MANUALE ESCAPE

FORMAZIONE DOCENTI

Co-funded by the European Union

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

Partner

INSTITUTO DE EDUCACION SECUNDARIA
JAVIERGARCIATELLEZ

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

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

Co-funded by
the European Union

Questo progetto è stato cofinanziato con il sostegno della Commissione europea. La presente pubblicazione [comunicazione] riflette esclusivamente il punto di vista dell'autore e la Commissione non può essere ritenuta responsabile per qualsiasi uso possa essere fatto delle informazioni in essa contenute.

Indice

Co-funded by
the European Union

SINTESI DEI CONTENUTI

SCOPO: una guida pratica per i docenti su come organizzare o adattare Escape Room a tema sicurezza informatica nella formazione sanitaria.

1. Introduzione
– Il ruolo della sicurezza informatica nella formazione sanitaria
– Perché le Escape Room sono strumenti di apprendimento efficaci
– Panoramica degli scenari e dei materiali digitali disponibili

2. Obiettivi di apprendimento
– Conoscenze, competenze e atteggiamenti sviluppati dall'attività
– Collegamento con le competenze in ambito sanitario (es. sicurezza del paziente, protezione dei dati, lavoro di squadra)
– Come valutare il successo dell'attività e l'apprendimento

3. Progettazione dell'Escape Room
– Selezione e allineamento delle trame, in base agli storyboard
– Collegamento tra gli enigmi e i problemi reali di sicurezza informatica
– Suggerimenti su tempi, risorse e possibili adattamenti

4. Il ruolo del docente
– Checklist di preparazione
– Durante la sessione: facilitatore, osservatore, guida
– Gestione delle dinamiche di gruppo

5. Esperienza degli studenti
– Età/livello di competenza (studenti o professionisti)
– Come garantire inclusione e coinvolgimento

6. Organizzazione pratica
– Logistica, preparazione dell'aula e sicurezza
– Come gestire problemi tecnici o scarsità di risorse

7. Debriefing e riflessione
– Come condurre la riflessione finale
– Esempi di domande per il confronto dopo la sessione

8. Adattamento delle Escape Room
– Regolazione del livello di difficoltà
– Adattamento per sessioni online o ibride

Appendice
– Spazio dedicato a risorse didattiche ed esercizi digitali
– Elenco completo dei video, con link o codici QR

1. Introduzione

Il ruolo della sicurezza informatica nella formazione sanitaria
La sicurezza informatica è un tema sempre più rilevante nel settore sanitario, dove le violazioni dei dati e le vulnerabilità dei sistemi possono incidere direttamente sulla sicurezza del paziente. I docenti devono preparare gli studenti a riconoscere e affrontare le minacce digitali nei contesti clinici.

Perché le Escape Room sono strumenti di apprendimento efficaci

Le Escape Room offrono esperienze di apprendimento immersive basate sulla risoluzione di problemi. Favoriscono la collaborazione, il pensiero critico e la capacità di prendere decisioni in tempo reale: competenze essenziali sia nella sicurezza informatica sia nell'assistenza sanitaria.

Panoramica degli scenari e dei materiali digitali disponibili

Questo manuale fa riferimento a una serie di scenari video e materiali didattici digitali (vedi "Appendice"). Queste risorse fungono da supporto didattico e possono essere integrate nella progettazione della vostra Escape Room.

2. Obiettivi di apprendimento

Conoscenze, competenze e atteggiamenti sviluppati dall'attività

I partecipanti acquisiranno la capacità di:

- *comprendere i principi di base della sicurezza informatica, come phishing, igiene delle password e protezione dei dati;*
- *mettere in pratica il lavoro di squadra e strategie di comunicazione sotto pressione;*
- *sviluppare consapevolezza etica e senso di responsabilità nei contesti di sanità digitale.*

Collegamento con le competenze in ambito sanitario

(es. sicurezza del paziente, protezione dei dati, lavoro di squadra)

Le attività sono collegate a competenze quali:

- *sicurezza del paziente;*
- *protezione dei dati e della privacy;*
- *collaborazione interprofessionale;*
- *processo decisionale clinico in condizioni di incertezza.*

Come valutare il successo dell'attività e l'apprendimento

Utilizzare rubriche di valutazione, checklist osservative e riflessioni finali dopo la sessione per valutare:

- *le strategie di risoluzione dei problemi;*
- *l'efficacia della comunicazione;*
- *il livello di consapevolezza sulla sicurezza informatica.*

3. Progettazione dell'Escape Room

Selezione e allineamento delle storie

Utilizzate gli storyboard per scegliere gli scenari che rappresentano sfide reali di sicurezza informatica in ambito sanitario, ad esempio l'accesso non autorizzato ai dati dei pazienti o un attacco ransomware in ospedale.

Collegamento tra gli enigmi e i problemi reali di sicurezza informatica

Progettate enigmi che simulino:

- *l'identificazione di email di phishing;*
- *la creazione e la valutazione di password sicure;*
- *il tracciamento di accessi non autorizzati nei registri di sistema.*

Suggerimenti su tempi, risorse e possibili adattamenti

Durata consigliata: 45–60 minuti
Materiali: indizi stampabili, interfacce digitali e materiali di scena
Suggerimenti: prevedere una certa flessibilità, tenendo conto della dimensione del gruppo, della disponibilità di tecnologia e del livello di apprendimento.

4. Il ruolo del docente

Checklist di preparazione

- *Rivedete lo scenario e gli obiettivi di apprendimento.*
- *Preparate i materiali necessari e la configurazione tecnologica.*
- *Informate i partecipanti sulle regole e sugli obiettivi della sessione.*

Durante la sessione

Il docente può assumere tre funzioni principali:
Facilitatore: guida il gruppo senza fornire direttamente le risposte.
Osservatore: annota le dinamiche di gruppo e le modalità di risoluzione dei problemi.
Guida: offre suggerimenti quando il gruppo incontra difficoltà.

Gestione delle dinamiche di gruppo

Promuovete una partecipazione inclusiva, alternate i ruoli di leadership e monitorate eventuali comportamenti dominanti o situazioni di scarso coinvolgimento.

5. Esperienza degli studenti

Età / livello di competenza

L'attività può essere adattata a:

- *studenti delle discipline sanitarie;*
- *percorsi di formazione continua per professionisti;*
- *gruppi interdisciplinari.*

Come garantire inclusione e coinvolgimento

- *Utilizzate scenari diversificati.*
- *Offrite più modalità di risoluzione degli enigmi.*
- *Stimolate la riflessione su dilemmi etici.*

6. Organizzazione pratica

Logistica, preparazione dell'aula e sicurezza

- *Utilizzate aule di lavoro o spazi fisici con confini ben definiti.*
- *Assicurate l'affidabilità della tecnologia disponibile, inclusi dispositivi e connessione Wi-Fi.*
- *Fornite indicazioni di sicurezza per l'uso degli elementi fisici presenti nella sessione.*

Come gestire problemi tecnici o scarsità di risorse

- *Prevedete alternative cartacee o enigmi di riserva.*
- *Se i dispositivi non funzionano, utilizzate codici QR o schermate stampate.*

7. Debriefing e riflessione

Come condurre la riflessione finale

Guidate un momento di confronto strutturato, ad esempio attraverso queste domande:

- *Che cosa ha funzionato bene?*
- *Quali concetti di sicurezza informatica abbiamo applicato?*
- *In che modo questa esperienza si collega alla pratica sanitaria reale?*

Esempi di domande per il confronto dopo la sessione

- *"Quali rischi ha individuato il vostro gruppo?"*
- *"Come avete deciso chi avrebbe assunto il ruolo di leader?"*
- *"Che cosa fareste in modo diverso in un contesto clinico reale?"*

8. Adattamento delle Escape Room

Regolazione del livello di difficoltà

- *Aggiungete o rimuovete enigmi.*
- *Modificate i limiti di tempo.*
- *Introducete distrazioni o dilemmi etici.*

Adattamento per sessioni online o ibride

- *Utilizzate piattaforme per il lavoro collaborativo, come Zoom o Microsoft Teams.*
- *Condividete enigmi tramite documenti condivisi o chat private.*
- *Integrate scenari video come risorse collegate.*

Appendice

Risorse didattiche digitali

- *(da aggiungere)*

Elenco degli scenari video

- *(con link o codici QR)*
- *[Scenario 1: Violazione dei dati nel reparto di radiologia]*
- *[Scenario 2: Attacco di phishing rivolto al personale infermieristico]*
- *[Scenario 3: Accesso non autorizzato al sistema di cartelle cliniche elettroniche (CCE)]*
- *(Aggiungere qui link o codici QR)*

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

Questo progetto è stato cofinanziato con il sostegno della Commissione europea. La presente pubblicazione [comunicazione] riflette esclusivamente il punto di vista dell'autore e la Commissione non può essere ritenuta responsabile per qualsiasi uso possa essere fatto delle informazioni in essa contenute.