HANDBOEK ESCAPE

LERAREN

Co-funded by
the European Union

ESCAPE. Zorgprofessionals voorbereiden op cyberaanvallen.
Projectnummer 2023-1-ES01-KA220-VET-000151536

Socios

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

Co-funded by the European Union

Este proyecto ha sido co-financiado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable de ningún uso que pueda hacerse de la información contenida en la misma.

Inhoudsopgave

Co-funded by
the European Union

SAMENVATTING VAN DE INHOUD

DOEL: Een praktische handleiding voor docenten over hoe ze escape rooms met een cybersecuritythema kunnen organiseren of aanpassen voor trainingen in de gezondheidszorg.

Escape Rooms over cyberbeveiliging in trainingen voor de gezondheidszorg

Praktisch handboek voor docenten

1. Inleiding

De rol van cyberbeveiliging in de opleiding van zorgprofessionals

Cyberbeveiliging is een steeds belangrijker thema in de gezondheidszorg, waar datalekken en systeemlekken de patiëntveiligheid direct in gevaar kunnen brengen. Docenten moeten studenten voorbereiden op het herkennen en reageren op digitale bedreigingen in klinische omgevingen.

Waarom escape rooms effectieve leermiddelen zijn

Escape rooms bieden meeslepende, probleemoplossende leerervaringen. Ze bevorderen samenwerking, kritisch denken en realtime besluitvorming – essentiële vaardigheden in cybersecurity en de gezondheidszorg.

Overzicht van beschikbare digitale scenario's en materialen

Deze handleiding verwijst naar een reeks videoscenario's en digitaal lesmateriaal (zie "bijlage"). Deze hulpmiddelen dienen als lesmateriaal en kunnen worden geïntegreerd in het ontwerp van uw Escape Room.

Co-funded by
the European Union

2. Leerdoelen

Kennis, vaardigheden en houdingen ontwikkeld door de activiteit.

Deelnemers ontvangen:
Begrijp de basisprincipes van cyberbeveiliging (bijv. phishing, "wachtwoordhygiëne", gegevensbescherming).
Oefen teamwerk en communicatiestrategieën onder druk.
Het ontwikkelen van ethisch bewustzijn en verantwoordelijkheid in digitale gezondheidszorgcontexten.

Relatie met competenties in de gezondheidszorg (bijv. patiëntveiligheid, gegevensbescherming, teamwork)

De activiteiten sluiten aan op vaardigheden zoals:
Patiëntveiligheid
Gegevensbescherming en privacy
Interprofessionele samenwerking
Klinische besluitvorming onder onzekerheid

Hoe meten we succes en leerresultaten?

Gebruik beoordelingscriteria, checklists, observatie en nabesprekingen na de wedstrijd om het volgende te evalueren:
Probleemoplossingsstrategieën
De effectiviteit van communicatie
Bewustzijn van cyberbeveiliging

Co-funded by the European Union

3. Ontwerp van een escape room

Selectie en uitlijning van kaders

Gebruik je storyboards om scenario's te kiezen die realistische cybersecurity-uitdagingen in de gezondheidszorgsector weergeven (bijvoorbeeld ongeautoriseerde toegang tot patiëntendossiers of een ransomware-aanval in een ziekenhuis).

Verband tussen puzzels en cyberbeveiligingskwesties

Ontwerp puzzels die het volgende simuleren:
Phishing-e-mails (identiteitsdiefstal) herkennen
Het creëren en evalueren van veilige wachtwoorden
Logboeken voor ongeautoriseerde toegang bijhouden

Advies over timing, middelen en aanpassingen.

Aanbevolen duur: 45-60 minuten
Materialen: printbare tracks, digitale interfaces en rekwisieten.
Tips: Zorg voor enige flexibiliteit, rekening houdend met de groepsgrootte, de beschikbaarheid van technologie en het leerniveau.

Co-funded by
the European Union

4. De rol van de leraar

Kennis, vaardigheden en houdingen ontwikkeld door de gereedheidschecklist

Bekijk het scenario en de leerdoelen.
Zorg voor de benodigde materiële middelen en de technologische infrastructuur.
Informeer de leerlingen over de regels en doelstellingen.

Tijdens de wedstrijd

Optreden als:
Begeleider: als gids, zonder de antwoorden te geven.
Observator: Let op de groepsdynamiek en het probleemoplossingsproces.

- *Handleiding: Geef hints als de groep vastloopt.*

Groepsdynamiekmanagement

Bevorder inclusieve participatie, laat leidinggevende rollen rouleren en houd potentiële dominante of juist afstandelijke gedragingen in de gaten.

5. Studentenervaring

Leeftijd/vaardigheidsniveau

Geschikt voor:
Studenten gezondheidswetenschappen
Bijscholing voor professionals
Interdisciplinaire teams

- *Garandeer inclusie en participatie.*

Gebruik diverse scenario's
Bied meerdere perspectieven aan voor het oplossen van de puzzels.
Stimuleer reflectie op ethische dilemma's.

Co-funded by
the European Union

6. Praktische configuratie

Logistiek, voorbereiding van de lessen en beveiliging

Gebruik werkruimtes of fysieke ruimtes met duidelijk afgebakende grenzen.

- *Zorg voor technologische betrouwbaarheid (apparaten, wifi).*

Geef veiligheidsinstructies voor de fysieke objecten.

Technische problemen oplossen met beperkte middelen.

Zorg voor papieren of puzzelachtige back-upalternatieven. Als de apparaten niet werken, gebruik dan QR-codes of afgedrukte schermafbeeldingen.

Co-funded by
the European Union

7. Verslag en reflectie

Hoe stuur je reflectie?

- *Faciliteer een gestructureerde sessie voor het delen van ervaringen:*

Wat heeft gewerkt?
Welke cybersecurityconcepten hebben we toegepast?
Hoe verhoudt dit zich tot de daadwerkelijke zorgpraktijk?

Voorbeeldvragen voor verdere reflectie

- *"Welke risico's heeft uw team geïdentificeerd?"*

"Hoe hebben ze besloten wie de leider zou worden?"
"Wat zou u anders doen in een echte klinische situatie?"

Co-funded by
the European Union

8. Adaptaties van escape rooms

Aanpassing van de moeilijkheidsgraad

Puzzels toevoegen of verwijderen
De tijdslimieten aanpassen
Introduceer afleidingen of ethische dilemma's.

Aanpassing voor online of hybride sessies

Gebruik samenwerkingsplatformen (bijvoorbeeld Zoom, Microsoft Teams).
Deel puzzels via gedeelde documenten of privéchatrooms.
Voeg videoscenario's toe als gekoppelde bronnen.

Co-funded by
the European Union

Bijlage

Digitale lesmaterialen (worden nog toegevoegd)
Lijst met videoscenario's (met links of QR-codes)
[Scenario 1: Gegevenslekken in de radiologie]
[Scenario 2: Phishingaanval op verplegend personeel]
[Scenario 3: Ongeautoriseerde toegang tot het elektronisch patiëntendossier (EPD)-systeem]
(Voeg hier links of QR-codes toe)

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

Este proyecto ha sido co-financiado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable de ningún uso que pueda hacerse de la información contenida en la misma.