ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles for learners

Password Security Quiz for Healthcare Professionals

ESCAPE: Preparing healthcare professionals for cyberattacks	
Password security in healthcare	
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	
Password security in healthcare	
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	
Password security in healthcare	
Language	**English**

1. Password Security Quiz for Healthcare Professionals

This factsheet contains six quiz questions aimed at improving password security among healthcare professionals. It focuses on common risks and practical strategies derived from passwortcheck.ch to enhance secure access to sensitive systems and data.The website also offers a professional password check tool.

2. Classification

Category	Mark if applies
Sector	**X Healthcare**
	General
Topics covered	Cybersecurity
	Data protection
Situation type	**X 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
	X English
	X German
	X 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	
Password security in healthcare	
Language	**English**

	Games
	Applications & interactive videos
	X Checklists

3. Quiz questions

1) You work in a hospital and access several IT systems daily. Which method is recommended to create a strong but memorable password?
    a. A single long word with special characters.
    b. Use a simple password like "Pflege123" that is easy to remember and quick to type.
    c. Use a personal sentence and take the initials, numbers, and capital letters to generate a complex but memorable password.
    d. Use the same password as for your private accounts to avoid confusion.

Right answer: c. Use a personal sentence and take the initials, numbers, and capital letters to generate a complex but memorable password.

Feedback: A memorable phrase (e.g. "Ich arbeite dreimal mit Clara an 5 Montagen ab 9 Uhr") turned into initials (Iadmca5ma9U) generates a complex but memorable password.

2) You see a colleague storing login data on a sticky note next to the screen. What is the safer alternative?
    a. It's not a problem as long as no one else is around. Keeping it visible is fine in such cases.
    b. Store passwords in a secure password manager.
    c. Create a text file for passwords with a non-obvious name on your computer.
    d. If you hide notes under the keyboard, they are less likely to be found and it's a safer alternative.

Right answer: b. Store passwords in a password manager.

Feedback: Storing passwords on sticky notes or in unprotected files poses a significant security risk. Use a secure password manager to store sensitive credentials.

3) You use the same password for your hospital access, private email, and social media. What's the issue?

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.

a. If you forget your password, you'll have a problem on many systems.
b. Reusing passwords increases the risk of multiple breaches.
c. If you use a password manager, it's not a problem.
d. Enabling 2FA is less effective in this case.

Right answer: b. Reusing passwords increases the risk of multiple breaches.

Feedback: Reusing passwords means that one leaked password can compromise several systems, including sensitive health data.

4) You notice that your hospital's web application uses "http://" rather than the secure "https://". Is there a security risk?
   a. No risk as long you use the official site.
   b. There is a risk. Passwords can be transmitted unencrypted.
   c. No risk. Using long passwords is safe enough to keep your data safe, even on HTTP websites.
   d. There is a risk. HTTPS is mainly used for speed, not for security reasons.

Right answer: b. There is a risk. Passwords can be transmitted unencrypted.

Feedback: HTTP lacks encryption. Sensitive data (logins, patient info) should only be entered on HTTPS-secured sites. HTTPS is used for security reasons.

5) Passwords like "123456" or "qwertz" are frequently used. Even in the healthcare sector. Evaluate the use of such passwords.
   a. These are established and particularly good passwords. That's why their frequent use is justified.
   b. Combined, they would make a strong password, since they include both numbers and letters.
   c. They are widely known keyboard sequences. They follow predictable patterns and are included in most password-cracking dictionaries. This is a serious problem.
   d. The main issue is that they do not contain special characters.

Right answer: c They are widely known keyboard sequences. They follow predictable patterns and are included in most password-cracking dictionaries. This is a serious problem.

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: Such passwords are extremely insecure. Their predictability makes them a common target in automated password-cracking tools and they must be avoided entirely, especially in clinical environments.

6) Your clinic enables two-factor authentication (2FA). What should you do?
    a. Use your regular password only, since 2FA is already enabled and provides enough protection.
    b. Enable 2FA wherever possible to add an extra layer of security in addition to a strong password.
    c. Save the password in a plain text file on your desktop so you don't forget it.
    d. Reenter your password multiple times to increase security through repetition.

Correct answer: b Enable 2FA wherever possible to add an extra layer of security in addition to a strong password.

Feedback: 2FA is one of the most effective ways to prevent unauthorized access, especially in healthcare settings.

4. More information

The quiz questions were adapted from the official password guidelines published at www.passwortcheck.ch by the Lucerne University of Applied Sciences and Arts. These guidelines aim to raise awareness about safe password usage for end users, with a special focus on healthcare professionals. The materials are publicly accessible and published in German, French, Italian and English. The website offers a professional password check tool.

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.