ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

The use of gamification on cybersecurity awareness of healthcare professionals

ESCAPE: Preparing healthcare professionals for cyberattacks	
The use of gamification on cybersecurity awareness of healthcare professionals	
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.

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	
The use of gamification on cybersecurity awareness of healthcare professionals	
Language	*English*

1. Name of the material and description

*The material titled **"The use of gamification on cybersecurity awareness of healthcare professionals"** is a scientific article that explores how gamification can be applied to improve cybersecurity awareness among healthcare workers. It highlights the growing cybersecurity threats in the healthcare sector—especially due to human error—and argues that traditional training methods are often ineffective. The paper reviews existing gamified training tools and concludes that a tailored gamified approach for healthcare settings could significantly enhance staff engagement, knowledge retention, and overall cyber resilience.*

2. Classification

Category	**Mark if applies**
Sector	☑ Healthcare
	☐ 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.)*

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.

	☑ Impact on all other activities not involving direct patient care. *(e.g. recording data, lab tests, etc.)*
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

Short description of the materials, which covers the following topics:

3.1. Origin

This scientific paper was developed by researchers from the Lisbon School of Health Technology, Health and Technology Research Center, Polytechnic of Leiria, and INESC-TEC in Portugal. It is published by Elsevier within Procedia Computer Science, a peer-reviewed academic journal that presents research presented at international conferences, in this case, CENTERIS / ProjMAN / HCist 2023. The publishing entities are higher education and research institutions focusing on healthcare and technology innovation.

3.2. Why is it relevant/important for ESCAPE

The material is directly relevant to the ESCAPE project as it raises awareness on cybersecurity among healthcare professionals, highlighting specific vulnerabilities of the healthcare sector—especially human error—as a leading cause of cyber incidents, and presents gamification as an innovative, more engaging

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.

alternative to traditional training. It addresses the critical challenge ESCAPE focuses on: how to educate busy, multidisciplinary healthcare staff on cybersecurity in a motivating and effective way.

3.3. Lessons learned

Lessons Learned

Guidelines or Manuals

The objective of the material is to evaluate the effectiveness of gamified training programs for improving cybersecurity awareness in the healthcare sector, and to propose a strategy tailored to healthcare professionals' realities.

The target group is Healthcare professionals including doctors, nurses, administrative staff, and other non-IT personnel in medical institutions.

Short description of the risks addressed:

- *Phishing and ransomware attacks*
- *Loss or theft of devices containing sensitive data*
- *Insider threats (accidental or intentional)*
- *Attacks on connected medical devices (IoMT)*

These risks can severely disrupt medical workflows, compromise patient safety, and cause financial and reputational damage.

Solutions or contingency measures proposed:

- *Gamified cybersecurity training as an effective tool to improve awareness and behavior*
- *Customized content based on healthcare-specific risks and user profiles*
- *Integration of national cybersecurity frameworks (e.g., Portugal's CNCS competency model)*
- *Inclusion of simulation-based learning (phishing scenarios, data protection challenges)*

Tips & tricks for implementation:

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.

- *Modular and flexible learning formats, so busy staff can train at their own pace*
- *Include visuals, rewards, and interactive content to increase engagement*
- *Align training content with real-world healthcare situations and systems*
- *Regular updates and repetition to combat knowledge decay over time*
- *Monitor incident reports before and after training to measure impact*

4. Direct link to the material

https://www.sciencedirect.com/science/article/pii/S1877050924014455

5. Other resources (optional)

No other sources

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.