ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles for learners

The Weakest Link Part 2

ESCAPE: Preparing healthcare professionals for cyberattacks	
Are you ready to face cyberattacks?	
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	
Are you ready to face cyberattacks?	
Language	English

1. The weakest link – part 2

This puzzle consists of 5 new questions aiming to educate users on workplace security risks in the healthcare sector. The goal is to help users avoid becoming 'the weakest link' in the security chain.

2. Classification

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

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	
Are you ready to face cyberattacks?	
Language	English

	Games
	Applications & interactive videos
	Checklists

3. Quiz questions

It's your first week as a pharmacy assistant in a hospital. You must also learn the pharmacy's cybersecurity practices.

1. You receive your work phone. It isn't locked with a password or biometric security.

What do you do?

A. You manually lock the screen when you're not using it. It's faster without a password.

B. You set a simple code like 1234 to work quickly.

C. You set a strong code or biometric lock in line with hospital policy.

D. You use your personal phone and leave the work phone in your locker.

Right answer: C

Feedback: Work devices should always be protected with strong passwords or biometric access. This prevents unauthorized access if lost or stolen.

2. You receive an email from 'IT Support' asking you to click a link and confirm your password due to 'suspicious activity'.

A. You click the link and enter your details immediately to avoid problems.
B. You reply asking for clarification.
C. You ignore the email because it seems suspicious.
D. You verify the sender and then call the IT department to confirm the email.

Right answer: D

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: Always verify suspicious emails. Don't click links or give credentials. Contact IT directly to check legitimacy.

3. On your break, you use a shared staff computer to browse an online shop. It asks to save your password in the browser.

A. You save the password — it's convenient since you rarely use this computer.

B. You decline and clear your browsing data afterward.

C. You leave the computer unlocked for the next person.

D. You save the password but make sure to log out.

Right answer: B

Feedback: Never save passwords on shared devices. Always log out and erase browsing history to protect your data.

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.

4. A vendor visits the pharmacy to perform maintenance on a computer. He asks to use your login to install software.

A. You enter your login details for him so he can proceed quickly.

B. You log in for him and supervise while he works.

C. You refuse and report the request to IT.

D. You tell him to ask your supervisor.

Right answer: C

Feedback: Never share login credentials or allow third parties to use your account. All external access should go through proper channels and with IT's oversight.

5. You receive a USB stick from a colleague who found it in the hallway. She says it might belong to someone from your department.

A. You plug it into your workstation to see what's on it and identify the owner.

B. You put it aside and ask around later.

C. You turn it in to IT without connecting it to any device.

D. You assume it's trash and throw it away.

Right answer: C

Feedback: Unknown USB devices can contain malware. Never plug them into a work computer. Always report and hand them over to IT.

More information

These questions were inspired by scenarios from the IS Decisions User Security Awareness Game: https://www.isdecisions.com/user-security-awareness-game/

This material is part of the ESCAPE project, aimed at training healthcare professionals to recognize and avoid cybersecurity risks in the workplace.

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.