ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles for learners

Warning! Detection of cyber security threats. - Game

ESCAPE: Preparing healthcare professionals for cyberattacks	
Warning! Detection of cyber security threats. - Game	
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	
Warning! Detection of cyber security threats. - Game	
Language	*English*

Table of contents

1. Name of the material and description..... 3
2. Classification..... 3
3. Description..... 4
4. More information..... 4

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	
Warning! Detection of cyber security threats. - Game	
Language	*English*

1. Name of the material and description

This quiz is designed for social care staff to test their awareness of cyber threats in healthcare and care home environments. It focuses on data protection, safe use of technology, and identifying phishing attempts in daily work.

2. Classification

*Mark with an X **all** the items that apply to the materials. These are the criteria to be used for the filtering of materials on the website.*

Category	Mark if applies
Sector	☐ Healthcare (*all materials focusing specifically on the healthcare sector)*
	☑ General *(not directly related to healthcare)*
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.)*
Language of the original materials	☐ Dutch
	☑ English
	☐ German
	☐ Italian

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	
Warning! Detection of cyber security threats. - Game	
Language	*English*

	☐ Spanish
Type of the material	☑ Quiz questions *(independent if these are test or more formal education, or informal Q&A activities such as Kahoot or Quizzizz)*
	☐ Games *(including role playing)*
	☐ Applications & interactive videos
	☐ Checklists

3. Description

1. A pop-up says *"Your system is infected! Download cleaner now!"*. What's the safest action?

   a) Download the cleaner immediately

   b) Close the browser and run your antivirus

   c) Restart your computer and ignore

   d) Click the ad just to check

   Right Answer: b) Close the browser and run your antivirus
   Feedback: Fake pop-ups are traps—trust only official security software.

2. You receive a prize link from a stranger on social media. What's the biggest warning sign?

   a) Spelling errors in the message

   b) Request for personal info

   c) Unknown sender

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.

d) All of the above

Right Answer: d) All of the above
Feedback: Fake links often have multiple red flags.

3. You're about to log in to your bank on public Wi-Fi. What's the danger?

a) It's too slow

b) Hackers may steal your credentials

c) The café owner might ban you

d) Your battery will drain faster

Right Answer: b) Hackers may steal your credentials
Feedback: Avoid sensitive logins on public Wi-Fi without a VPN.

4. A flashlight app asks for contact list and microphone access. What do you do?

a) Allow access to use it fully

b) Deny permissions and uninstall

c) Restart and ignore

d) Share the app with friends

Right Answer: b) Deny permissions and uninstall
Feedback: Extra permissions may signal spyware.

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.

5. Which is the strongest password?

   a) Summer2025

   b) P@ssword123

   c) 7r$Qm!z4Gv#pL

   d) MyBirthday1990

   Right Answer: c) 7r$Qm!z4Gv#pL
   Feedback: Random, long, mixed characters = strongest defense.

4. More information

- Source: Hacktale Cybersecurity Game

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.