN
Number: 2024-1-LT02-KA210-YOU-000243179
Dates: 01/10/2024 - 31/03/2026

MAIN AIM

To equip young women from disadvantaged backgrounds with the skills and knowledge necessary to navigate online spaces safely, recognize and respond to online gender-based violence (OGBV), and engage as informed digital citizens.



OBJECTIVES

- Equip youth, especially young women from disadvantaged groups, with critical digital and media literacy skills to safely navigate and engage in online spaces.
- Strengthen the capacity of these individuals to recognize, respond to, and recover from instances of OGBV and online harassment.
- Encourage and facilitate the active participation of youth in online discussions and civic activities, fostering their role as informed and engaged digital citizens.
- Develop and disseminate tools such as the e-Safety Toolkit and Card Game to educate youth about online safety and the implications of OGBV.
- Work towards creating online environments where all individuals, regardless of gender or background, can participate without fear of harassment or discrimination.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

ACTIVITIES

- Project management and implementation, dissemination.
- Development of a toolkit through informal and non-formal learning in Digital Literacy & online safety for migrant youth.
- Local trainings.
- International meeting in Spain.
- Development of e-Safety Card Game and the Handbook.

RESULTS

- A measurable decrease in the instances of OGBV experienced by the target groups.
- Increased Participation: Higher levels of participation by disadvantaged youth in online forums, discussions, and civic activities.
- Wider recognition and understanding of the challenges of OGBV within the community, leading to more supportive and inclusive online environments.
- Effective use of the e-Safety Toolkit and Card Game in various settings, demonstrating their utility in educating about online safety.
- Enhanced self-efficacy and confidence among young women and disadvantaged youth in navigating the digital world.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

PARTNERS

Lithuania

IVAIGO is dedicated to empowering disadvantaged groups, especially women and youth, through digital literacy, social inclusion, and education. They focus on key societal challenges like discrimination, digital transformation, and women's empowerment. With expertise in media literacy, digital tools, and content creation, IVAIGO has led projects such as 'Tool4Youth' and 'EDUMOM,' which address online safety, fake news awareness, and digital skills development. Their work, particularly in organizing workshops and creating toolkits, aligns with the eSAFETY WOMEN project's goal of equipping young women with the skills to navigate online spaces safely and combat online gender-based violence.

Spain

TeneLearning, based in Tenerife, Spain, is dedicated to equipping individuals with essential skills to thrive in today's digital and social landscapes. The center offers diverse courses focusing on well-being, outdoor learning, sustainability, inclusion, and IT, fostering a supportive environment for personal and professional growth. TeneLearning's initiatives address key societal challenges such as online gender-based violence (OGBV) and digital safety, aiming to mitigate the negative impacts of OGBV like anxiety, depression, and social isolation, particularly in vulnerable populations. Through workshops, lectures, and interactive discussions, TeneLearning enhances digital literacy, confidence, and resilience, empowering participants to navigate and shape online spaces responsibly while cultivating their creativity and career skills.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

PARTNERS

Turkey

KSKD (Association of Sustainable Development) is a new, dynamic organisation formed with the mission of catalysing positive change and promoting sustainable practices within our communities. Our vision is to create a future where environmental, social and economic well-being coexist harmoniously and individuals thrive in a balanced and equitable society.Our activities include:

1. Enabling participants to use social media tools for the communication, promotion, financing and management of their projects aiming to raise employment of young people and establishing non – violence social media communication;
2. Stimulating participants to share their personal and professional practices in using social media in youth work through teamwork and networking;
3. Raising the employability of the participants through improving social media skills and through personal branding

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

FACTS ABOUT GBV ONLINE AND OFFLINE

Lithuania

➔ Lithuania has one of the highest reported rates of gender-based violence in the European Union. According to studies, nearly 1 in 3 women in Lithuania has experienced physical or sexual violence since the age of 15. (https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report)

➔ The Lithuanian Police reported over 16,000 incidents of domestic violence in 2020. This accounts for approximately 62% of all violent crimes reported in the country, highlighting the significant issue of domestic violence as a form of GBV. (https://en.wikipedia.org/wiki/Domestic_violence_in_Lithuania)

➔ A study by the Lithuanian Ministry of Social Security and Labour found that 26% of young women aged 18-29 have experienced some form of online harassment. This includes stalking, unwanted sexual advances, and derogatory comments on social media. (https://en.wikipedia.org/wiki/Domestic_violence_in_Lithuania)

➔ According to a survey conducted by the Baltic Institute of Social Sciences, around 70% of young women in Lithuania have encountered negative comments or harassment online, emphasizing the vulnerability of this demographic to digital forms of GBV. (https://www.bissurveys.com/)

➔ Victims of GBV, both online and offline, often suffer from mental health issues. Research indicates that 65% of women who experienced GBV reported symptoms of anxiety or depression, demonstrating the profound psychological impact of such violence. (https://www.who.int/news-room/fact-sheets/detail/violence-against-women)

➔ Lithuania has made legal advancements in addressing domestic violence, including the adoption of the Law on Protection Against Domestic Violence in 2011. However, laws specifically targeting online gender-based violence remain limited and fragmented. (https://eige.europa.eu/publications-resources/publications/lithuania-laws-policies-domestic-violence)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

FACTS ABOUT GBV ONLINE AND OFFLINE

Spain

➔ Recent data from Spain shows a worrying surge in gender-based violence cases, with a 32% increase among young victims, particularly affecting those aged 30-44. A significant portion involved current or former romantic partners.
https://www.theolivepress.es/spain-news/2024/05/17/gender-violence-surges-in-spain-number-of-young-victims-increased-by-32-last-year-figures-show/

➔ During the pandemic, Spain saw a surge in domestic violence cases due to lockdowns, with limited access to support services worsening victims' situations.
https://english.elpais.com/society/2021-06-17/in-spain-gender-violence-claims-more-lives-in-last-30-days-than-in-first-four-months-of-2021.html

➔ Spain is pioneering efforts to end violence against women and girls by leveraging administrative data to enhance policy, evaluate interventions, and better protect victims, with support from UN Women.
https://www.unwomen.org/en/news-stories/take-five/2023/07/take-five-how-spain-is-using-administrative-data-to-help-end-violence-against-women-and-girls

➔ In the early months of 2023, Spain reported a nearly 18% increase in female victims of gender violence, highlighting the urgent need for enhanced protective measures and societal intervention to combat this persistent issue.
https://www.theolivepress.es/spain-news/2023/06/14/female-victims-of-gender-violence-in-spain-up-by-nearly-18-in-early-months-of-2023/

➔ 98% of women in Spain experience street harassment, with 80% encountering it monthly. This harassment elevates anxiety and lowers self-esteem, pushing many women to limit their movements to avoid public spaces, reflecting the widespread impact on their mental well-being and freedom.
https://phys.org/news/2024-10-street-women-spain-frequency-anxiety.html

➔ Studies indicate that 20% of Spanish women who experienced online harassment have received inappropriate messages via social networks and instant messaging platforms like Instagram, Facebook, and WhatsApp.
https://letslaw.es/en/gender-based-crimes-digital-violence/

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

FACTS ABOUT GBV ONLINE AND OFFLINE

Turkey

➔ Approximately 38% of women in Turkey have experienced physical and/or sexual violence during their lives.Interview: How Turkey's Failure to Protect Women Can Cost Them Their Lives | Human Rights Watch

➔ In 2021, there were 307 reported cases of femicide in Turkey. Combatting Domestic Violence in Turkey: The Deadly Impact of Failure to Protect | HRW

➔ 14.7% of women aged 20–24 were married or in a union before age 18. Country Fact Sheet | UN Women Data Hub

➔ Social media platforms are the most common venues for cyberbullying incidents in Turkey. Turkey: Most common platforms for cyberbullying 2018 | Statista

➔ Victims of online GBV often experience anxiety, depression, and social withdrawal, highlighting the need for comprehensive support systems. Violence against women is met with impunity in Turkey · Global Voices

➔ A 2020 study revealed that 58% of women in Turkey have experienced online harassment, including threats and unwanted explicit content.Turkiye | World Bank Gender Data Portal

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

EMPOWERING SAFETY ONLINE

The Importance of Digital Literacy in Combating Gender-Based Violence

In today's digital landscape, our online presence has become deeply woven into our lives, influencing how we communicate, access information, and engage with communities. Yet, as digital platforms expand, they can also expose users—particularly women and marginalized groups—to various forms of online abuse, including gender-based violence (GBV). Online GBV can take many forms: cyberstalking, harassment, threats, doxxing, unwanted explicit messages, and even identity theft. Such harmful behaviors are not just disruptive; they can be profoundly damaging, leading to psychological distress, anxiety, and, in severe cases, social withdrawal or professional setbacks.

With the right knowledge and tools, however, users can take proactive steps to protect themselves and build resilience against these threats. Strengthening digital literacy is essential in this effort. Digital literacy is more than basic tech skills; it's about equipping individuals with the critical skills and awareness needed to navigate online spaces safely and confidently. For instance, knowing how to spot red flags in messages or posts, understanding how to report or block abusive users, and recognizing phishing attempts are key skills that enhance personal safety. Moreover, a well-rounded digital literacy empowers users to manage their digital footprint effectively, setting strong privacy controls, recognizing misinformation, and safeguarding personal data to reduce the risk of exploitation.

This kind of literacy fosters not only self-protection but also a more informed, assertive approach to digital engagement. When individuals are digitally literate, they are better prepared to advocate for their own rights online, respond constructively to inappropriate behaviors, and support others who may face similar issues. Additionally, fostering a strong sense of digital safety and responsibility helps create online communities where respect, dignity, and inclusion are valued.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Beyond personal safety, strengthening digital literacy contributes to a broader societal impact by counteracting the harmful effects of online GBV on communities. As more people are empowered to recognize and stand up against digital threats, online platforms become safer and more inclusive spaces for everyone. In an interconnected world, digital literacy is a form of empowerment—an essential skill that promotes resilience, confidence, and a more balanced and respectful digital culture.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULES

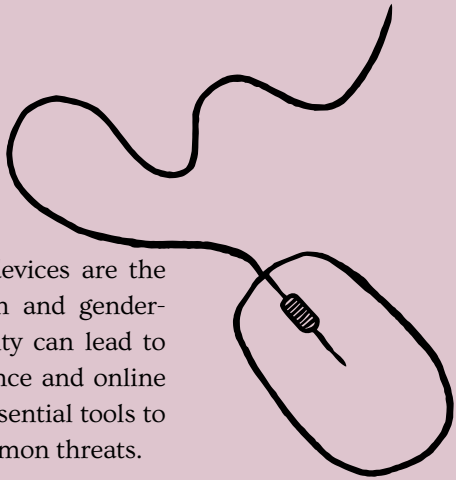
1. Using your device safely
2. Connecting safely
3. Being Social
4. Life Admin
5. Dating & Relationships
6. Navigating difficult situations
7. Cyberbullying
8. Online hate
9. Digital footprint
10. Fake news
11. Catfishing
12. Trolling
13. Consent for sharing photos & videos
14. Balancing time on social media

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 1

Using Your Device Safely



OVERVIEW

In an increasingly connected world, our devices are the gateways to our private lives. For women and gender-diverse individuals, a lack of digital security can lead to serious risks - from data theft to surveillance and online harassment. This module introduces the essential tools to protect yourself and your devices from common threats.

KEY OBJECTIVES

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

- Set up strong security settings on your device.
- Safeguard personal information from digital threats.
- Connect safely to networks like Wi-Fi and Bluetooth.
- Recognize and respond to suspicious activity or phishing attempts.

KEY CONCEPTS

Password Protection: Use long, complex passwords that combine uppercase and lowercase letters, numbers, and symbols. Never reuse passwords across different accounts.

Software Updates: Regular updates patch known vulnerabilities. Set your device to update automatically to stay protected.

Two-Factor Authentication (2FA): Adds a second step (e.g., a text message or app code) after entering your password—offering double the protection.

Public Wi-Fi Awareness: Avoid online banking or sharing personal info on open networks. If needed, use a Virtual Private Network (VPN) to encrypt your connection.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

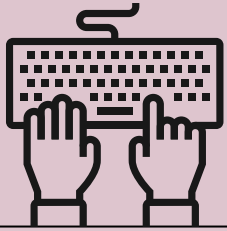
1. How to Set Up a Strong Password
   - Go to your device's settings.
   - Find the section for security or privacy settings.
   - Choose the option to change or set a password.
   - Create a password with at least 12 characters, including letters, numbers, and symbols.
2. Enabling Two-Factor Authentication
   - Go to the security settings of the app or service (e.g., your email account).
   - Select the option for "Two-Factor Authentication."
   - Choose how you would like to receive your second verification code (e.g., SMS or an authentication app).
   - Follow the prompts to complete the setup.

REAL-LIFE SCENARIO

Scenario: Alex receives an email claiming to be from their bank, asking them to log in and verify account details. The email looks official, but Alex notices something strange about the URL. Before responding, Alex checks the URL and realizes it's not from the real bank. Instead of clicking on the link, Alex reports the phishing attempt to the bank's customer service.

REFLECTIVE QUESTION:

What should you do when receiving suspicious emails or messages on your device?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

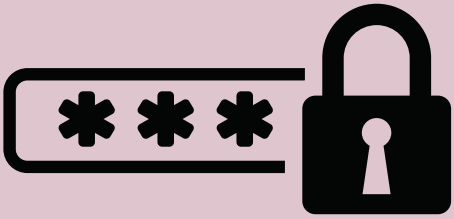
INTERACTIVE ACTIVITIES

Quiz: How Safe Is Your Device?

- Have you updated your device's software in the last month? Yes / No
- Is two-factor authentication enabled on your device? Yes / No
- Do you avoid using public Wi-Fi for sensitive tasks without a VPN? Yes / No
- Are your device passwords strong (at least 12 characters)? Yes / No
- (Provide feedback based on their answers and suggest ways to improve device safety.)

RECAP

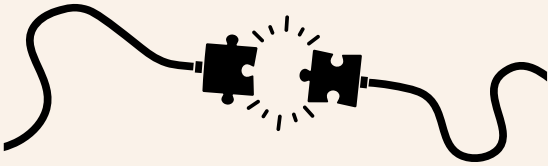
- Always use strong, unique passwords for your devices and accounts.
- Keep your software up to date.
- Use two-factor authentication for extra security.
- Avoid public Wi-Fi for sensitive tasks unless using a VPN.
- By following these practices, you'll significantly reduce the risk of your device being compromised.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 2
Connecting Safely



OVERVIEW

Our devices constantly connect to the digital world—through Wi-Fi, apps, Bluetooth, and the cloud. But behind convenience can lie risk, especially for women. From being tracked by abusers through shared networks to having private content intercepted or leaked, these connections can expose us to serious threats if not managed carefully.

This module will help you take control of your digital connections with practical tools and safety tips that reflect how real women live, work, and survive online.

KEY OBJECTIVES

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

- Recognize how unsafe connections can be used to monitor or harm you.
- Safely connect to Wi-Fi, apps, and online services while limiting exposure.
- Understand risks related to Bluetooth, cloud syncing, and shared devices.
- Use built-in tools to block, limit, or encrypt digital access.

KEY CONCEPTS

- Public Wi-Fi Safety: Always use VPNs when connecting to public Wi-Fi networks, especially when accessing sensitive information.
- Secure Web Browsers: Use trusted web browsers with built-in security features and make sure they are updated regularly.
- App Permissions: Review the permissions requested by apps and limit access to only what is necessary for their function.
- Bluetooth & Cloud Security: Be cautious when pairing devices via Bluetooth and use encrypted cloud storage services for sensitive data.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Use a VPN for Safe Wi-Fi Connection
   - Download a VPN app from a trusted provider.
   - Open the VPN app and log in.
   - Select a server location and connect to it.
   - Confirm that the VPN is active before using public Wi-Fi.
2. How to Set App Permissions
   - Go to your device's settings.
   - Find the section for apps and permissions.
   - Select the app you want to adjust.
   - Toggle off unnecessary permissions (e.g., camera, microphone) unless required by the app.

REAL-LIFE SCENARIO

Scenario: Maria is connecting her phone to a public Wi-Fi network in a café. She activates her VPN before entering any personal details or checking her bank account. Afterward, she disconnects from the Wi-Fi to prevent her data from being intercepted by potential hackers.

REFLECTIVE QUESTION:

What steps do you take before using a public Wi-Fi network for tasks like online shopping or banking?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: How Secure Is Your Connection?

- Do you use a VPN when connecting to public Wi-Fi? Yes / No
- Do you regularly review app permissions? Yes / No
- Do you ensure your web browser is updated regularly? Yes / No
- Do you use encrypted cloud storage for your sensitive files? Yes / No
- (Provide feedback based on their answers and suggest improvements.)

RECAP

- Always use a VPN when connecting to public Wi-Fi.
- Keep your web browser and apps updated for security.
- Review and limit app permissions.
- Use encrypted cloud storage for sensitive data.

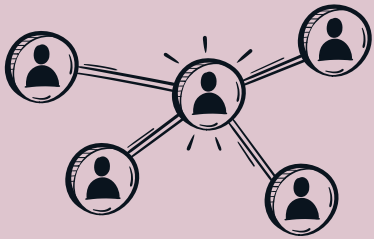


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 3

Being social online



OVERVIEW

Online spaces can be incredibly empowering for women—offering platforms to connect, express yourself, and build communities. Social media, email, gaming platforms, and online forums provide opportunities for friendship, activism, creativity, and learning. Yet these same spaces can expose users to serious risks, particularly gender-based harassment, image-based abuse, doxxing, or identity exposure.

The way you present yourself online can affect not just your safety but also your emotional well-being and autonomy. Understanding how your visible and invisible digital footprint works is essential to navigating these spaces safely.

This module explores how to engage socially online while maintaining control over your identity, privacy, and boundaries. It also introduces an often-overlooked topic: metadata—the hidden information attached to your photos and files that can unintentionally expose personal details such as location or device information.

KEY OBJECTIVES

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

- Safely share personal information online.
- Recognize and avoid online harassment or cyberbullying.
- Understand privacy settings on social media platforms and other online communication tools.
- Make empowered choices about your visibility, safety, and emotional boundaries online.
- Explain what metadata is, why it matters, and how to manage or remove it before sharing content.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

KEY CONCEPTS

Privacy Settings on Social Media

Most platforms allow you to control who sees your posts, who can comment, and who can message you. Use “Friends Only” or “Close Friends” settings for posts that contain personal details. Platforms like Instagram, TikTok, and Facebook also offer tools to hide your story from specific users or disable comments altogether. Remember: privacy settings can change over time, so review them regularly.

Gender-Based Harassment & Cyberbullying

Women and girls experience targeted forms of abuse online: slut-shaming, threats of sexual violence, body-shaming, racialized abuse, and stalking. These are not just “mean comments”—they are acts of harm and control. Learn how to document abuse (screenshots with time stamps), report it through platform mechanisms, and seek help from support services. Abuse is never the victim’s fault.

Safe Sharing Practices

Avoid sharing real-time locations, personal routines, or information that can be pieced together (e.g., street names, school or workplace names, family members). Consider whether something you share could be used to locate, impersonate, or threaten you.

Email and Identity Protection

Avoid clicking on links or downloading attachments from unfamiliar emails. Women are increasingly targeted with fake messages that appear to be from HR departments, dating services, or government agencies. These are often phishing attacks aiming to gather private information or install spyware.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Metadata – The Invisible Risk

Even if you never share your location directly, your photos and files often carry hidden information called metadata. Metadata is "data about data." For example:

- Photos taken on smartphones often embed GPS coordinates, date/time, and the device model.
- Documents can include the author's name, the software used, and editing history.

Why does this matter? Harassers and abusers have used metadata to track women's homes, workplaces, or daily habits. If you upload a photo straight from your phone, someone with basic tools could extract its hidden GPS data. For survivors of domestic violence, activists, or any woman concerned about privacy, understanding metadata is critical.

Step-by-Step Guide

How to Adjust Privacy Settings on Social Media

1. Go to your social media account settings.
2. Find the privacy section and adjust visibility options for your posts (e.g., "Friends Only").
3. Enable two-factor authentication for an extra layer of protection.
4. Regularly review who can tag you or view your stories.

How to Manage Metadata Before Sharing

- Disable location tagging: On iPhones, go to Settings > Privacy > Location Services > Camera and set to "Never" or "Ask." On Android, open Camera > Settings > Location Tags and turn them off.
- Remove metadata from existing images: On Windows, right-click the file > Properties > Details > Remove Properties. On Mac, open the image in Preview > Tools > Show Inspector > Info > remove GPS data.
- Use free scrubbing apps: Tools like ExifCleaner (desktop), Scrambled EXIF (Android), or Metapho (iOS) can quickly strip metadata.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

How to Report Cyberbullying or Harassment

1. Use the platform's reporting tool to flag inappropriate content.
2. Block the user to prevent further harassment.
3. Document messages and images with timestamps for evidence.
4. Reach out to support groups or local authorities if necessary.

REAL-LIFE SCENARIO

Emma posts a photo on Instagram and later receives derogatory comments. She uses the platform's privacy settings to limit who can comment and blocks the harassing user. Emma also learns that her photo contained hidden location data. She disables geotagging on her phone so future posts don't reveal her location, and she shares what she learned with friends to keep them safer too.

REFLECTIVE QUESTIONS

- What steps would you take if you encounter cyberbullying or harassment on social media?
- What invisible information (metadata) might be in your recent posts or photos?
- How can you balance self-expression and safety online?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

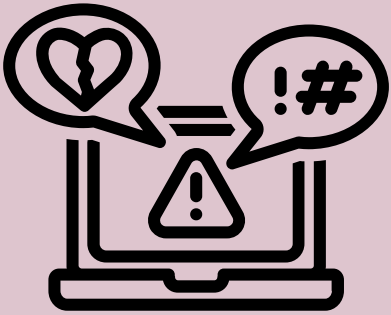
Quiz: How Safe Are You Online?

- Do you adjust your privacy settings regularly? Yes / No
- Do you avoid sharing personal information like location and contact details online? Yes / No
- Do you know how to report and block someone online? Yes / No
- Have you enabled two-factor authentication on your social media accounts? Yes / No
- Do you know how to check and remove metadata from your photos? Yes / No

Group Activity: Practice removing metadata from a sample photo and adjusting privacy settings. Discuss how this makes you feel more in control.

RECAP

- Adjust your social media privacy settings to control who can view and comment on your posts.
- Always report and block online harassment or cyberbullying.
- Avoid sharing personal information or real-time location online.
- Metadata matters: strip or manage it to protect your hidden digital footprint.
- Stay vigilant and empowered while interacting online.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 4

Life Admin Online



OVERVIEW

For many women, handling life's responsibilities—paying bills, shopping, sending money—has increasingly moved online. But with this convenience comes vulnerability.

From phishing attacks designed to look like official bank emails to fraudulent online stores collecting personal data, women face real risks when managing daily tasks online. These threats can also be used to exert financial control in abusive situations or enable identity theft.

This module focuses on how to protect your financial and personal information, so your autonomy and privacy are never compromised.

KEY OBJECTIVES

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

- Safely conduct online banking and financial transactions.
- Recognize and avoid phishing scams and fraudulent websites.
- Use secure online shopping practices to protect personal data.

KEY CONCEPTS

Online Banking Security

Use only verified apps or websites from your bank. Never access banking through a link in an email or message. Always enable two-factor authentication (2FA), which requires a second step—like a code sent to your phone—before login.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Phishing & Impersonation Scams

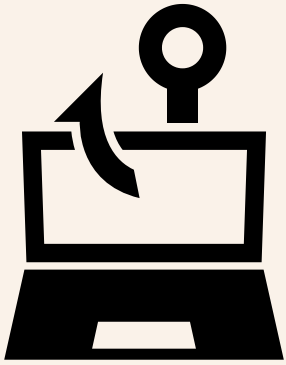
Phishing emails often mimic banks, utility companies, or delivery services. These scams can target women with urgent language, emotional manipulation, or threats (e.g., “Your account will be closed unless you act now”). Abusive partners may also impersonate institutions to gain access to your data or accounts.

Secure Online Shopping

Before entering payment details, ensure the website uses “https://” and a visible padlock icon. Use credit cards or trusted payment platforms like PayPal instead of debit cards. Never shop via public Wi-Fi unless you're using a VPN.

Monitoring for Fraud & Financial Abuse

Check bank activity regularly—not just for external fraud but also to detect signs of financial abuse (e.g., money taken without permission, purchases made in your name). Keep a secure list of your financial accounts and access credentials in a protected place.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Secure Online Banking
   - Use strong, unique passwords for your banking apps or website.
   - Enable two-factor authentication (2FA) for extra protection when accessing your accounts.
   - Always log out of your banking session after completing a transaction, especially on public or shared devices.
2. How to Spot a Phishing Email
   - Look for signs such as generic greetings (e.g., “Dear Customer”), suspicious sender addresses, and urgent messages asking for sensitive data.
   - Never click on links or download attachments from unknown sources.
   - If you receive a suspicious email or message from your bank or any financial institution, contact them directly through their official channels to verify its authenticity.
3. How to Shop Securely Online
   - Only shop on websites with "https://" in the URL, which indicates a secure connection.
   - Use reputable payment methods, such as credit cards or trusted payment systems like PayPal, instead of debit cards.
   - Avoid making purchases on websites that seem untrustworthy, have a poor reputation, or lack customer service contact information.

REAL-LIFE SCENARIO

Scenario: John receives an email from what looks like his bank, asking him to click on a link to confirm his recent transaction. The email contains a sense of urgency and threats about his account being locked. John remembers the advice he learned in the module and doesn't click the link. Instead, he opens his banking app directly and sees no alerts. He contacts his bank to report the phishing attempt.

REFLECTIVE QUESTION:

What steps can you take to protect yourself from fraud and scams when managing online finances or making purchases?

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: Are You Ready for Secure Online Transactions?

- Do you use unique and strong passwords for your online banking and shopping accounts? Yes / No
- Have you enabled two-factor authentication (2FA) for your online banking? Yes / No
- Do you check your bank statements and credit card activity regularly for unauthorized transactions? Yes / No
- Do you shop online only on secure websites (look for https://)? Yes / No
- (Provide feedback based on their answers and recommend actions to improve their online security practices.)

RECAP

- Use official banking apps and turn on 2FA for all financial accounts.
- Be skeptical of urgent emails or messages, even if they seem legitimate.
- Shop only on secure websites and with traceable payment methods.
- Monitor your accounts regularly to catch fraud or financial abuse early.
- Keep a list of your financial accounts and passwords stored safely and privately.

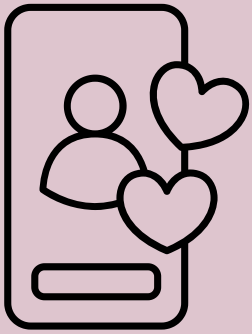


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 5

Dating & Relationships Online



OVERVIEW

Online dating can be empowering, offering connection, companionship, and opportunities to build relationships. But for many women and marginalized groups, it also introduces unique risks: harassment, manipulation, stalking after rejection, and sexual coercion.

Understanding these dangers does not mean avoiding dating—it means equipping yourself with the tools to engage safely and confidently, protect your privacy, recognize red flags, and assert your boundaries.

This module provides in-depth strategies for navigating online dating and relationships with a focus on:

- Privacy and safety practices.
- Recognizing and responding to stalking.
- Identifying and resisting sexual coercion.
- Building healthy, respectful online connections.

KEY OBJECTIVES

By completing this module, participants will:

- Understand how to build and manage safe online dating profiles.
- Identify manipulative and coercive behaviors early.
- Recognize different types of stalkers and how to respond safely.
- Understand sexual coercion and how it undermines consent.
- Build skills for asserting boundaries and seeking support if harm occurs.

KEY CONCEPTS

1. Privacy and Boundaries from the Start

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

- Avoid sharing full name, home address, workplace, daily schedule, or children's details early in conversations.
- Use only in-app messaging initially; don't rush to give out phone numbers or connect on social media.
- Consider using a secondary email/number (like Google Voice) for additional safety.
- Don't feel pressured to meet before you're ready.

2. Recognizing Manipulative Behavior and Red Flags

- Love bombing: Excessive compliments, talking about future plans too soon.
- Gaslighting: Making you doubt your feelings or memories.
- Boundary pushing: Ignoring or questioning your stated limits.
- Financial scams: Sudden "emergencies" or requests for money.
- Control-seeking: Demands for constant communication, jealousy over other relationships.

3. Stalking After Match Rejection

Some individuals react badly when boundaries are enforced or contact is ended. This can escalate from unwanted messages to surveillance or harassment.

Different stalker profiles:

- Rejected stalker: Refuses to accept that a relationship or interaction is over.
- Intimacy seeker: Fantasizes about a deep relationship without consent.
- Incompetent suitor: Socially unaware, persistent despite polite rejection.
- Resentful stalker: Motivated by anger, revenge, or entitlement.
- Predatory stalker: Uses calculated tactics, including surveillance or location tracking.

Common stalking behaviors:

- Repeated calls or messages after clear rejection.
- Showing up uninvited at places you frequent.
- Contacting your friends or family to reach you.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

- Creating fake accounts to monitor your activities.
- Threatening behavior or doxxing (posting your personal information online).

4. Sexual Coercion

Sexual coercion undermines consent. It includes any behavior that pressures, manipulates, or intimidates someone into sexual activity without their free and enthusiastic agreement. It often begins online.

Forms of coercion:

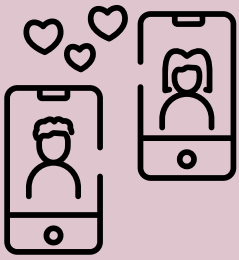
- Verbal pressure: Repeatedly asking despite refusal; guilt-tripping.
- Threats or intimidation: Threatening to end the relationship or harm reputation.
- Sextortion: Threatening to leak intimate images.
- Abuse of authority: Using power imbalance to pressure (e.g., employer/mentor).
- Substance use: Taking advantage of someone intoxicated.
- Emotional manipulation: Claims like "If you loved me, you would..." or blaming you for saying no.

Why coercion happens:

Entitlement, desire for control, lack of consent education, harmful cultural narratives about persistence or "owing" intimacy.

Psychological impact:

Victims may experience guilt, shame, confusion, anxiety, hypervigilance, or depression. Recognizing that coercion is never the victim's fault is crucial for healing.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDES

Building a Safe Online Dating Profile

1. Use non-identifiable photos; avoid landmarks that reveal your home/work.
2. Create usernames that don't include your full name or birthdate.
3. Avoid linking dating profiles to public social media accounts.
4. Be cautious with location-sharing; disable location tags in apps and photos.

Communicating and Meeting Safely

- Start with in-app messaging.
- Video call before meeting to verify identity if possible.
- If meeting, choose a public, well-lit place.
- Arrange your own transport.
- Tell a trusted friend where you are going and share your live location if possible.

Responding to Stalking or Harassment

1. Trust your instincts: If behavior feels intrusive, take it seriously.
2. Block all contact: On the dating app, social media, messaging platforms, and phone.
3. Document evidence: Screenshots, call logs, messages with timestamps.
4. Inform trusted contacts: Friends, family, and co-workers can help you stay safe and alert.
5. Report: Use in-app reporting tools and consider contacting law enforcement if threats escalate.
6. Increase personal security: Change routines, review home security, tighten social media privacy.

Avoiding and Responding to Sexual Coercion

1. Know your boundaries: Be clear about what you're comfortable with.
2. Communicate assertively: Use "I" statements—"I'm not ready for that," "I want to take things slow."

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

3. Recognize coercive tactics: Watch for guilt-tripping, persistent requests, or threats.
4. Trust your gut: Discomfort is a valid warning sign.
5. Protect your digital space: Block, adjust privacy settings, delete triggering content.
6. Seek support: Friends, counselors, and support hotlines can provide resources and advocacy.

REAL-LIFE SCENARIOS

Scenario 1 – Rejected Stalker:
After two dates, Sarah tells David she doesn't feel a connection. David starts texting daily and appears outside her apartment. Sarah documents all incidents, blocks him, tells her friends, and files a police report. The stalking stops after law enforcement intervenes.

Scenario 2 – Intimacy Seeker:
Anna chats briefly with Josh. After a week, he sends love letters and calls her "his future wife." When she blocks him, he finds her Facebook. Anna locks down her social profiles and reports him.

Scenario 3 – Sexual Coercion (Verbal Pressure):
Maria's online partner pressures her to send intimate photos. When she refuses, he says she's "killing the relationship." Maria recognizes the manipulation, blocks him, and seeks support from a women's help group.

Scenario 4 – Sextortion:
Sofia shares intimate photos with someone she trusted. Months later, he threatens to leak them unless she sends more. Sofia doesn't comply, saves evidence, reports him to police and the platform, and seeks therapy for emotional support.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

REFLECTIVE QUESTIONS

- What specific boundaries do you want to set before meeting someone online?
- How can you differentiate between genuine affection and manipulative love bombing?
- If a friend confided that they were being stalked, how would you help?
- Why is it important to separate coercion from consensual intimacy?

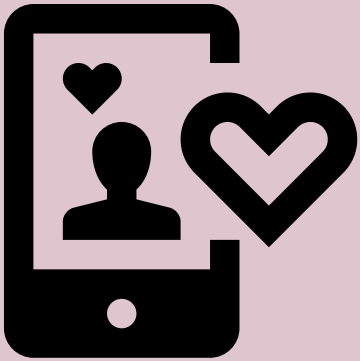
INTERACTIVE ACTIVITIES

Quiz: How Safe Is Your Online Dating Experience?

- Do you avoid sharing personal details like your home address or workplace? Yes / No
- Have you ever encountered red flags in an online relationship? Yes / No
- Do you feel comfortable asking a trusted friend for advice if you're unsure about someone? Yes / No

RECAP

- Online dating is safest when you control your personal information and pace.
- Stalking after rejection is a serious violation: Block, document, report, seek support.
- Sexual coercion is never your fault: It includes verbal pressure, manipulation, threats, and sextortion.
- Consent must be enthusiastic, ongoing, and freely given.
- Healthy relationships respect your autonomy and safety.

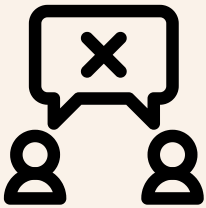


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 6

Navigating Difficult Situations Online



OVERVIEW

Online spaces bring connection and opportunity, but they can also bring conflict and harm. Sometimes this takes the form of everyday disagreements in comment threads; other times, it escalates into harassment, threats, or even exploitation. Women disproportionately face these harms due to gender-based abuse and power imbalances online.

In this module, you'll learn strategies for navigating difficult situations across the full spectrum – from staying calm during an online argument to responding to serious abuse such as photo-based blackmail (sextortion). These skills are vital for maintaining your safety, dignity, and mental well-being.

KEY OBJECTIVES

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

- Handle online disagreements calmly and constructively.
- Apply de-escalation techniques when conversations get heated.
- Recognize when a situation has crossed the line into harassment or abuse.
- Report harmful content effectively and know where to seek support.
- Understand how photo-based blackmail works and what immediate and long-term steps to take if you or someone you know is targeted.

KEY CONCEPTS

1. Everyday Conflict and De-Escalation

It's normal to disagree online. Heated debates happen, but not all disagreements are harmful. The key is to respond in ways that prevent escalation:

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

- Stay calm; avoid insults or sarcasm.
- Stick to facts rather than emotions.
- Step away if the exchange becomes unproductive or hostile.

2. Harassment and Harmful Content

Sometimes online interactions cross the line into abuse: threats, hate speech, misogynistic slurs, or coordinated attacks. These are not "just opinions" – they are harmful acts. Learn to:

- Document abuse (screenshots with timestamps).
- Use platform tools to report threats, hate speech, or impersonation.
- In serious cases, involve moderators, advocacy groups, or law enforcement.

3. Severe Abuse: Photo-Based Blackmail (Sextortion)

A particularly dangerous form of online abuse uses your images as weapons. Photo-based blackmail happens when someone threatens to share personal or intimate images to force you into compliance – asking for more content, money, sexual favors, or control over your behavior.

This can happen with photos shared in trust or stolen through deceit. It's about power and fear, not consent.

How Blackmailers Operate

- Gaining trust: Flattery, emotional manipulation, fake romantic interest (catfishing).
- Obtaining content: Coaxing explicit or personal photos or hacking accounts.
- Threats: "Send more or I'll send this to your family."
- Fear tactics: Urgent deadlines, guilt-tripping ("You brought this on yourself"), isolation ("If you tell anyone, it'll get worse").
- Even paying or complying rarely makes it stop; demands often escalate.

Who is targeted? Teens, young adults, people seeking connection – but anyone can be victimized.

Why victims stay silent? Fear of judgment, shame, or exposure; hope compliance will end it. Silence is exactly what blackmailers rely on.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP STRATEGIES

For everyday disagreements:

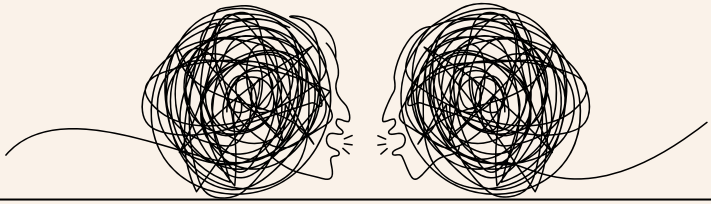
- Stay calm; avoid hostile language.
- Respond with facts or disengage.
- Don't feel obligated to "win" an argument online.

For harassment or threats:

- Document everything with screenshots.
- Use the platform's reporting features.
- Block perpetrators.
- If threats are credible or persistent, contact support organizations or law enforcement.

For photo-based blackmail:

1. Do not panic, pay, or send more.
2. Stop engaging: Block the blackmailer on all platforms.
3. Collect evidence: Screenshot threats, save usernames, emails, headers.
4. Secure accounts: Change all passwords, enable 2FA, remove unknown devices.
5. Report:
    - To the platform (Instagram, TikTok, etc.)
    - To removal services (StopNCII.org, Google removal, DMCA takedown)
    - To law enforcement or cybercrime agencies (IC3.gov, Europol, local police)
6. Tell someone you trust: Break the secrecy; support reduces shame and fear.
7. If images are posted: File removal requests (StopNCII.org, DMCA); document all steps.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

uick emergency checklist (first 10 minutes): Block, screenshot, change passwords, enable 2FA, report, and tell someone you trust.

REFLECTIVE QUESTIONS

- How do you respond to online disagreements? What helps you stay calm?
- At what point does conflict become harassment?
- What would you do if someone threatened to share your images?
- What support resources exist in your country or community for online abuse victims?

INTERACTIVE ACTIVITIES

Quiz:

- Do you try to stay calm when confronted online?
- Do you report harmful content you encounter?
- Have you ever de-escalated a conflict successfully?
- Do you know emergency steps if someone threatens to share your private photos?

Role-play: In pairs, practice supporting a friend disclosing sextortion without blame; list next steps together.

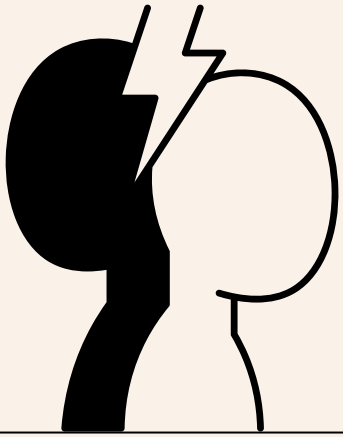


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

RECAP

- Difficult online situations range from minor disagreements to serious abuse.
- Remain calm and respectful; disengage if needed.
- Report harmful behavior; document everything.
- Photo-based blackmail is a crime; you are not to blame. Break the secrecy, document, report, and seek support.
- You are not alone; help exists, and the abuser's power collapses when you reclaim your voice.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 7
Cyberbullying



OVERVIEW

Cyberbullying is more than just mean comments online - it can be a coordinated, persistent form of abuse that deeply affects a person's mental health and sense of safety.
Women, girls, and marginalized groups are more likely to face gender-based and sexualized cyberbullying, such as:

- Misogynistic insults & sexist harassment
- Unwanted sexual messages or "slut-shaming"
- Image-based abuse (sharing private photos without consent)
- Doxxing (leaking private information)

KEY OBJECTIVES

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

- Recognize different types of cyberbullying, including gender-specific forms.
- Understand the short- and long-term mental health impact.
- Learn proactive steps to reduce risk (privacy settings, content moderation tools).
- Respond effectively to cyberbullying, whether you're a target or a bystander.
- Know when and how to escalate—to platform moderators, trusted adults, or authorities.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

KEY CONCEPTS

Types of Cyberbullying

- Direct Harassment: Hurtful messages, public insults, hate speech.
- Spreading Rumors: Sharing lies or manipulated content to damage someone's reputation.
- Exclusion: Intentionally leaving someone out of online groups, forums, or chats.
- Impersonation: Creating fake profiles to harass or embarrass someone.
- Gender-Based Abuse: Slut-shaming, sexual harassment, sharing private images.
- Doxxing & Stalking: Revealing personal info to enable further harassment.

How Cyberbullying Impacts Mental Health

- Immediate Effects: Shock, embarrassment, anger, sadness.
- Medium-Term: Anxiety, fear of using social media, social withdrawal.
- Long-Term: Depression, PTSD-like symptoms, loss of self-esteem.
- Offline Consequences: Cyberbullying can lead to real-world harassment and even unsafe encounters.

Platform Safety & Legal Tools

Most platforms now have advanced safety features:

- Instagram: Restrict, Limit Comments, Hide Offensive Content.
- Twitter/X: Block, Mute, Advanced Filters.
- Facebook: Report, Block, Timeline Review.
- Dating Apps: Photo Verification, Private Mode, In-App Reporting.

In serious cases, cyberbullying can break the law (e.g., blackmail, threats, revenge porn). In such cases, you can:

- Collect evidence (screenshots, timestamps).
- File a report with local cybercrime units or legal authorities.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

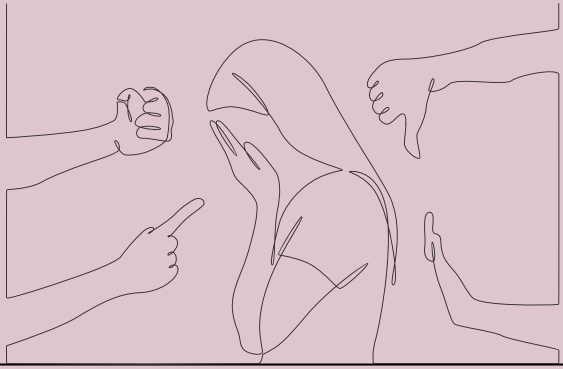
1. How to Recognize Cyberbullying
   - Look for signs like aggressive language, rumors, exclusion, or personal attacks.
   - Pay attention to the emotional toll it may take on the person targeted.
2. How to Report Cyberbullying
   - Identify the harmful behavior on the platform.
   - Use the platform's reporting tool and explain the issue clearly.
   - Consider blocking the bully to stop further harassment.

REAL-LIFE SCENARIO

Scenario: Lucy notices that her friend Jason is being relentlessly teased in an online group. The bullying involves cruel comments and exclusion from group activities. Lucy reports the bullying to the group admin, offers support to Jason, and helps him block the bullies.

REFLECTIVE QUESTION:

What would you do if you witnessed someone being cyberbullied online?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

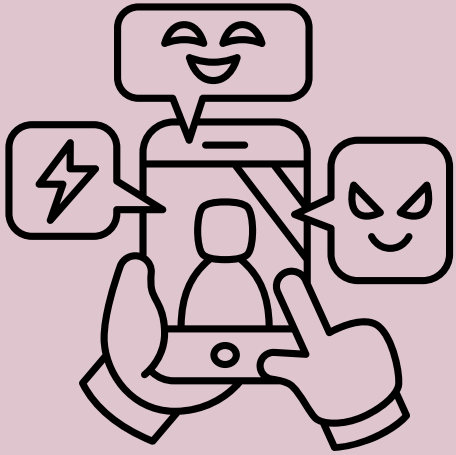
INTERACTIVE ACTIVITIES

Quiz: Are You Prepared to Deal with Cyberbullying?

- Do you know how to recognize the signs of cyberbullying? Yes / No
- Have you ever reported cyberbullying to a platform or moderator? Yes / No
- Would you offer support to someone being cyberbullied? Yes / No
- (Provide feedback based on their answers and suggest ways to intervene safely.)

RECAP

- Recognize the signs of cyberbullying, such as harassment or exclusion.
- Report cyberbullying behavior to platform moderators.
- Support those who are being bullied by listening and helping them seek help.

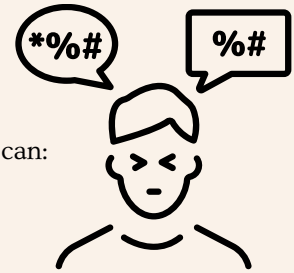


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 8

Online Hate



OVERVIEW

Online hate speech is more than just offensive words - it can:

- Dehumanize and intimidate targeted groups
- Create an unsafe online environment
- Lead to real-life discrimination or violence
- Silence voices, especially those from marginalized communities

Women, LGBTQ+ people, ethnic and religious minorities, and refugees often face intersectional online hate, which combines sexism, racism, homophobia, or xenophobia.

KEY OBJECTIVES

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

- Recognize different forms of online hate, including gender-based hate.
- Understand the psychological and social impact of hate speech.
- Learn where the line is between free speech and hate speech.
- Respond appropriately—whether you're a target, bystander, or moderator.
- Contribute to positive, inclusive online spaces.

KEY CONCEPTS

- What is Hate Speech?
- Hate speech targets people's identity—their race, religion, ethnicity, gender, sexual orientation, disability, or immigration status—and can include:
- Slurs and derogatory language ("Go back to your country," "You don't belong here")
- Calls for violence or extermination ("They should all be killed")
- Spreading harmful stereotypes ("All women are liars," "Refugees are criminals")
- Misogynistic hate ("She deserves it because she's a woman")

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Impact of Online Hate

- On individuals: Fear, anxiety, trauma, self-censorship
- On communities: Polarization, exclusion, normalization of discrimination
- On society: Encourages offline violence, weakens democratic dialogue

Intersectionality: Why Some Groups Are Targeted More

Online hate often overlaps:

- A Black woman may face both racism and sexism simultaneously (misogynoir).
- LGBTQ+ people face homophobic and transphobic slurs alongside gendered abuse.
- Refugee women may experience xenophobia combined with misogyny.

How Hate Spreads Online

- Dogpiling: Many users attack someone at once.
- Echo chambers: Hate groups amplify each other's messages.
- Memes & coded language: Hate disguised as "jokes" or symbols.
- Disinformation campaigns: Spreading false claims to justify hate.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Identify Hate Speech
    - Look for language that targets specific groups based on their identity, race, religion, gender, or other characteristics.
    - Recognize calls for violence, hatred, or discrimination.
2. How to Respond as a Bystander

- Support the Target
- Send a private message offering help.
- Publicly show solidarity if it feels safe.
- Report the Content
- Use the platform's hate speech reporting options.
- Add details (why it's hate speech, screenshots).
- Disrupt the Hate
- Counter misinformation with facts.
- Flood hateful hashtags with positive content (counter-speech).
- Protect Yourself
- Don't engage directly with organized hate groups.
- Avoid boosting hateful content's visibility by quoting or sharing it.

3. How to Report Hate Speech
    - Use the platform's report button to flag offensive content.
    - Provide details about the hate speech and why it violates community guidelines.

REAL-LIFE SCENARIO

Scenario: Tom encounters a post on social media that includes hate speech towards a minority group. He reports the post to the platform and encourages others to speak out against harmful content.

REFLECTIVE QUESTION:

What steps would you take if you saw hate speech online, and how can you contribute to promoting respectful discussions?

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: How to Handle Online Hate

- Do you know how to recognize hate speech online? Yes / No
- Have you reported hate speech on any platform? Yes / No
- Do you participate in promoting positive conversations online? Yes / No
- (Provide feedback based on their answers and offer suggestions for promoting inclusivity.)

RECAP

- Recognize hate speech and its harmful effects.
- Report hateful content to moderators or platform administrators.
- Foster a positive, respectful online environment.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 9

Digital Footprint



OVERVIEW

Everything you do online—posts, comments, likes, searches—leaves a digital trace. Your digital footprint can:

- Shape your online reputation for employers, schools, or future relationships.
- Be used by scammers or stalkers to gather personal info.
- Feed into targeted advertising & data collection by tech companies.
- In some cases, expose you to online harassment or blackmail (especially for women).

Your footprint isn't just what you post—it's also what others share about you, and what companies collect silently in the background.

Example: A photo shared on social media might include location metadata. Combined with other online info, someone could figure out where you live or work.

This module helps you understand, audit, and control your digital footprint to protect your privacy and reputation.

KEY OBJECTIVES

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

- Understand how digital footprints are created—both actively and passively.
- Identify risks tied to oversharing (identity theft, stalking, online abuse).
- Learn how to manage and clean up old or unwanted digital content.
- Proactively shape a positive online presence that reflects your current values.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

KEY CONCEPTS

1. Active vs. Passive Digital Footprint

- Active footprint: What you post or share—photos, tweets, comments, reviews.
- Passive footprint: Data collected about you—IP addresses, cookies, location tracking, search history.

2. Why Your Digital Footprint Matters

- Privacy Risks: Too much public info can make it easy for scammers or stalkers to target you.
- Reputation Risks: Old posts may not reflect who you are now but could affect jobs, scholarships, or relationships.
- Security Risks: Public details like your birthday or pet's name can be used for password hacking.
- Gender-Specific Risks: Women often face doxxing (leaking personal info), harassment, and misuse of photos.

3. Who Looks at Your Digital Footprint?

- Employers & Universities: Checking your online presence before hiring or accepting you.
- Data Brokers: Selling your personal info for advertising or analytics.
- Harassers & Abusers: Using online clues to intimidate or stalk.
- Algorithms: Recommending content based on your browsing & social activity.

4. How Digital Footprints Become Permanent

- Even if you delete a post:
- Screenshots or archives may still exist.
- Cached pages can remain online for years.
- Data you "agree" to share (via app permissions) might already be sold.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Control Your Privacy Settings
   - Go to the privacy settings of each social media platform.
   - Adjust who can see your posts, who can comment, and who can contact you.
   - Periodically review these settings as platforms often update them.
2. How to Check Your Digital Footprint
   - Search your name or username in a search engine.
   - Review the results and decide whether you want to delete or edit anything that may negatively impact your reputation.

REAL-LIFE SCENARIO

Scenario: Mark realizes that his old blog posts from a decade ago are still accessible online, and they no longer align with his current views. He uses the platform's privacy settings to limit access and decides to update or delete outdated content.

REFLECTIVE QUESTION:

What online actions or content could be part of your digital footprint, and how might they affect your future?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: How Well Do You Manage Your Digital Footprint?

- Do you regularly review and update your privacy settings? Yes / No
- Have you ever searched yourself online to see what information is available? Yes / No
- Do you think about the long-term consequences before posting content online? Yes / No
- (Provide feedback based on their answers and suggest steps for improving digital footprint management.)

RECAP

- Understand that everything you do online can contribute to your digital footprint.
- Regularly review and adjust your privacy settings to maintain control over your online presence.
- Always consider the long-term impact of your online actions.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 10

Fake News



OVERVIEW

Fake news is more than just "wrong information"—it is often deliberately designed to mislead, manipulate emotions, or cause harm. It can:

- Spread fear or confusion during crises (e.g., health scares, natural disasters).
- Fuel hate speech and discrimination against specific groups.
- Damage reputations, especially of women and public figures.
- Influence elections, public opinion, and social movements.

Women and marginalized communities are frequent targets of fake news campaigns.

Example: Female journalists and activists often face fake stories about their personal lives to discredit them or provoke harassment.

Understanding how fake news works—and how to stop it—protects you, your community, and society.

KEY OBJECTIVES

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

- Recognize common signs of fake news and misinformation.
- Understand why people believe and share fake news (confirmation bias, emotional triggers).
- Learn practical fact-checking tools and methods.
- Take action to reduce the spread of misinformation in your networks.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

KEY CONCEPTS

1. What is Fake News?

Fake news includes:

- Completely false stories created to deceive.
- Manipulated content (doctored images, deepfakes).
- Misleading headlines attached to unrelated or distorted facts.
- Clickbait rumors designed to generate profit.

2. Why People Believe & Share Fake News

- Confirmation Bias: We tend to believe things that align with our existing beliefs.
- Emotional Triggers: Fear, anger, or outrage make us react quickly without checking.
- Social Pressure: Seeing friends share something makes it feel more credible.
- Echo Chambers: Algorithms show us similar content, reinforcing false ideas.

3. How Fake News Spreads

- Viral Social Media Posts → Shared thousands of times before being debunked.
- Bots & Troll Farms → Automated accounts amplifying disinformation.
- Misleading Images/Videos → Old photos shared as "breaking news" in a new context.

4. Impact of Fake News

- On individuals: Panic, confusion, reputational harm.
- On communities: Polarization, mistrust, hate.
- On society: Undermines democracy, fuels extremist movements.
- For women & minorities, fake news can escalate into targeted harassment, doxxing, or even offline violence.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Spot Fake News
   - Check the credibility of the source—look for reputable news outlets.
   - Verify the author's credentials and check if the story is covered by multiple trusted sources.
   - Be skeptical of sensational headlines and verify the information before sharing.
2. How to Fact-Check Information
   - Use fact-checking websites like Snopes, FactCheck.org, or PolitiFact.
   - Cross-reference the information with multiple sources to see if the claims are supported by evidence.

REAL-LIFE SCENARIO

Scenario: Julia receives an urgent post claiming that a local event is being canceled due to a health concern. Before sharing, she checks the official event page and finds that the post is fake. She warns her friends not to trust unverified sources.

REFLECTIVE QUESTION:

How do you ensure that the information you share online is accurate?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: Can You Spot Fake News?

- Do you check the credibility of sources before sharing information? Yes / No
- Have you ever shared something only to find out it was fake news? Yes / No
- Do you regularly use fact-checking websites? Yes / No
- (Provide feedback based on their answers and encourage more vigilance in verifying news.)

RECAP

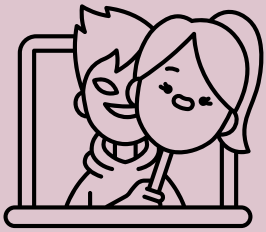
- Always verify news from multiple credible sources before sharing it.
- Be aware of fake news techniques, such as sensationalism and misleading headlines.
- Use fact-checking websites to verify information before believing or sharing it.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 11
Catfishing



OVERVIEW

Catfishing isn't just about "pretending to be someone else." It can lead to:

- Emotional harm (betrayal, humiliation, broken trust)
- Financial scams (romance scammers asking for money)
- Identity theft (your own photos/info being used in fake profiles)
- Blackmail or sextortion, especially targeting women

Women are often deliberately targeted with catfishing tactics, especially on dating apps and social media, because scammers assume they are more likely to be emotionally or financially manipulated.

KEY OBJECTIVES

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

- Recognize red flags of catfishing and online deception
- Use safe verification methods before trusting someone online
- Learn how to respond, block, and report catfishing attempts
- Understand why people catfish and how scams evolve

KEY CONCEPTS

1. What is Catfishing?

- Catfishing is when someone creates a fake online identity to:
- Trick you into a romantic or emotional relationship
- Scam you for money or personal data
- Harass or embarrass you
- Impersonate someone for revenge or control

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

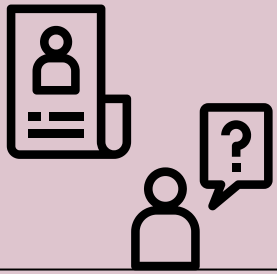
1. How to Recognize Catfishing
   - Look for inconsistent or overly vague personal details.
   - Be wary if the person refuses to meet in real life or engage in video calls.
   - Watch out for requests for money or personal help that seem suspicious.
2. How to Protect Yourself from Catfishing
   - Always verify someone's identity through multiple channels, such as video calls or other online accounts.
   - Never share financial details or sensitive information with someone you haven't met in person.

REAL-LIFE SCENARIO

Scenario: Emma starts chatting with someone online who seems too perfect. After weeks of online communication, the person starts asking for money to cover a supposed emergency. Emma becomes suspicious and decides to stop communicating and report the account.

REFLECTIVE QUESTION:

How can you verify that someone you meet online is who they claim to be?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

2. Why Do People Catfish?

- Romance scams: Gaining your trust, then asking for money ("I need money for a flight to see you").
- Insecurity or low self-esteem: Pretending to be more attractive, successful, or younger.
- Entertainment or boredom: Playing with someone's emotions for fun.
- Harassment or revenge: Using fake profiles to bully or stalk.
- Identity theft: Using your pictures/details to trick others.

3. Common Tactics Catfishers Use

- Too Good to Be True → They seem perfect or overly interested in you right away.
- Fast Emotional Attachment → Quickly saying "I love you," "you're my soulmate."
- Avoiding Video Calls or Meetings → Always have an excuse ("My camera is broken").
- Inconsistent Stories → Details about their life don't add up.
- Stolen Photos → Using pictures of models, influencers, or random people.
- Requests for Money or Favors → Emergency medical bills, travel tickets, or "helping with a business deal."



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: Are You a Victim of Catfishing?

- Has anyone online ever asked you for money or personal information? Yes / No
- Do you always verify someone's identity before getting too involved? Yes / No
- Have you encountered any red flags that made you suspicious about someone online? Yes / No
- (Provide feedback based on their answers and suggest steps to avoid being catfished.)

RECAP

- Always verify the identity of people you meet online.
- Be cautious about sharing personal or financial details.
- Report any suspicious profiles or requests for money.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 12
Trolling



OVERVIEW

Trolling isn't just someone "being annoying online." It can be:

- Harmless provocation (someone teasing or making jokes).
- Disruptive & inflammatory behavior to derail discussions.
- Targeted harassment, often tied to sexism, racism, or other hate speech.
- Coordinated trolling campaigns designed to silence people—especially women, activists, or journalists.

Trolling can cause emotional distress, mental health strain, and fear, especially when it escalates into threats or doxxing (sharing private info).

KEY OBJECTIVES

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

- Recognize different types of trolls and their tactics
- Learn safe, effective responses—when to ignore, report, or document
- Understand the psychological & social impact of trolling
- Promote healthier online spaces by not feeding trolls

KEY CONCEPTS

1. What is Trolling?

- Trolling is deliberately provoking others online for attention, amusement, or disruption. Trolls often:
- Post offensive or controversial comments to get reactions.
- Attack people's identity, beliefs, or appearance.
- Spread misinformation just to confuse others.
- Target specific people (e.g., women in gaming or politics) to intimidate them.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

2. Why Do People Troll?

- For Fun (Casual Trolls): Enjoying reactions and chaos.
- For Power (Aggressive Trolls): Trying to dominate or silence others.
- For Ideology (Hate Trolls): Pushing sexist, racist, or extremist agendas.
- For Revenge: Targeting someone personally.
- For Money: Some are paid to troll in political or commercial campaigns.

3. Different Levels of Trolling

- Mild Annoyance: Jokes or sarcastic comments.
- Harassment: Insults, name-calling, spamming.
- Abuse & Hate Speech: Sexist, racist, or violent threats.
- Organized Attacks: Multiple trolls coordinating to overwhelm a target.

Women, LGBTQ+ individuals, and minorities are more likely to face targeted trolling that includes personal insults, slurs, or threats.

4. Impact of Trolling

- Emotional Harm: Stress, anxiety, fear.
- Silencing Effect: People stop sharing opinions online.
- Community Damage: Healthy discussions turn toxic.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Identify Trolling Behavior
   - Look for comments that are designed to provoke, insult, or upset others.
   - Trolls often use inflammatory language or try to manipulate emotions.
2. How to Respond to Trolls
   - Consider ignoring the troll and not responding to their provocations.
   - Use platform tools to report abusive behavior or block the troll.
   - Stay calm and avoid escalating the situation.

REAL-LIFE SCENARIO

Scenario: Tom posts an opinion on a social media platform, and a user responds with aggressive comments. Instead of engaging, Tom ignores the troll and reports the comments. The user is eventually banned from the platform.

REFLECTIVE QUESTION:

How do you feel when you encounter trolling behavior online, and how can you respond effectively?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: How Do You Handle Trolling?

- Do you engage with trolls when they post provocative comments? Yes / No
- Do you report or block individuals who troll you or others? Yes / No
- Have you ever experienced the negative effects of trolling? Yes / No
- (Provide feedback based on their answers and offer strategies for handling trolls.)

RECAP

- Avoid engaging with trolls—ignore or block them instead.
- Use the reporting tools on platforms to flag abusive behavior.
- Promote respectful communication and foster positive online interactions.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 13

Consent for Sharing Photos & Videos



OVERVIEW

In the digital age, sharing photos and videos seems easy—but once something is online, it can spread instantly and permanently. Without consent:

- You could violate someone's privacy or harm their safety.
- Shared images could be used for harassment or blackmail.
- It can lead to legal consequences for both the sharer and platforms hosting the content.

Women and marginalized groups are disproportionately harmed by non-consensual sharing—photos can be sexualized, misused, or weaponized for harassment, sometimes leading to real-life threats or violence.

KEY OBJECTIVES

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

- Understand why explicit consent is essential before sharing any image or video
- Learn how to ask for and give consent clearly
- Recognize the risks & consequences of sharing without permission
- Know how to protect yourself and others from privacy violations

KEY CONCEPTS

1. What is Consent in Digital Sharing?

- Consent means clear, voluntary, and informed permission from the person in the photo/video before you:
- Post it on social media
- Send it in a private chat
- Use it for any public purpose
- Silence is NOT consent. Just because someone didn't say "no" doesn't mean they agreed.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

2. Why Is Consent Important?

- Ethical Reasons → Respecting people's autonomy & privacy.
- Safety Reasons → Some people may face harm if their location, face, or activities are revealed.
- Legal Reasons → Many countries have laws protecting image rights & privacy.
- Emotional Impact → Sharing without consent can cause embarrassment, anxiety, or trauma.

3. Common Misconceptions

❌ "It's my phone, I can post whatever I want."

✅ Wrong. Even if you took the photo, the person in it still owns their image rights.

❌ "But it's already online!"

✅ Just because it's visible doesn't mean you can reshare or distribute it further without permission.

❌ "It was a joke, no harm intended."

✅Intent doesn't erase harm—private moments can have serious consequences when made public.

4. Risks of Sharing Without Consent

- Reputation damage → embarrassing or private photos going public
- Doxxing → revealing someone's location or identity
- Sextortion & blackmail → intimate images being misused
- Online abuse campaigns → images fueling trolling or harassment
- Legal action → lawsuits, platform bans, or even criminal charges

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

STEP-BY-STEP GUIDE

1. How to Ask for Consent Before Sharing
   - Ask the person directly whether they are comfortable with you sharing their photo or video.
   - Provide details about where and how the content will be shared (e.g., social media, blog).
   - Respect their decision if they decline to give consent.
2. How to Handle Consent in Group Settings
   - In group photos or videos, ask everyone involved if they are comfortable with the content being shared.
   - Be mindful of whether anyone in the background or far off-screen is inadvertently included in the image.

REAL-LIFE SCENARIO

Scenario: Sarah takes a group photo at a party and wants to share it on her social media. Before posting, she checks with her friends to see if they are comfortable with it. One friend expresses concerns about being online, so Sarah decides not to post the image out of respect for her privacy.

REFLECTIVE QUESTION:

What are some reasons someone might not want their photo or video shared online, and how can you respect their decision?



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: Are You Asking for Consent Before Sharing?

- Do you always ask for permission before sharing photos or videos of others? Yes / No
- Have you ever posted something that someone later asked you to take down? Yes / No
- Do you respect the privacy settings of others when it comes to their photos and videos? Yes / No
- (Provide feedback based on their answers and encourage ongoing respect for privacy.)

RECAP

- Always ask for explicit consent before sharing photos or videos of others.
- Be aware of the right to privacy and ensure everyone involved is comfortable with the sharing of content.
- If in doubt, respect the decision not to share.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

MODULE 14

Balancing Time on Social Media



OVERVIEW

Social media helps us connect, learn, and share, but too much time online can:

- Affect mental health → anxiety, depression, FOMO (fear of missing out)
- Hurt self-esteem → comparing your life to others' highlight reels
- Disrupt sleep & focus → late-night scrolling reducing rest & productivity
- Feed addictive patterns → endless notifications keeping you hooked

For women and young people, overuse can also lead to:

- Increased body image pressures from unrealistic beauty standards
- More exposure to harassment or toxic online communities
- Emotional burnout from constant social comparison

KEY OBJECTIVES

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

- Understand the mental, emotional, and social impact of overusing social media
- Learn practical strategies to manage your time online
- Develop a more mindful, intentional relationship with social media

KEY CONCEPTS

1. Digital Well-Being

- Digital well-being means using technology in ways that improve your life, not control it. It's about setting healthy boundaries with screens so you stay in charge of your time and energy.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

2. Social Media Addiction
Signs of problematic use include:

- Checking apps compulsively, even when busy
- Feeling anxious when not online
- Losing time or neglecting real-life responsibilities
- Constantly comparing yourself to others online

3. Mindful Use
Mindful use means being intentional with your online time:

- Ask: "Why am I opening this app right now?"
- Notice how you feel before and after scrolling
- Focus on quality content that inspires or educates you

Step-by-Step Guide

- How to Set Time Limits for Social Media
  - Use built-in features on devices (like Screen Time on iPhones or Digital Wellbeing on Android) to set limits for social media apps.
  - Schedule specific times during the day to check social media, and stick to those boundaries.
- How to Unfollow or Mute Accounts
  - Unfollow accounts that make you feel anxious, inadequate, or negatively affect your mood.
  - Use the mute feature to silence posts or stories without unfollowing or blocking the person.

Real-Life Scenario

Scenario: Lisa spends hours scrolling through social media each evening, leading to feelings of comparison and stress. After reading about digital well-being, she decides to limit her social media use to 30 minutes per day and removes any accounts that promote negativity. She feels more productive and less anxious.

Reflective Question:

How does social media usage affect your mood and overall well-being? What changes could you make to improve your balance?

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

INTERACTIVE ACTIVITIES

Quiz: Are You Balancing Your Social Media Time?

- Do you often feel overwhelmed or anxious after using social media? Yes / No
- Have you set limits on how much time you spend on social media each day? Yes / No
- Do you have a habit of checking social media first thing in the morning or last thing at night? Yes / No

(Provide feedback based on their answers and suggest strategies for healthier social media habits.)

RECAP

- Set time limits on social media use to maintain balance in your life.
- Follow or mute accounts that contribute to negative feelings or stress.
- Practice mindful social media usage and check in with how it affects your mood.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

CONCLUSION

In a world where digital interactions are increasingly intertwined with daily life, fostering digital literacy has never been more crucial. By equipping individuals with the skills to recognize, respond to, and protect themselves against online threats, we not only enhance personal safety but also contribute to creating a more respectful and inclusive digital environment. Empowered with digital literacy, users can confidently navigate online spaces, advocate for their own rights, and support others facing similar challenges. Strengthening digital skills is a proactive step toward a future where everyone can enjoy the benefits of technology without fear, promoting a culture of respect, safety, and empowerment in the digital world.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.