Activity Title: Case Study – Digital Identity Theft

Objective:

To help participants understand the consequences of digital identity theft, identify security mistakes, and learn the steps for prevention and recovery.

Duration:

30 minutes

Materials Needed:

- **Printed copies** or a **digital display** of the case study scenario.
- **Notepads and pens** for note-taking during group discussion.

Scenario:

A user's online identity was stolen after they used an **unsecured public Wi-Fi connection** in a café to access their bank account. An attacker intercepted the connection and obtained their login credentials. Over the next few days, the attacker used the person's digital identity to make fraudulent purchases and take out loans in the user's name, severely damaging their credit score.

Instructions:

1. **Group Formation**:
   - Divide participants into **small groups** of 3-5 people.
2. **Discussion Points**:
   - Each group will read the scenario and discuss the following questions:
     - **What mistakes did the user make that led to their digital identity being stolen?**

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.

        - Focus on the use of unsecured public Wi-Fi for accessing sensitive accounts.
    - **What steps could have been taken to prevent this?**
        - Discuss best practices such as using a VPN, enabling two-factor authentication, and avoiding public Wi-Fi for sensitive transactions.
    - **How can individuals recover from digital identity theft?**
        - Explore steps such as contacting financial institutions, freezing credit, and reporting the theft to the authorities.

3. **Steps to Follow in Group Discussion**:
    - **Step 1**: Identify the **Security Mistakes**:
        - Groups should focus on the poor decision to use unsecured public Wi-Fi and other possible mistakes (e.g., not using two-factor authentication).
    - **Step 2**: Brainstorm **Preventative Measures**:
        - Discuss practical ways to prevent digital identity theft (e.g., using a VPN, checking for HTTPS, avoiding sensitive transactions on public Wi-Fi).
    - **Step 3**: Discuss **Recovery Steps**:
        - Groups should identify key recovery steps like contacting the bank, freezing accounts, and monitoring credit scores. They can also talk about the importance of reporting to legal authorities and changing passwords immediately.

Facilitator Role:

- Guide groups to focus on the **mistakes made** and **preventative solutions**.
- Encourage participants to think critically about recovery steps and how they could have protected their digital identity.
- Be available to answer questions and clarify best practices.

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.

Debrief (10 minutes):

- After group discussions, each group will share their conclusions:
    - The **mistakes** identified in the user's behavior.
    - **Preventative steps** that should have been taken to avoid the digital identity theft.
    - **Recovery steps** and actions to take if identity theft occurs.
- Facilitate a **whole-group discussion** on:
    - **Why is public Wi-Fi a risk?**
    - **What other common behaviors can put your digital identity at risk?**
    - **What should individuals do after their digital identity has been compromised?**

Key Takeaways:

- Avoid accessing sensitive accounts on public Wi-Fi.
- Always use a **VPN** or wait until a **secure network** is available.
- Protect accounts with **strong passwords** and **two-factor authentication**.
- If digital identity theft occurs, **act quickly** to minimize damage by contacting relevant institutions and freezing accounts.

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.