ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach

ESCAPE: Preparing healthcare professionals for cyberattacks	
Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach	
Language	*English*

Co-funded by
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach	
Language	*English*

Table of contents

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach	
Language	*English*

1. Name of the material and description

This is a master's thesis by Iris Rieff (2018) that proposes a structured framework for integrating gamification into existing cyber security awareness training programs. The work includes a conceptual model and a real-world case study comparing the original training and its gamified version, measuring participant perceptions through pre- and post-training evaluations. Most respondents rated the gamified training as more engaging and effective.

2. Classification

Category	**Mark if applies**
Sector	□ Healthcare *(all materials focusing specifically on the healthcare sector)*
	□ General public *(materials targeting citizens but that are considered useful and relevant for working with the students and for the professionals, these tend to be more generic materials not targeting a specific sector)*
	□ Other *(other materials considered relevant event though targeting a specific sector, for instance a company, but that are considered relevant for learning about cybersecurity and data protection)*
Topics covered	☑ Cybersecurity
	□ Data protection
Situation type	☑ Prevention
	□ Impact (i.e. when it is occurring or has occurred) on patient care. *(e.g. direct treatments, medicine distribution, etc.)*
	□ Impact on all other activities not involving direct patient care. *(e.g. recording data, lab tests, etc.)*

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach	
Language	*English*

Language of the original materials	□ Dutch
	☑ English
	□ German
	□ Italian
	□ Spanish
Type of the material	□ Guidelines or manuals
	□ Case or examples
	☑ Training courses
	□ Others

3. Description

This is a framework-based training enhancement resource designed to gamify existing cybersecurity awareness programs by embedding game mechanics to boost engagement and perceived effectiveness.

3.1. Origin

- ***Author:*** *Iris Rieff, Delft University of Technology (2018)*
- ***Material Type:*** *Master's thesis presenting a gamification framework and an empirical case study*

3.2. Why is it relevant/important for ESCAPE

- *Provides a **structured methodology**—broken into three phases (Fundamentals, Blueprint, and Design)—for systematically incorporating gamification into security awareness training.*

- *Anchored in theory (design-science research, gamification principles, cybersecurity awareness constructs) and validated through expert input and user trials.*

- *Demonstrates measurable improvements in aspects like **interaction**, **participation**, and **actions** through controlled comparison with non-gamified training*

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach	
Language	*English*

3.3. Lessons learned

Training courses:

- ***Introduction:*** *Offers a repeatable, research-grounded method to gamify cybersecurity awareness content methodically.*
- ***Target group:*** *Organizational training designers, HR and cybersecurity teams responsible for employee training.*
- ***Risks addressed:*** *Low engagement, training fatigue, poor retention and behavior change due to traditional, non-interactive formats.*
- ***Solutions proposed:*** *Embed game design elements (e.g., progression, feedback loops, cooperation/competition, surprises) into existing trainings via a phased model—Fundamentals, Blueprint, Design—supported by empirical validation.*
- ***Tips & tricks for implementation:***
    - ***Conduct expert reviews.*** *Use interviews to refine the framework.*
    - ***Run pre/post assessments.*** *Measure awareness constructs (knowledge, skills, attitude, actions, participation, interaction) to evaluate impact.*
    - ***Be adaptable in deployment.*** *The model works for both digital and tabletop formats; be conscious of context differences.*
    - ***Manage expectations.*** *Some participants may expect a full-fledged gamified environment; clearly set scope and medium (paper vs. digital).*

4. Direct link to the material

https://thesai.org/Downloads/Volume9No9/Paper_32-A_Serious_Game_for_Healthcare_Industry.pdf

5. Other resources (optional)

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

- ***Design-Science in Gamification:*** *Insights drawn from Werbach & Hunter’s 6D model and design-science research methods adapted for gamifying cybersecurity training SciSpace.*
- ***SETA Frameworks & Gamification in Practice:*** *Related works include organizational security training design (e.g., Scrimgeour & Ophoff, 2019) and empirical applications in awareness gamification.*

Co-funded by
the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.