# ESCAPE:

## Preparing healthcare professionals for cyberattacks

# Puzzles for learners

How Safe Are You? A Quiz for Healthcare Professionals

| ESCAPE: Preparing healthcare professionals for cyberattacks | |
|---|---|
| How Safe Are You? A Quiz for Healthcare Professionals | |
| **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 | |
|---|---|
| **How Safe Are You? A Quiz for Healthcare Professionals** | |
| **Language** | English |

# 1. How Safe Are You? A Quiz for Healthcare Professionals?

This factsheet presents six quiz questions that introduce key practices for staying secure in healthcare workplaces. The questions are adapted from the online course "Sicherheit am Arbeitsplatz" from the platform secaware.nrw, an awareness project by the Ministry of the Interior of North Rhine-Westphalia.

# 2. Classification

| Category | Mark if applies |
|---|---|
| Sector | Healthcare |
| | **X General** |
| Topics covered | **X Cybersecurity** |
| | Data protection |
| Situation type | Prevention |
| | 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 |
| | English |
| | **X 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 | |
|---|---|
| **How Safe Are You? A Quiz for Healthcare Professionals** | |
| **Language** | English |

| | |
|---|---|
| | Games |
| | Applications & interactive videos |
| | Checklists |

## 3. Quiz Questions

1) You work at the reception desk of a healthcare facility. A person claiming to be an IT technician wants to access your computer without showing any identification. What should you do?

   a. Let them use the computer if they seem trustworthy.

   b. Allow access if they say it's urgent and mention technical issues.

   c. Politely refuse access and report the situation to your supervisor or IT department.

   d. Let them use the PC if they wear work clothes that look official.

**Right answer:** c. Politely refuse access and report the situation to your supervisor or IT department.

**Feedback:** Never allow anyone to access systems without proper identification. Social engineering often relies on urgency and assumed authority to bypass security protocols.

2) You find a USB stick in the staff kitchen. What is the best course of action?
   a. Plug it into your workstation to find the owner.
   b. Give it to your IT department or security officer.
   c. Leave it in a drawer at the nurses' station.
   d. Give it to your IT department or security officer.
   e. Take it home for safekeeping.

**Right answer:** b. Give it to your IT department or security officer.

**Feedback:** Unknown devices can be infected with malware. Always hand them over to designated security personnel.

3) Someone from "technical support" calls and urgently asks for your system login credentials. What should you do?
   a. Provide them since they claim to be IT.
   b. Ask them to send an email first.

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.

c. Refuse and report the incident to your supervisor or IT.
d. Share only part of your password for safety.

**Right answer:** c. Refuse and report the incident to your supervisor or IT.

**Feedback:** Legitimate IT staff never ask for your password. Always verify requests and report suspicious contacts.

4) You receive a suspicious email with an attachment. What is the safest response?
   a. Delete the email or report it via the security channel.
   b. Open it to see if it's relevant to your work.
   c. Forward it to a colleague to ask for advice.
   d. Reply and ask the sender to confirm their identity.

**Right answer:** a. Delete the email or report it via the security channel.

**Feedback:** Suspicious emails should never be opened or forwarded. Use internal reporting tools to alert your IT team.

5) Which of the following habits best supports secure behavior in the healthcare workplace?
   a. Writing down PINs and passwords on a sticky note hidden in your locker.
   b. Logging off your computer when you leave your desk.
   c. Sharing your access badge with colleagues in your team.
   d. Using the same badge for personal and professional facilities.

**Right answer:** b. Logging off your computer when you leave your desk.

**Feedback:** Logging off ensures that no one can access sensitive systems while you're away. All personal credentials must be kept secure.

6) You're unsure if your current working area complies with the latest workplace safety rules. What should you do?
   a. Wait until the next team meeting.
   b. Ask your colleagues informally.
   c. Check your organization's internal guidelines or contact safety personnel.
   d. Assume everything is in order if no one has complained.

**Right answer:** c. Check your organization's internal guidelines or contact safety personnel.

**Feedback:** Workplace safety is a shared responsibility. If you're unsure, seek clarification from official channels.


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 Safe Are You? A Quiz for Healthcare Professionals** | |
| **Language** | English |

## 4. More information

The questions and scenarios are based on the online self-learning module “Sicherheit am Arbeitsplatz” available at https://secaware.nrw/selbstlernakademie. This module was developed as part of the “SecAware” initiative funded by the Ministry of the Interior of North Rhine-Westphalia. The original content targets general workplace security in public institutions.

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.