CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Non-formal education practices:

Doxing

R2 CYBER TOOLKIT

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 European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#15	**Anti-Doxing Tactics: Keeping Your Private Life Private**
Threat(s)	**Doxing**
	Doxing, in the context of youth cyber-threats, is the malicious practice of collecting and publishing private or identifying information about an individual without their consent, typically through the internet. This act is often intended to intimidate, threaten, harass, shame, or exert power over the victim. Doxing can lead to severe consequences for young individuals, including psychological distress, loss of privacy, and in some cases, physical harm. It exploits the accessibility of personal information in the digital age, violating individuals' right to privacy and safety online.
Typology	Simulation exercises
Duration	110 minutes/1 hour & 50 Minutes (can be adjusted based on depth of activities)
Modality	In-presence [classroom setting]
Aim	The aim of this practice is to equip participants with the knowledge and skills needed to protect their privacy online, understand ethical online behaviour, and respond effectively to doxing and related cyber threats.
Learning Objectives	Privacy Protection Strategies: Able to employ strategies to protect their own privacy and sensitive information online, reducing the risk of becoming a doxing victim. Ethical Online Conduct: Demonstrate an understanding of ethical behaviour in online spaces, committing to respect the privacy and dignity of others. Critical Response to Cyberbullying: Develop skills to respond appropriately to cyberbullying and harassment, including actions to take if they or someone they know is a victim of doxing. Risk Mitigation for Identity Theft: Apply knowledge of how to safeguard personal and financial information to prevent identity theft and fraud. Legal Literacy Regarding Doxing: Understand their legal rights and the potential legal actions that can be taken against perpetrators of doxing, as well as the legal implications of engaging in doxing.
Trainee profile	Age Group: 15-17 years old Educational Background: High school students s Prerequisites: Basic understanding of internet use and social media platforms
n° participants	20-25
Materials	Internet-connected devices (laptops/tablets) Projector and screen for presentations Whiteboard and markers Printed handouts on privacy protection strategies and legal rights

	Scenario cards for simulation exercises Notebooks and pens for participants
Preparation	Set Up Venue: Arrange the classroom seating in a way that facilitates group discussions and easy viewing of the projector screen. Prepare Materials: Prepare the computers/tablets with necessary software and internet access. Print and organize handouts and scenario cards.
Implementation	*Introduction (10 minutes):* Welcome participants and introduce the topic of doxing. Explain the session's aim and learning objectives. *Overview of Doxing (10 minutes):* Present a brief overview of doxing, including real-life examples and potential impacts. Discuss why it's a significant threat, especially for youth. *Privacy Protection Strategies (15 minutes):* Distribute handouts and explain various strategies to protect personal information online (optional). Engage participants in a discussion about the importance of privacy settings on social media platforms. *Simulation Exercise: Identifying Vulnerabilities (20 minutes):* Divide participants into small groups. Provide each group with a fictional scenario (see annex) where they must identify potential privacy vulnerabilities and suggest protective measures. Groups present their findings and suggestions. *Ethical Online Conduct (10 minutes):* Discuss ethical behaviours online and the importance of respecting others' privacy. Highlight the consequences of unethical behaviours like doxing. *Critical Response to Cyberbullying (15 minutes):* Briefly present strategies for responding to cyberbullying and doxing.

	Conduct a role-playing exercise where participants practice responding to a doxing incident. *Risk Mitigation for Identity Theft (10 minutes):* Explain how to safeguard personal and financial information. Provide practical tips and examples. *Legal Literacy Regarding Doxing (10 minutes):* Discuss the legal aspects of doxing, including potential legal actions and rights of victims. Answer participants' questions about the legal implications. *Q&A and Wrap-up (10 minutes):* Open the floor for any remaining questions. Summarize key points and distribute evaluation forms for feedback (optional).
Tips and hints	Encourage open discussion and ensure every participant has a chance to contribute. Monitor group activities to provide guidance and keep discussions on track. Use real-life examples to make the session more relatable and impactful.
Safety measures	Ensure internet safety during online activities. Maintain a supportive environment where participants feel safe to share and discuss. Be prepared to handle any distress or discomfort among participants due to the sensitive nature of the topic.
Added value	Practical Knowledge: Concrete strategies and techniques to protect their online privacy and sensitive information. Ethical Awareness: A deeper understanding of ethical online behaviour and the importance of respecting others' privacy. Response Skills: Improved ability to respond effectively to cyberbullying and doxing incidents, including knowing what actions to take and who to contact for help. Risk Mitigation: Enhanced skills in safeguarding personal and financial information to prevent identity theft and fraud. Legal Understanding: A clearer comprehension of their legal rights regarding doxing and the potential legal actions against perpetrators.
Feedback and Evaluation	Encourage participants to provide feedback at the end of the session to improve future practices.

Conclusion	This practice effectively educates young individuals on the critical aspects of online privacy, ethical conduct, and cyberbullying response. This practice not only enhances their knowledge of legal rights and responsibilities but also fosters a respectful and safe online environment. Ultimately, the practice empowers youth to navigate the digital world confidently, mitigating the risks associated with doxing and other cyber threats, and reinforcing the importance of maintaining privacy and ethical behavior online.

Annex. Role-Playing Exercise: Responding to a Doxing Incident

Objective: To enable participants to practice responding to a doxing incident effectively, equipping them with the necessary skills to handle such situations in real life.
Duration: 15 minutes
Steps: **Introduction to the Exercise:** Explain the purpose of the role-playing exercise. Emphasize the importance of practicing responses to be better prepared in real-life situations. **Distribution of Scenario Cards:** Divide participants into small groups of 4-5. Distribute one scenario card to each group. **Group Preparation:** Allow each group time to read their scenario and discuss how they will respond. Encourage participants to refer to their handouts on response strategies and legal rights. **Role-Playing:** Each group acts out their scenario, with group members taking on different roles (e.g., the victim, the friend, the doxer, a bystander). Facilitators observe and provide guidance as needed. **Group Presentations:** Each group presents their scenario and demonstrates their response. After each presentation, allow time for feedback from facilitators and peers. **Debrief and Discussion:** Lead a brief discussion on what was learned from the exercise. Highlight effective strategies and address any areas for improvement.

Annex. Scenario Cards Examples

Scenario Card 1: Personal Info Exposed **Description**: A participant discovers that their personal information (home address, phone number) has been posted online by an anonymous user. **Task**: Determine immediate steps to secure their accounts, report the incident, and inform trusted adults or authorities.
Scenario Card 2: Friend in Distress **Description**: A participant's friend is being doxed after a heated online argument. The friend is distressed and doesn't know what to do. **Task**: Provide emotional support to the friend, help them report the incident, and advise on how to protect their information.
Scenario Card 3: Classmate Under Attack **Description**: A participant witnesses a classmate being doxed in a group chat. The doxer is someone they know. **Task**: Decide whether to confront the doxer, report the incident to the group admin and authorities, and support the victim.

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

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 European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.