ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles for learners

How much do you know about general cybersecurity?

ESCAPE: Preparing healthcare professionals for cyberattacks	
How much do you know about general cybersecurity?	
Language	English

Table of contents

1) How much do you know about general cybersecurity?.....3
2) Classification.....3
3) Quiz questions..... 4
6) More information.....6

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	
How much do you know about general cybersecurity?	
Language	English

1) How much do you know about general cybersecurity?

This puzzle consists of 5 questions related to different attacks you can have in your healthcare entity. Choose wisely in order to properly protect your valuable data from cybercriminals.

2) Classification

Category	**Mark if applies**
Sector	☑ Healthcare
	☐ General
Topics covered	☑ Cybersecurity
	☑ Data protection
Situation type	☑ Prevention
	☐ Impact (i.e. when it is occurring or has occurred) on patient care.
	☑ Impact on all other activities not involving direct patient care.
Language of the original materials	☐ Dutch
	☑ English
	☐ German
	☐ Italian
	☐ Spanish
Type of the material	☑ Quiz questions
	☐ Games

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	
How much do you know about general cybersecurity?	
Language	English

	☐ Applications & interactive videos
	☐ Checklists

3) Quiz questions

1) Which of the following activities is not safe while surfing on the web with your working computer at the hospital?
    a) Verify the authenticity of links before clicking on them.
    b) Shop on official sites.
    c) Download apps from official stores.
    d) Download programs or files from unknown links or sources.

Right answer: Download programs or files from unknown links or sources.

Feedback: Though none of the options are recommended while working, the correct option is 4 because downloads from unknown links or sources can contain malware, ransomware, or unauthorized software that compromises the hospital network and patient data confidentiality. Verifying link authenticity and using official sources reduce risks and protect information integrity.

2) How would you create a secure password?
    a) Generating a long password (more than 14 characters).
    b) Using a different password on each online platform.
    c) Not sharing it with anyone.
    d) Restoring the backups onto new drives and resuming work.
    e) All options apply.

Right answer: All options apply.

Feedback: A secure password should be long (over 14 characters), unique per platform, not shared with anyone, and include a mix of upper and lower case letters, numbers, and symbols. Each element reduces the likelihood of guess-based or credential-stuffing attacks and helps protect patient data and hospital systems.

3) If I receive a message with a link, which of the following are correct?
    a) I copy the link and run it through a URL analyzer.
    b) I check if the link text matches the official website.
    c) All of them are correct.
    d) I click the link to see where it goes.

Right answer: All of them are correct.

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.

Feedback: All the listed steps are prudent: analyzing the URL can reveal malicious or spoofed domains, verifying link text helps detect spoofing, and neither clicking unknown links nor bypassing checks is advisable. Combined, these practices reduce phishing risk and protect patient data and hospital systems.

4) Point out the statement that seems correct to you:
    a) An antivirus is only useful on old devices and systems.
    b) Along with the antivirus, updates are necessary.
    c) Antivirus software only detects vulnerabilities.
    d) The antivirus detects all viruses and removes them automatically.

Right answer: Along with the antivirus, updates are necessary.

Feedback: Antivirus software requires periodic updates of signatures and heuristics to recognize new threats. No antivirus detects “all” viruses or removes everything automatically without intervention; updates also improve detection and incident response. Statement 1 is incorrect (antivirus software is not only useful for old systems) and statement 3 is incorrect (antiviruses do not only detect vulnerabilities; they also detect malware). Statement 4 is incorrect because it does not guarantee detection/removal of all threats and is not always automatic.

5) A pharmacy assistant is learning about cybersecurity threats. Which of the following best describes *ransomware*?
    a) A type of malicious software that secretly collects customers’ personal data for marketing purposes.
    b) A malicious program that encrypts files or systems and demands payment (a ransom) to restore access.
    c) A computer virus that automatically updates the pharmacy’s software without permission.
    d) A scam email that tries to trick the pharmacy staff into sharing passwords.

Right answer: A malicious program that encrypts files or systems and demands payment (a ransom) to restore access.

Feedback: Ransomware is a type of malware that locks or encrypts a victim’s files or systems, making them inaccessible. The attacker then demands money (the ransom) to unlock them.

For example, in a pharmacy, ransomware could encrypt the database containing patients’ prescriptions or medical histories, preventing staff from accessing vital information. This disruption could stop the pharmacy from dispensing medicines until the ransom is paid (or the systems are restored from backups).

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	
How much do you know about general cybersecurity?	
Language	English

6) More information

These questions have been inspired and adapted to the healthcare sector by the scenarios presented by INCIBE in the following web https://www.incibe.es/menores/juegos/cyberscouts. This material is published in Spanish, as INCIBE is a Spanish institution.

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.