ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles for learners

Are you ready to face cyberattacks?

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

Table of contents

1) Are you ready to face cyberattacks?..... 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	
Are you ready to face cyberattacks?	
Language	English

1) Are you ready to face cyberattacks?

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	
Are you ready to face cyberattacks?	
Language	English

	☐ Applications & interactive videos
	☐ Checklists

3) Quiz questions

1) You are in charge of the management of a private dental clinic. One employee clicked in an attached document, allegedly sent by a client, and the computer was immediately blocked with a pop-up message that urge to pay money to restore their access and data. In the case of a ransomware attack to your clinic, which of the following measurements are not recommended to prevent or alleviate it?
    a) Change all passwords, including the website admin password and the Wi-Fi password, as a precaution.
    b) Click on the email attachment by accessing it from another computer not connected to the network.
    c) Remove the infected drives to disinfect them and see if the data can be recovered.
    d) Restore the backups onto new drives and resume work.

Right answer: Click on the email attachment by accessing it from another computer not connected to the network.

Feedback: Though it may seem convenient, malicious data can be stored in that new computer. You must contact your IT support or official organisms (police, cybersecurity institutions, etc.) to address the best way to solve the problem.

2) One of your laboratory employees received a call urging him to provide web page admin passwords to make critical maintenance of the server. As it seemed trustable, he provided them. As a result, your web page related to your laboratory has been redirected by cybercriminals. It was a phishing attempt where the criminals want to collect username and passwords or bank accounts of your clients by redirecting your web page to their malicious environment. Which of these actions is not useful to mitigate the issue?
    a) Make an encrypted copy (to send to the police along with the report) of the server logs where the cybercriminals' and potential victims' access attempts can be seen.
    b) Request the web hosting provider to take the website offline.
    c) To fire the employee so that it won't' happen again.
    d) Restore the backups onto new drives and resume work.

Right answer: To fire the employee so that it won't happen again.

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

Feedback: The best solution to get well protected in these scenarios is proper education, staff training and learning from mistakes. Firing the employee will not mitigate the issue nor train the remaining employees to avoid these kind of attacks again.

3) You work at a pharmacy as an assistant pharmacist, and you work remotely from home twice a week alongside other staff that, ultimately, have had several substitutions. From one day to another, some patients' clinical data from your pharmacy appeared on the dark web, and local authorities called you to check what was happening. Which of the following options could better explain this data leak?
    a) Forget to remove remote access to the temporary staff at your pharmacy once they finished their work.
    b) Use a secure VPN connection to access patient records while working from home.
    c) Implement strong password policies and two-factor authentication for all staff accounts.
    d) Regularly update and patch all pharmacy systems to fix known security vulnerabilities.

Right answer: Forget to remove remote access to the temporary staff at your pharmacy once they finished their work.

Feedback: Although working from remote has their undeniable advantages, you must ensure your data is well protected to avoid data leaks. One of the measurements is ensuring only authorised staff have access to this special protected data.All the other options, are, indeed, good measures to avoid this data leak.

4) You work as a nurse assistant in a private elderly care clinic and you are in charge of the stock of general medical supplies. After coming back from holidays, you notice several payments to strange providers, and there is no reception of the material nor receipt. Talking to the accountants, there was a message from your boss asking for their credentials in order to proceed with these transfers. While you look at it carefully, the remittent address was fake. ¿Which kind of issue are we facing here?
    a) Cyberattacks.
    b) DDos.
    c) Social engineering.
    d) Software not updated.

Right answer: Social engineering.

Feedback: **Social engineering** is a type of attack technique that relies on psychological manipulation to trick individuals into revealing confidential information, granting unauthorized access, or performing actions that compromise security. Instead of exploiting technical vulnerabilities, social engineering exploits human trust, curiosity, fear, or urgency to bypass security measures.

5) You are in charge of a private hospital network in Barcelona, Spain. You receive a call from the manager of a large corporation who reports that their website has been rendered inoperable by massive volumes of network traffic originating from your company's servers. Investigation reveals an exposed internal DNS service, no perimeter firewall, and that a

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.

malicious actor has likely installed malware to enroll your machines in a remotely controlled botnet which then sends traffic to the victim. What type of attack is described?

a) SQL injection.
b) Man-in-the-middle (MitM) attack.
c) Distributed Denial of Service (DDoS) attack.
d) Ransomware.

Right answer: Distributed Denial of Service (DDoS) attack.

Feedback: The scenario describes many infected hosts (a botnet) being used to send large volumes of traffic to a target, overwhelming its web server and making the site unavailable. That is the definition of a Distributed Denial of Service (DDoS) attack. The exposed DNS service and lack of firewall explain how the attacker was able to compromise internal machines and use them to generate the traffic. Options A, B and D describe different attack types that do not match the mass-traffic, availability-impact, botnet behavior in this scenario.

6) More information

These questions have been inspired and adapted to healthcare sector by the scenarios presented by INCIBE in the following web https://www.incibe.es/empresas/formacion/juego-rol-pyme-seguridad. 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.