TEASER

Teacher as Avatar

Lehr- und Lernszenario

Cybersecurity Basics: Identifying & Preventing Cyber Threats

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Nationalen Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung wider. Weder die Europäische Union noch die Bewilligungsbehörde können dafür verantwortlich gemacht werden.

Kofinanziert von der Europäischen Union

Inhalt

I. Stammdaten und Kontext 3
II. Pädagogisches Design 4
III. Technologische Umsetzung 5
IV. Detaillierter Unterrichtsablauf (Lesson Plan) 6
1. Einführung und Orientierung 6
2. Durchführung der Aufgabe 6
3. Bewertung / Überprüfung 7
4. Abschluss der Einheit 7
V. Ressourcen und Begleitmaterialien 8
1. Videos 8
2. Interaktive Komponenten 9
3. Medien-Portfolio 9

I. Stammdaten und Kontext

- **Szenario-Titel und Abstrakt:** Das Szenario trägt den Titel **„Cybersecurity Basics: Identifying & Preventing Cyber Threats“**. Es bietet eine fundierte Einführung in die Identifizierung und Prävention gängiger digitaler Bedrohungen, wobei der Fokus insbesondere auf **Phishing-Versuchen** und **Malware** liegt. Die Lernenden werden zunächst durch einen **KI-generierten Avatar** in die theoretischen Grundlagen eingeführt, bevor sie in eine interaktive Phase des **Problem-Solving mit ChatGPT** übergehen. Ziel dieser Kombination ist es, durch die visuelle Unterstützung des Avatars und die direkte Interaktion mit der KI eine immersive Lernumgebung zu schaffen, die das Sicherheitsbewusstsein nachhaltig stärkt.

- **Berufsfeld und Zielgruppe:** Das Szenario ist im Fachbereich der **digitalen Kompetenzen, IT-Grundlagen und der Sensibilisierung für Cybersicherheit** angesiedelt. Die primäre Zielgruppe umfasst **Auszubildende (ab dem 2. Lehrjahr)**, VET-Lernende (Vocational Education and Training) sowie Berufseinsteiger aus verschiedenen Disziplinen wie Programmierung, Wirtschaft oder Finanzen. Darüber hinaus richtet sich das Material an **VET-Lehrkräfte und Ausbilder**, die ihre pädagogischen Methoden durch den Einsatz von KI und Avataren modernisieren möchten. Das Training ist so konzipiert, dass es auch für Lernende ohne tiefgreifenden IT-Hintergrund zugänglich ist, indem komplexe Begriffe durch die KI in Echtzeit erklärt werden können.

- **Lernziele:** Die Kompetenzentwicklung in diesem Szenario gliedert sich in drei Bereiche:

    - **Wissen (Knowledge):** Die Lernenden erwerben die Fähigkeit, **Phishing- und Malware-Bedrohungen** sicher zu erkennen und verstehen die zugrunde liegenden Muster gängiger Angriffsstrategien. Dazu gehört auch die Kenntnis über verschiedene Angriffsarten wie Spear Phishing, Whaling oder Ransomware.

    - **Fähigkeiten (Skills):** Sie lernen, reale Szenarien kritisch zu analysieren, um **verdächtige Elemente** (wie manipulierte Links oder fehlerhafte E-Mail-Adressen) zu identifizieren. Zudem trainieren sie die Fertigkeit, **gezielte Fragen an eine KI** zu formulieren, um Unklarheiten bei potenziellen Angriffen zu beseitigen.

    - **Kompetenzen (Competencies):** Die Auszubildenden werden befähigt, ihr Cybersecurity-Bewusstsein in **realen Arbeitskontexten** anzuwenden. Sie können ihre Sicherheitsentscheidungen auf Basis von KI-gestützten Erkenntnissen begründen und entwickeln ein verantwortungsvolles Verhalten im digitalen Raum.

II. Pädagogisches Design

- **Die „Educational Question“:** Die zentrale pädagogische Herausforderung dieses Szenarios besteht darin, dass Lernende – insbesondere solche ohne tiefgehenden IT-Hintergrund (wie Auszubildende in den Bereichen Wirtschaft oder Finanzen) – oft Schwierigkeiten haben, **subtile digitale Bedrohungen** zu erkennen und das notwendige Fachvokabular zu verstehen. Das Szenario adressiert die Frage: **Wie kann das Verständnis für komplexe Cybersecurity-Konzepte und Akronyme durch eine interaktive, sichere Lernumgebung verbessert werden?**. Der Einsatz von KI und Avataren löst dieses Problem, indem er eine **konsistente und engagierte Wissensvermittlung** bietet, eine gefahrlose Simulation von Angriffsszenarien erlaubt und die kognitive Belastung durch geführte Interaktionen reduziert.
- **Didaktisches Setting:** Das Szenario ist fest in den europäischen Kompetenzrahmen **DigComp 2.2** und **DigCompEdu** verankert, insbesondere in den Bereichen Informationskompetenz, Sicherheit und Problemlösung. Im Kontext des **SAMR-Modells** erreicht die Lerneinheit die Stufe der **„Modification“ (Umgestaltung)**, da die Aufgabenstellung (die Analyse von Angriffen mittels Echtzeit-KI-Feedback) ohne diese Technologie nicht in derselben Tiefe möglich wäre. Die gewählte Lehrmethode folgt einem **strukturierten 4-Phasen-Modell**:
    1. **Orientierung:** Theoretischer Input durch einen linearen Avatar.
    2. **Durchführung:** Aktives, exploratives Lernen, bei dem die Lernenden als **„digitale Detektive“** fungieren und reale Fälle (Phishing-E-Mails, Malware-Popups) untersuchen.
    3. **Bewertung:** Problemlösungsaufgaben mit direktem KI-Feedback.
    4. **Abschluss:** Kollaborative Reflexion in der Gruppe über die Grenzen und Möglichkeiten der KI-Unterstützung.
- **Rolle des Ausbilders/Lehrers:** In diesem Szenario wandelt sich die Rolle der Lehrkraft grundlegend vom alleinigen Wissensvermittler hin zum **Moderator, Coach und pädagogischen Berater**. Zu den spezifischen Aufgaben gehören:
    - **Einleitung und Rahmensetzung:** Vorstellung des Themas und Erläuterung der Rolle des Avatars.
    - **Unterstützung bei der KI-Interaktion:** Unterstützung der Lernenden bei der Formulierung gezielter Fragen (**Prompt Engineering**) an ChatGPT.
    - **Qualitätssicherung:** Durchführung von **Plausibilitätschecks**, um sicherzustellen, dass die Lernenden KI-generierte Informationen kritisch hinterfragen und keine Fehlinterpretationen (Halluzinationen) übernehmen.
    - **Feedbackgeber:** Moderation der Abschlussdiskussion und Verknüpfung der virtuellen Erfahrungen mit der realen Arbeitspraxis.

III. Technologische Umsetzung

- **KI- und Avatar-Lösung:** In diesem Szenario werden **2D- oder 3D-KI-generierte Avatare** eingesetzt, die vorwiegend **lineare Instruktionsinhalte** in Form von Video-Tutorials vermitteln. Der Avatar fungiert im Lernprozess als **engagierter visueller Leitfaden und Tutor**: Er führt in die theoretischen Konzepte der Cybersicherheit ein, erläutert Fachbegriffe und demonstriert anschaulich Beispiele für Phishing-E-Mails oder Malware-Angriffe. Ergänzend dazu übernimmt **ChatGPT** die Funktion eines **interaktiven Gesprächspartners und „digitalen Detektivs“**, mit dem die Lernenden in einen aktiven Dialog treten können, um spezifische Bedrohungsszenarien in Echtzeit zu analysieren.
- **Technische Werkzeuge:** Für die Realisierung des Szenarios wird eine Auswahl an modernen „Low-Threshold“-Tools und Standard-Hardware verwendet:
    - **Avatar-Generierung: Synthesia** oder **HeyGen** dienen zur schnellen Erstellung der sprechenden Avatare aus Skripten.
    - **Interaktive KI: ChatGPT** (basierend auf GPT-4) wird für die Szenarioanalyse, das Beantworten von Teilnehmerfragen und als Unterstützung beim „Troubleshooting“ von Sicherheitsvorfällen genutzt.
    - **Lernplattform (LMS):** Die Bereitstellung der Kurse erfolgt über **Learnpress**, welches die interaktiven Elemente und Videos strukturiert zusammenführt.
    - **Hardware:** Die Lernenden nutzen handelsübliche **Laptops oder PCs** mit stabilen Internetverbindungen.
    - **Zusatzressourcen:** Einsatz von **YouTube** zum Hosten der Avatar-Videos sowie digitale Notizblätter zur Ergebnissicherung.
- **Software-Hopping-Ansatz:** Die Erstellung der Inhalte folgt einem **niederschwelligen „Software-Hopping-Ansatz“**, der die Stärken verschiedener Anwendungen kombiniert, ohne dass Programmieraufwand erforderlich ist. Der Prozess gliedert sich in folgende Schritte:

1. **Textoptimierung:** Fachliche Rohmanuskripte der Ausbilder werden mit **ChatGPT** sprachlich verfeinert und in ein didaktisch ansprechendes Skript umgewandelt.

2. **Bild- und Videoproduktion:** Die optimierten Texte werden in **Synthesia** geladen, um lippensynchrone Videos mit einem gewählten Avatar-Charakter zu rendern.

3. **Interaktive Verzahnung:** Die fertigen Videos werden in das LMS integriert und mit spezifischen **Prompts für ChatGPT** verknüpft. So können Lernende direkt nach einer Avatar-Erklärung in eine KI-gestützte Fallstudie wechseln, um das Gelernte praktisch anzuwenden.

IV. Detaillierter Unterrichtsablauf (Lesson Plan)

Die Durchführung dieser Lerneinheit ist darauf ausgelegt, die Lernenden in die Rolle von **„Cybersecurity-Ermittlern“** zu versetzen. Der Ablauf gliedert sich in die folgenden vier Phasen:

1. Einführung und Orientierung

- **Dauer:** 4 Minuten.
- **Inhalte:** Grundlegende Einführung in die Konzepte der Cybersicherheit sowie die Identifizierung der zwei häufigsten Bedrohungen: **Phishing** und **Malware**.
- **Aktivitäten:**
    - Die Lernenden betrachten ein Lernvideo, in dem ein **KI-generierter Avatar** (erstellt mit Synthesia) die Bedeutung von Netzwerkschutz erklärt und die Gefahren von Online-Betrugsmethoden aufzeigt.
    - Der Ausbilder (Moderator) führt in die Sitzung ein, erläutert die **Rolle des Avatars** als digitaler Tutor und steht für erste Verständnisfragen bereit.
- **Medien:** Avatar-Videos, erzeugt mittels **Synthesia** oder **HeyGen**.

2. Durchführung der Aufgabe

- **Dauer:** Flexibel (Teil der aktiven Erarbeitungsphase).
- **Inhalte:** Praktische Analyse von realen Angriffsszenarien zur Erkennung von Schwachstellen.
- **Aktivitäten:**
    - Die Lernenden führen eine **interaktive Untersuchung mit ChatGPT** durch. Sie erhalten spezifische Fallbeispiele, wie etwa eine gefälschte **Netflix-Zahlungsaufforderung** („support@netflix-pay.com“) oder einen manipulierten **„Antivirus Defender 3000“**-Pop-up-Alarm.
    - Die Aufgabe besteht darin, ChatGPT gezielte Fragen zu stellen (z. B. „Ich habe einen Pop-up gesehen, der behauptet, mein PC sei infiziert – ist das Malware?“), um die Bedrohung zu verifizieren.
    - Der Ausbilder unterstützt die Lernenden beim **Prompt Engineering** und überwacht die Diskussionen über die gefundenen Merkmale wie verdächtige URLs oder grammatikalische Fehler.
- **Medien: ChatGPT** als interaktiver Assistent, Online-Notizen.

3. Bewertung / Überprüfung

- **Dauer:** 8 Minuten.
- **Inhalte:** Anwendung des erworbenen Wissens auf eine komplexe, reale Situation und verbale Begründung der Sicherheitsentscheidungen.
- **Aktivitäten:**
    - **CEO-Szenario:** Ein Avatar löst eine Aufgabe aus, bei der die Lernenden eine dringende SMS vom „CEO“ erhalten, die sie zu einer schnellen Geldüberweisung auffordert.
    - Die Lernenden müssen die Unstimmigkeiten (z. B. eine leicht abweichende E-Mail-Adresse wie „CEO@yourcornpay.com“) identifizieren, ChatGPT um Rat fragen und ihre **Handlungsweise gegenüber dem Ausbilder mündlich begründen**.
    - Optional kann ein interner Wissenscheck durch Eingabe des Befehls **„test“ im Chat** gestartet werden, um ein kurzes Quiz mit sofortigem Feedback zu absolvieren.

4. Abschluss der Einheit

- **Dauer:** 8 Minuten.
- **Inhalte:** Zusammenfassung der wichtigsten Erkenntnisse und Reflexion über den Lernprozess.
- **Aktivitäten:**
    - In einer moderierten **Gruppendiskussion** reflektieren die Teilnehmenden über die Wirksamkeit der KI-Unterstützung und die Grenzen der Technologie.
    - Es werden Schutzstrategien für den Arbeitsalltag konsolidiert, wie z. B. die Aktivierung der Zwei-Faktor-Authentifizierung oder die Meldung verdächtiger Nachrichten an das IT-Team.
    - Der Transfer in die Praxis wird durch die Besprechung menschlicher Wachsamkeit als „beste Verteidigung“ abgeschlossen.

V. Ressourcen und Begleitmaterialien

1. Videos

Die Wissensvermittlung stützt sich auf **KI-Avatar-Videos**. Diese enthalten nicht nur fachliche Informationen, sondern nutzen auch einprägsame **Analogien**, um die Konzepte zu verdeutlichen.

- **Phase 1: Mastering Cybersecurity – Spotting Phishing & Malware**
    - *Kernbotschaft:* Definition von Cybersicherheit als Praxis zum Schutz von Systemen, Netzwerken und Daten.
    - *Inhalt:* Einführung in **Phishing** (betrügerische Versuche, sensible Informationen zu stehlen) und **Malware** (schädliche Software zur Beschädigung von Systemen).
    - *Sicherheitsregeln:* Warnung vor dem Öffnen von Anhängen aus verdächtigen Quellen, Nutzung aktueller Antivirensoftware und regelmäßige Backups.
    - *Analogie:* „Stellen Sie sich Ihren Computer wie eine **Festung** vor. Phishing ist wie ein Spion, der den Wachposten anruft und sich als General ausgibt, um das Tor zu öffnen. Malware ist wie ein **hölzernes Pferd**, das Soldaten einschleust, die nachts alle Türen verriegeln“.
- **Phase 2: Understanding and Recognizing Cyber Threats**
    - *Kernbotschaft:* Anleitung zur aktiven Detektivarbeit.
    - *Beispiele:* Analyse einer gefälschten **Netflix-Zahlungsaufforderung** („support@netflix-pay.com“) und eines manipulierten Pop-ups für den „Antivirus Defender 3000“.
    - *Anleitung:* Lernende werden aufgefordert, ChatGPT detaillierte Beschreibungen ihrer Beobachtungen zu geben, um Bedrohungen zu verifizieren.
- **Phase 3: Are we under attack?!**
    - *Kernbotschaft:* Anwendung des Wissens auf komplexe Szenarien.
    - *Fallstudie 1:* Eine dringende SMS vom **CEO** bezüglich einer Geldüberweisung, bei der die E-Mail-Adresse leicht abweicht (z. B. CEO@yourcornpay.com).
    - *Fallstudie 2:* Ein Angriff in einem Online-Multiplayer-Spiel, der durch ein vermeintliches Sicherheitsupdate ausgelöst wurde und zu geänderten Passwörtern führt.

2. Interaktive Komponenten

Das Szenario zeichnet sich durch eine hohe Interaktivität aus, die über den bloßen Videokonsum hinausgeht.

- **Interaktive ChatGPT-Untersuchung:** Lernende nutzen ChatGPT als **„digitalen Detektiv“**. Sie geben spezifische Beobachtungen ein (z. B. „Ich habe ein Pop-up gesehen, das behauptet, mein PC sei infiziert…“) und erhalten von der KI eine Einschätzung zur Gefahrenlage.
- **Wissensquiz (Knowledge Check):** Innerhalb der Chat-Umgebung kann durch Eingabe des Befehls **„test“** ein kurzes Quiz gestartet werden.
    - *Format:* 4 Fragen mit sofortigem Feedback zum Lernfortschritt.
- **Verbale Bewertung:** Ein KI-Avatar löst eine Reflexionsphase aus, in der die Lernenden ihre Entscheidungen gegenüber dem Ausbilder mündlich begründen müssen.

3. Medien-Portfolio

Für die Umsetzung wurde ein Portfolio aus verschiedenen digitalen Werkzeugen zusammengestellt:

- **KI-Avatar-Tools:** Erstellung der visuellen Tutoren mit **Synthesia** oder **HeyGen**.
- **Lernplattform:** Die Bereitstellung erfolgt über das LMS **Learnpress**.
- **Video-Hosting:** Die fertigen Lerneinheiten sind als **YouTube-Videos** dokumentiert, was eine einfache Einbindung in verschiedene VET-Plattformen ermöglicht.
- **Visuelle Materialien:** Screenshots von realen Phishing-Versuchen und Malware-Pop-ups dienen als visuelle Ankerpunkte während der Durchführung.