TEASER

Teacher as Avatar

Teaching and learning scenario

Cybersecurity Basics: Identifying & Preventing Cyber Threats

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Contents

I. Master Data and Context

- **Scenario Title and Abstract:** The scenario is titled **"Cybersecurity Basics: Identifying & Preventing Cyber Threats".** It provides an in-depth introduction to identifying and preventing common digital threats, with a particular focus on **phishing attempts** and **malware**. Learners are first introduced to the theoretical basics by an **AI-generated avatar** before moving on to an interactive problem-solving phase **with ChatGPT**. The aim of this combination is to create an immersive learning environment that sustainably strengthens security awareness through the visual support of the avatar and direct interaction with the AI.
- **Professional field and target group:** The scenario is located in the field of **digital skills, IT basics and raising awareness of cybersecurity**. The primary target group includes **trainees (from the 2nd year of apprenticeship),** VET apprentices (Vocational Education and Training) as well as career starters from various disciplines such as programming, economics or finance. In addition, the material is aimed at **VET teachers and instructors** who want to modernize their pedagogical methods through the use of AI and avatars. The training is designed to be accessible to learners without a deep IT background by allowing complex terms to be explained in real time by AI.
- **Learning objectives:** Competence development in this scenario is divided into three areas:
    - **Knowledge:** Learners acquire the ability to reliably detect **phishing and malware threats** and understand the underlying patterns of common attack strategies. This also includes knowledge of different types of attacks such as spear phishing, whaling or ransomware.
    - **Skills:** You will learn to critically analyze real-world scenarios to **identify suspicious elements** (such as manipulated links or erroneous email addresses). In addition, they train the ability to formulate **specific questions to an AI** in order to eliminate ambiguities in the event of potential attacks.
    - **Competencies:** Trainees are enabled to apply their cybersecurity awareness in **real work contexts** . They can justify their security decisions on the basis of AI-supported insights and develop responsible behavior in the digital space.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

II. Educational Design

- **The "Educational Question":** The central pedagogical challenge of this scenario is that learners – especially those without an in-depth IT background (such as trainees in business or finance) – often struggle to identify **subtle digital threats** and understand the necessary technical vocabulary. The scenario addresses the question: **How can the understanding of complex cybersecurity concepts and acronyms be improved through an interactive, secure learning environment?**. The use of AI and avatars solves this problem by providing **consistent and engaged knowledge transfer**, allowing for safe simulation of attack scenarios, and reducing the cognitive burden of guided interactions.
- **Didactic setting:** The scenario is firmly anchored in the European competence frameworks **DigComp 2.2** and **DigCompEdu**, especially in the areas of information literacy, security and problem solving. In the context of the **SAMR model,** the learning unit reaches the level of **"modification" (redesign),** as the task (the analysis of attacks using real-time AI feedback) would not be possible in the same depth without this technology. The chosen teaching method follows a **structured 4-phase model**:
    1. **Orientation:** Theoretical input through a linear avatar.
    2. **Delivery:** Active, exploratory learning where learners act as **"digital detectives"** and investigate real-world cases (phishing emails, malware pop-ups).
    3. **Assessment:** Problem-solving tasks with direct AI feedback.
    4. **Conclusion:** Collaborative reflection in the group on the limits and possibilities of AI support.
- **Role of the trainer/teacher:** In this scenario, the role of the teacher changes fundamentally from the sole knowledge imparter to **the facilitator, coach and pedagogical advisor**. Specific tasks include:
    - **Introduction and setting: Introduction of** the topic and explanation of the role of the avatar.
    - **AI interaction support:** Supporting learners in formulating targeted questions (**prompt engineering**) to ChatGPT.
    - **Quality assurance:** Conducting **plausibility checks** to ensure that learners critically question AI-generated information and do not adopt misinterpretations (hallucinations).
    - **Feedback provider:** Moderation of the final discussion and linking of virtual experiences with real work practice.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

III. Technological implementation

- **AI and avatar solution:** In this scenario, **2D or 3D AI-generated avatars** are used, which mainly convey **linear instructional content** in the form of video tutorials. The avatar acts as **a dedicated visual guide and tutor** in the learning process: it introduces the theoretical concepts of cybersecurity, explains technical terms and vividly demonstrates examples of phishing emails or malware attacks. In addition, **ChatGPT takes on** the function of an **interactive interlocutor and "digital detective"** with whom learners can enter into an active dialogue to analyze specific threat scenarios in real time.
- **Technical tools:** A selection of modern "low-threshold" tools and standard hardware is used to realize the scenario:
    - **Avatar generation: Synthesia** or **HeyGen** are used to quickly create the talking avatars from scripts.
    - **Interactive AI: ChatGPT** (based on GPT-4) is used for scenario analysis, answering participant questions, and assisting in the "troubleshooting" of security incidents.
    - **Learning platform (LMS):** The courses are provided via **Learnpress**, which brings together the interactive elements and videos in a structured way.
    - **Hardware:** Learners use standard **laptops or PCs** with stable internet connections.
    - **Additional resources:** Use of **YouTube** to host the avatar videos as well as digital notebooks to save results.
- **Software hopping approach:** Content creation follows a **low-threshold "software hopping approach"** that combines the strengths of different applications without the need for coding. The process is divided into the following steps:

1. **Text optimization:** Raw technical manuscripts of the trainers are linguistically refined with **ChatGPT** and converted into a didactically appealing script.

2. **Image and video production:** The optimized texts are loaded into **Synthesia** to render lip-sync videos with a chosen avatar character.

3. **Interactive dovetailing:** The finished videos are integrated into the LMS and linked to specific **prompts for ChatGPT** . For example, learners can switch to an AI-powered case study immediately after an avatar explanation to apply what they have learned in practice.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

IV. Detailed Lesson Plan

The delivery of this unit is designed to put learners in the role of **"cybersecurity investigators".** The process is divided into the following four phases:

1. Introduction and orientation

- **Duration:** 4 minutes.
- **Content:** Basic introduction to cybersecurity concepts as well as how to identify the two most common threats: **phishing** and **malware**.
- **Activities:**
    - Learners watch a tutorial video in which an **AI-generated avatar** (created with Synthesia) explains the importance of network protection and highlights the dangers of online scams.
    - The trainer (moderator) introduces the session, explains the **role of the avatar** as a digital tutor and is available for initial comprehension questions.
- **Media:** Avatar videos, created using **Synthesia** or **HeyGen**.

2. Execution of the task

- **Duration:** Flexible (part of the active development phase).
- **Contents:** Practical analysis of real-world attack scenarios to identify vulnerabilities.
- **Activities:**
    - Learners conduct an **interactive investigation using ChatGPT**. You'll get specific case studies, such as a fake **Netflix payment request** ("support@netflix-pay.com") or a rigged **"Antivirus Defender 3000"** pop-up alert.
    - The task is to ask ChatGPT targeted questions (e.g., "I saw a pop-up claiming my PC is infected – is that malware?") to verify the threat.
    - The instructor assists learners with **prompt engineering** and monitors discussions about the features found, such as suspicious URLs or grammatical errors.
- **Media: ChatGPT** as an interactive assistant, online notes.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

3. Evaluation / Review

- **Duration:** 8 minutes.
- **Contents:** Application of the acquired knowledge to a complex, real situation and verbal justification of safety decisions.
- **Activities:**
    - **CEO scenario:** An avatar triggers a task where learners receive an urgent text message from the "CEO" asking them to make a quick money transfer.
    - Learners must identify the discrepancies (e.g., a slightly different email address such as "CEO@yourcornpay.com"), ask ChatGPT for advice, and **verbally justify their actions to the instructor**.
    - Optionally, an internal knowledge check can be started by entering the **"test" command in the chat** to complete a short quiz with immediate feedback.

4. Completion of the session

- **Duration:** 8 minutes.
- **Contents:** Summary of the most important findings and reflection on the learning process.
- **Activities:**
    - In a moderated **group discussion**, participants will reflect on the effectiveness of AI support and the limitations of the technology.
    - It consolidates day-to-day protection strategies, such as enabling two-factor authentication or reporting suspicious messages to the IT team.
    - The transfer into practice is completed by discussing human vigilance as the "best defense."

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

V. Resources and collateral

1. Videos

The knowledge transfer is based on **AI avatar videos**. These not only contain technical information, but also use memorable **analogies** to clarify the concepts.

- **Phase 1: Mastering Cybersecurity – Spotting Phishing & Malware**
    - *Key message:* Define cybersecurity as a practice to protect systems, networks, and data.
    - *Content:* Introduction to **phishing** (fraudulent attempts to steal sensitive information) and **malware** (malicious software that damages systems).
    - *Security rules:* Warning against opening attachments from suspicious sources, using up-to-date antivirus software, and regular backups.
    - *Analogy:* "Think of your computer as a **fortress**. Phishing is like a spy who calls the guard post and pretends to be a general to open the gate. Malware is like a **wooden horse** that infiltrates soldiers who lock all the doors at night."
- **Phase 2: Understanding and Recognizing Cyber Threats**
    - *Core message:* Instructions for active detective work.
    - *Examples:* Analysis of a fake **Netflix payment request** ("support@netflix-pay.com") and a manipulated pop-up for the "Antivirus Defender 3000".
    - *Instructions:* Learners are asked to provide ChatGPT with detailed descriptions of their observations to verify threats.
- **Phase 3: Are we under attack?!**
    - *Core message:* Applying knowledge to complex scenarios.
    - *Case study 1:* An urgent text message from the **CEO** regarding a money transfer where the email address is slightly different (e.g. CEO@yourcornpay.com).
    - *Case study 2:* An attack in an online multiplayer game triggered by a supposed security update that results in changed passwords.

2. Interactive Components

The scenario is characterized by a high level of interactivity that goes beyond mere video consumption.

- **Interactive ChatGPT investigation:** Learners use ChatGPT as a **"digital detective".** They enter specific observations (e.g., "I saw a pop-up claiming my PC is infected...") and receive an assessment of the danger situation from the AI.
- **Knowledge Quiz**: Within the chat environment, **a short quiz can be started** by entering the command "test".
    - *Format:* 4 questions with immediate feedback on learning progress.
- **Verbal evaluation:** An AI avatar triggers a period of reflection in which learners have to verbally justify their decisions to the instructor.

3. Media Portfolio

A portfolio of various digital tools was put together for the implementation:

- **AI avatar tools:** Create the visual tutors with **Synthesia** or **HeyGen**.
- **Learning platform:** Provision is done via the Learnpress LMS.
- **Video hosting:** The finished learning units are documented as **YouTube videos** , which allows for easy integration into various VET platforms.
- **Visual materials:** Screenshots of real-world phishing attempts and malware pop-ups serve as visual anchor points during execution.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union