

## **ESAFETY** WOMEN

## **TOOLKIT**



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







# 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	55









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.









### **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.











### **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.









### **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







## 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. (<a href="https://fra.europa.eu/en/publication/2014/violence-against-women-euwide-survey-main-results-report">https://fra.europa.eu/en/publication/2014/violence-against-women-euwide-survey-main-results-report</a>)
- → 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.

(<a href="https://eige.europa.eu/publications-resources/publications/lithuania-laws-policies-domestic-violence">https://eige.europa.eu/publications-resources/publications/lithuania-laws-policies-domestic-violence</a>)









## 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/spainnews/2024/05/17/gender-violencesurges-in-spain-number-of-youngvictims-increased-by-32-last-yearfigures-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/20 21-06-17/in-spain-gender-violenceclaims-more-lives-in-last-30-daysthan-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 with 80% street harassment. 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-streetwomen-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/









## 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.

  <u>Country Fact Sheet | UN Women Data Hub</u>
- → 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









### 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.









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.







- 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









### Using Your Device Safely

#### **OVERVIEW**

The Importance of Digital Literacy in Combating Gender-Based Violence

#### **KEY OBJECTIVES**

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

- Set up basic security settings for your devices.
- Protect your personal data from common threats.
- Understand how to safely connect to networks like Wi-Fi and Bluetooth.

- Password Protection: Use strong, unique passwords for each of your devices and accounts. Include numbers, symbols, and both upper and lower-case letters.
- Software Updates: Always update your devices to the latest software version to ensure security patches are installed.
- Two-Factor Authentication (2FA): Add an extra layer of protection by requiring a second form of identification (e.g., a text message code) when logging in.
- Public Wi-Fi Safety: Avoid using public Wi-Fi for sensitive tasks like online banking unless you are connected through a Virtual Private Network (VPN).









#### 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?











#### 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.)

- 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.









### Connecting Safely



#### **OVERVIEW**

In this module, you will learn how to connect to networks and online services securely. You will explore how to safely use Wi-Fi, web browsers, apps, Bluetooth, and cloud services to protect your data from cyber threats.

#### KEY OBJECTIVES

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

- Recognize the risks of public and unsecured networks.
- Use secure Wi-Fi, web browsers, and apps safely.
- Understand the importance of protecting data on the cloud and when using Bluetooth.

- 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.









#### 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?











#### 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.)

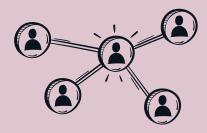
- Always use a VPN when connecting to public Wi-Fi.
- Keep your web browser and apps updated for security.
- Review and limit app permissions.
- Use encrypted cloud storage for sensitive data.







### Being social online



#### **OVERVIEW**

In this module, you will learn how to engage in social interactions online safely. Whether it's via email, social media, blogging, or online gaming, it's important to understand the risks of sharing personal information and how to protect yourself.

#### **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.

- Social Media Privacy Settings: Use privacy controls to limit who can see your posts and personal information.
- Cyberbullying & Online Harassment: Learn how to identify, report, and block harassment or harmful behavior online.
- Safe Sharing Practices: Avoid oversharing personal details like location or sensitive information on social media.
- Email Safety: Be cautious of unsolicited emails, and avoid clicking on suspicious links or attachments.









#### STEP-BY-STEP GUIDE

- 1. How to Adjust Privacy Settings on Social Media
  - Go to your social media account settings.
  - Find the privacy section and adjust visibility options for your posts.
  - Enable two-factor authentication for an extra layer of protection.
- 2. How to Report Cyberbullying
  - If someone is bullying you online, use the platform's reporting tool to flag inappropriate content.
  - Block the user to prevent further harassment.
  - Reach out to support groups or local authorities if necessary.

#### REAL-LIFE SCENARIO

Scenario: Emma posts a photo on Instagram but later receives derogatory comments. She uses the platform's privacy settings to limit who can comment on her posts and blocks the user who is harassing her. Emma reports the incident to Instagram for further investigation.

#### **REFLECTIVE QUESTION:**

What steps would you take if you encounter cyberbullying or harassment on social media?











#### 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
- (Provide feedback based on their answers and offer suggestions.)

- Adjust your social media privacy settings to control who can view your posts.
- Always report and block online harassment or cyberbullying.
- Avoid sharing personal information like location on social media.
- Stay vigilant and safe while interacting online.







### Life Admin Online

#### **OVERVIEW**

In this module, you will learn how to safely manage everyday tasks such as online banking and shopping. Securing your financial and personal information is crucial to avoid identity theft and fraud.



#### 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.

- Online Banking Security: Always use official banking apps or websites, and enable two-factor authentication for extra protection.
- Phishing Scams: Be cautious of unsolicited emails or messages that ask for sensitive information or financial details.
- Secure Shopping: Use trusted online stores with secure payment systems, and avoid shopping on unsecured websites.
- Fraud Detection: Regularly check bank statements and credit card transactions for unauthorized activity.









#### 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?









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.)

- Always use official banking apps and secure websites for financial transactions.
- Be wary of phishing scams and avoid clicking on suspicious links or downloading unknown attachments.
- Shop online only on secure, trusted websites and use reliable payment methods.
- Regularly review your bank statements and financial activity to detect any fraudulent transactions.



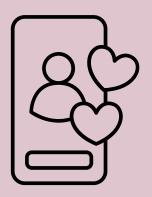




### Dating & Relationships Online

#### **OVERVIEW**

In this module, you will explore how to safely navigate online dating and relationships. Understanding the risks and best practices will help you maintain a positive and secure experience while interacting with others on dating apps or social media platforms.



#### KEY OBJECTIVES

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

- Recognize potential risks associated with online dating.
- Learn how to keep your personal information secure when interacting with others.
- Understand how to handle red flags or uncomfortable situations.

- Personal Information Security: Avoid sharing sensitive details, like your home address or financial information, until you feel fully comfortable with someone.
- Red Flags in Online Dating: Look out for behaviors such as overly possessive or secretive actions, manipulative language, or requests for money.
- Safe Meeting Practices: When meeting someone in person for the first time, choose a public place, and let a trusted friend know your plans.









#### STEP-BY-STEP GUIDE

#### 1. How to Set Up a Safe Online Dating Profile

- Choose a username and profile picture that don't reveal too much personal information.
- Avoid sharing details such as your home address, workplace, or financial situation.
- Use the platform's privacy features to control who can see your profile.

#### 2. How to Spot Red Flags

- Pay attention if someone is overly eager to communicate or is unwilling to share information about themselves.
- Watch for requests for money or urgent emotional appeals.
- Trust your instincts if something feels off.

#### REAL-LIFE SCENARIO

Scenario: Sarah meets a person on a dating app who seems kind and genuine at first. Over time, they begin to ask for money under the pretense of a personal emergency. Sarah remembers the red flag signs and blocks them immediately. She reports the account to the platform for further action.

#### **REFLECTIVE QUESTION:**

What signs would make you feel uncomfortable or suspicious when communicating with someone online?











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
- $\bullet\,$  Do you feel comfortable asking a trusted friend for advice if you're unsure about someone? Yes / No
- (Provide feedback based on their answers and offer safety tips.)

- Keep your personal details private when dating online.
- Watch for red flags such as requests for money or secrecy.
- Always meet in public places for the first few dates and let someone know your plans.







### Navigating Difficult Situations Online



#### **OVERVIEW**

In this module, you will learn how to manage difficult online situations, such as conflicts in online communities, harassment, or when you encounter a controversial issue. These skills are important for maintaining a positive digital experience.

#### KEY OBJECTIVES

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

- Understand how to handle online conflicts calmly and constructively.
- Learn the best practices for de-escalating a difficult situation.
- Know when and how to report harmful content or behaviors.

- Conflict Resolution: Engage respectfully in discussions and avoid escalating arguments online.
- Reporting Harmful Content: Know how to report hate speech, threats, and harassment to platform moderators or authorities.
- De-escalation Techniques: Focus on remaining calm, avoiding inflammatory language, and seeking mediation if necessary.









#### STEP-BY-STEP GUIDE

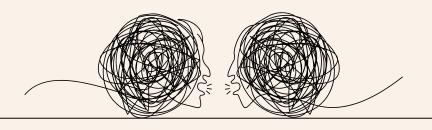
- 1. How to Manage Online Disagreements
  - Stay calm and don't engage in hostile language.
  - Respond with facts, not emotions, when addressing disagreements.
  - If the situation escalates, step away and disengage from the conversation.
- 2. How to Report Harmful Content
  - Identify the harmful content or behavior.
  - Use the platform's built-in reporting feature.
  - Provide as much detail as possible, including the reason for your report.

#### **REAL-LIFE SCENARIO**

Scenario: Mark finds a heated discussion in a social media group that quickly turns hostile. Instead of participating in the argument, he calmly expresses his perspective without insults and reports any inappropriate comments. Later, the group moderator removes the harmful posts.

#### **REFLECTIVE QUESTION:**

How do you typically respond to online disagreements, and what methods help you stay calm in difficult situations?











#### Quiz: Conflict Resolution in Online Spaces

- Do you try to stay calm when confronted with online conflict? Yes / No
- Do you report harmful or inappropriate content you encounter? Yes / No
- Have you ever successfully de-escalated a situation online? Yes / No
- (Provide feedback based on their answers and offer tips for handling online conflicts.)

- Remain calm and respectful during online disagreements.
- Use de-escalation techniques to prevent conflicts from escalating.
- Report harmful content or behaviors when necessary.







### Cyberbullying

#### **OVERVIEW**

In this module, you will learn how to recognize, respond to, and protect yourself from cyberbullying. Understanding the emotional and psychological impact of cyberbullying is essential for creating a safer and more supportive online environment.

#### KEY OBJECTIVES

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

- Identify signs of cyberbullying.
- Understand the impact of cyberbullying on mental health.
- Learn steps to take if you or someone else is being cyberbullied.

- Signs of Cyberbullying: Repeated harassment, spreading rumors, sending hurtful messages, or exclusion from online groups.
- Mental Health Impact: Cyberbullying can lead to feelings of isolation, anxiety, depression, and low self-esteem.
- Reporting and Seeking Help: Understand how to report cyberbullying on social media platforms and seek support from trusted individuals.









#### STEP-BY-STEP GUIDE

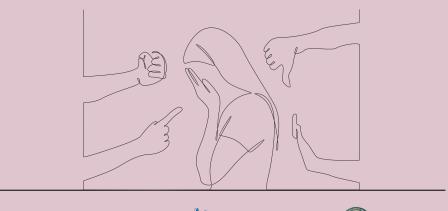
- 1. How to Recognize Cyberbullying
  - Look for signs like aggressive language, rumors, exclusion, or personal attacks.
  - Pay attention to the emotional toll it may take on the person targeted.
- 2. How to Report Cyberbullying
  - Identify the harmful behavior on the platform.
  - Use the platform's 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?











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.)

- 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.







### Online Hate

#### **OVERVIEW**

In this module, you will learn how to recognize, prevent, and respond to online hate speech. The goal is to promote respectful, inclusive, and constructive conversations online while understanding the impact of hate speech.



#### KEY OBJECTIVES

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

- Identify hate speech and understand its impact.
- Understand your role in preventing and reporting online hate.
- Learn how to foster a positive online environment.

- Hate Speech: Any speech, gesture, conduct, writing, or display that incites violence or discrimination against others based on race, religion, or other protected categories.
- Impact of Hate Speech: It can cause harm to individuals, communities, and societies, often perpetuating stereotypes and fostering division.
- Reporting and Moderating: Know how to report hate speech on social media platforms and support efforts to combat online hate.









#### 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 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?











#### 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.)

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







# Digital Footprint



#### **OVERVIEW**

In this module, you will learn about your digital footprint—how your online activities create a permanent record and influence your privacy, reputation, and future opportunities. Understanding how to manage your digital footprint is essential for maintaining control over your online presence.

# **KEY OBJECTIVES**

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

- Understand what a digital footprint is and how it's created.
- Learn how to manage and control your digital footprint.
- Recognize the potential long-term impact of your online actions.

- Active vs. Passive Footprint: Your active footprint is created by actions like
  posting on social media, while your passive footprint is created by things
  like website visits or searches.
- Privacy Settings: Adjust the privacy settings of your social media accounts to limit who can see your information.
- Search Engine Visibility: Be aware of what appears when someone searches your name or other personal information.









- 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?











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.)

- 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.







# Fake News

#### **OVERVIEW**

In this module, you will explore how to identify fake news and misinformation online. Being able to spot fake news is essential for maintaining a well-informed and responsible online presence.



# KEY OBJECTIVES

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

- Recognize the signs of fake news and misinformation.
- Learn how to verify information before sharing it.
- Understand the impact of fake news on society and individuals.

- Fake News: False or misleading information presented as news, often to deceive or manipulate.
- Fact-Checking: Using reputable sources and fact-checking websites to verify the accuracy of information.
- Confirmation Bias: The tendency to believe information that confirms your existing beliefs, which can contribute to the spread of fake news.









# 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?











# 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.)

- 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.







# Catfishing



#### **OVERVIEW**

In this module, you will learn how to identify catfishing—when someone creates a fake identity online to deceive others. Understanding how to protect yourself from these scams is crucial for safe online interactions.

# KEY OBJECTIVES

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

- Recognize the signs of catfishing.
- Understand how to protect yourself from online deception.
- Learn how to handle and report catfishing incidents.

- Catfishing: The act of creating a fake online persona to manipulate or deceive others.
- Red Flags of Catfishing: Inconsistent information, reluctance to meet in person, and requests for money or personal favors.
- How to Protect Yourself: Verify the identity of online acquaintances and avoid sharing sensitive personal information too soon.









# 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?











# 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.)

- 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.







# **Trolling**



#### **OVERVIEW**

In this module, you will explore the phenomenon of trolling—when someone intentionally posts inflammatory or offensive comments to provoke others. You'll learn how to deal with trolls and maintain a positive online environment.

# KEY OBJECTIVES

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

- Recognize the signs of trolling.
- Learn how to respond effectively (or not at all) to trolls.
- Understand the impact trolling can have on others.

- Trolling: Deliberately provoking others by posting offensive or inflammatory comments.
- Dealing with Trolls: Ignoring or reporting trolls can be the best way to handle them. Engaging in arguments often makes things worse.
- Online Etiquette: Promote respectful communication and avoid feeding into negative behavior.







# 1. How to Identify Trolling Behavior

- Look for comments that are designed to provoke, insult, or upset others.
- o 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?











# 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.)

- 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.







# Consent for Sharing Photos & Videos



#### **OVERVIEW**

In this module, you will learn about the importance of consent when it comes to sharing photos and videos online. Understanding when and how to ask for consent is vital to respecting others' privacy and protecting your own.

# KEY OBJECTIVES

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

- Understand the importance of asking for consent before sharing others' photos and videos.
- Learn how to respect privacy when posting online content.
- Recognize the potential consequences of sharing images or videos without permission.

- Consent: Explicit permission given by an individual to share or post their image, video, or personal information online.
- Right to Privacy: Everyone has the right to control their own image and personal content.
- Respectful Sharing: Even if a photo or video is publicly available, it doesn't necessarily mean it's okay to share without consent.









- 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?









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.)

- 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.







# Balancing Time on Social Media

#### **OVERVIEW**

In this module, you will learn about the importance of balancing your time on social media. While social media can be a valuable tool for connection, overuse can have negative effects on mental health and wellbeing. Learning to manage your social media habits is key to achieving a healthy online lifestyle.



# KEY OBJECTIVES

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

- Understand the impact of excessive social media use on mental health.
- Learn strategies for managing time spent on social media.
- Develop habits for a healthier relationship with social media.

- Digital Well-Being: Maintaining a healthy relationship with technology by setting limits and boundaries on screen time.
- Social Media Addiction: The compulsive use of social media that can interfere with daily life and well-being.
- Mindful Use: Being aware of how much time you spend on social media and using it in a balanced, intentional way.









#### 1. 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.

#### 2. 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?











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.)

- 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.







# **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.

