ESCAPE: TEACHER'S HANDBOOK

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAXXER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Co-funded by the European Union

ESCAPE: TEACHER'S HANDBOOK

1. Introduction

The Role of Cybersecurity in Healthcare Education
Cybersecurity is increasingly vital in healthcare, where data breaches and system vulnerabilities can directly impact patient safety. Educators must prepare learners to recognize and respond to digital threats in clinical environments.

Why Escape Rooms Are Effective Learning Tools?

Escape Rooms offer immersive, problem-based learning experiences. They foster collaboration, critical thinking, and real-time decision-making—skills essential in cybersecurity and healthcare.

Overview of Available Scenarios and Digital Materials

This handbook references a set of video scenarios and digital learning materials (see 'appendix'). These resources serve as teaching aids and can be integrated into your Escape Room design.

2. Learning Goals

Knowledge, Skills, and Attitudes Developed
Participants will:

- Understand basic cybersecurity principles (e.g., phishing, password hygiene, data protection).
- Practice teamwork and communication under pressure.
- Develop ethical awareness and responsibility in digital healthcare contexts.

Links to Healthcare Competencies
Activities align with competencies such as:

- Patient safety
- Data protection and privacy
- Interprofessional collaboration
- Clinical decision-making under uncertainty

Measuring Success and Learning
Use rubrics, observation checklists, and post-game reflections to assess:

- Problem-solving strategies
- Communication effectiveness
- Cybersecurity awareness

3. Designing the Escape Room

Choosing and Aligning Storylines

Use our Storyboards to select scenarios that reflect real-world healthcare cybersecurity challenges (e.g., ransomware in a hospital, unauthorized access to patient records).

Linking Puzzles to Cybersecurity Issues

Design puzzles that simulate:

- Identifying phishing emails
- Decoding secure passwords
- Tracing unauthorized access logs

Timing, Resources, and Modification Tips

- Recommended duration: 45–60 minutes
- Materials: printable clues, digital interfaces, props
- Tips: allow flexibility for group size, tech access, and learning level

4. Teacher's Role

Preparation Checklist

- Review scenario and learning goals
- Prepare materials and tech setup
- Brief students on rules and objectives

During Gameplay
Act as:

- Facilitator: guide without giving answers
- Observer: note group dynamics and problem-solving
- Guide: offer hints if teams are stuck

Managing Group Dynamics

Encourage inclusive participation, rotate leadership roles, and monitor for dominant or disengaged behavior.

5. Student Experience

Age/Ability Level
Adaptable for:

- Undergraduate healthcare students
- Continuing education for professionals
- Interdisciplinary teams

Ensuring Inclusivity and Engagement

- Use diverse scenarios
- Offer multiple entry points for solving puzzles
- Encourage reflection on ethical dilemmas

6. Practical Setup

Logistics, Classroom Setup, and Safety

- Use breakout rooms or physical spaces with clear boundaries
- Ensure tech reliability (Wi-Fi, devices)
- Provide safety instructions for physical props

Dealing with Technical Issues or Limited Resources

- Have backup puzzles or paper-based alternatives
- Use QR codes or printed screenshots if devices fail

7. Debrief & Reflection

Leading Reflection

Facilitate a structured discussion:

- What went well?
- What cybersecurity concepts were applied?
- How does this relate to real healthcare practice?

Example Debriefing Questions
- “What risks did your team identify?”
- “How did you decide who took the lead?”
- “What would you do differently in a real clinical setting?”

8. Adapting the Escape Room

Adjusting Difficulty

- Add or remove puzzles
- Vary time limits
- Introduce red herrings or ethical dilemmas

Scaling for Online or Hybrid Sessions

- Use collaborative platforms (e.g., Microsoft Teams, Zoom)
- Share puzzles via shared documents or breakout rooms
- Embed video scenarios as linked resources

9. Appendix

- Digital Learning Resources (to be added)
- Video Scenario List (with links or QR codes)
  - [Scenario 1: Data Breach in Radiology]
  - [Scenario 2: Phishing Attack on Nursing Staff]
  - [Scenario 3: Unauthorized Access in EHR System]
  - (Add links or QR codes here)

Co-funded by
the European Union

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.