TEASER

Teacher as Avatar

Onderwijs- en leerscenario

Cybersecurity Basis: Cyberdreigingen identificeren en voorkomen

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

Inhoud

I. Mastergegevens en context

- **Scenariotitel en samenvatting:** Het scenario heet **"Cybersecurity Basics: Identifying & Preventing Cyber Threats".** Het biedt een diepgaande introductie tot het identificeren en voorkomen van veelvoorkomende digitale dreigingen, met bijzondere aandacht voor **phishingpogingen** en **malware**. Leerlingen maken eerst kennis met de theoretische basisprincipes door een **door AI gegenereerde avatar**, waarna ze overgaan naar een interactieve probleemoplossende fase **met ChatGPT**. Het doel van deze combinatie is het creëren van een meeslepende leeromgeving die het beveiligingsbewustzijn duurzaam versterkt door visuele ondersteuning van de avatar en directe interactie met de AI.

- **Professioneel vakgebied en doelgroep:** Het scenario bevindt zich op het gebied van **digitale vaardigheden, IT-basisprincipes en het vergroten van het bewustzijn over cybersecurity**. De primaire doelgroep bestaat uit **stagiairs (vanaf het tweede jaar van de leer),** VET-leerlingen (Beroepsonderwijs en Opleiding) evenals starters uit verschillende disciplines zoals programmeren, economie of financiën. Daarnaast is het materiaal gericht op **VET-docenten en docenten** die hun pedagogische methoden willen moderniseren door gebruik te maken van AI en avatars. De training is ontworpen om toegankelijk te zijn voor cursisten zonder diepgaande IT-achtergrond, doordat complexe termen in realtime door AI kunnen worden uitgelegd.

- **Leerdoelstellingen:** Competentieontwikkeling in dit scenario is verdeeld in drie gebieden:

    - **Kennis:** Leerlingen verwerven het vermogen om **phishing- en malwaredreigingen** betrouwbaar te detecteren en de onderliggende patronen van veelvoorkomende aanvalstrategieën te begrijpen. Dit omvat ook kennis van verschillende soorten aanvallen zoals spear phishing, whaling of ransomware.

    - **Vaardigheden:** Je leert realistische situaties kritisch te analyseren om **verdachte elementen** te identificeren (zoals gemanipuleerde links of foutieve e-mailadressen). Daarnaast trainen ze het vermogen om **specifieke vragen aan een AI** te formuleren om ambiguïteiten te elimineren in het geval van mogelijke aanvallen.

    - **Competenties:** Trainees worden in staat hun cybersecurity-bewustzijn toe te passen in **echte werksituaties** . Zij kunnen hun beveiligingsbeslissingen rechtvaardigen op basis van AI-ondersteunde inzichten en verantwoord gedrag ontwikkelen in de digitale ruimte.

II. Onderwijsontwerp

- **De "Educatieve Vraag":** De centrale pedagogische uitdaging van dit scenario is dat leerlingen – vooral degenen zonder diepgaande IT-achtergrond (zoals stagiairs in bedrijfskunde of financiën) – vaak moeite hebben om **subtiele digitale bedreigingen** te identificeren en de benodigde technische woordenschat te begrijpen. Het scenario behandelt de vraag: **Hoe kan het begrip van complexe cybersecurityconcepten en acroniemen worden verbeterd door een interactieve, veilige leeromgeving?**. Het gebruik van AI en avatars lost dit probleem op door **consistente en betrokken kennisoverdracht te bieden**, waardoor een veilige simulatie van aanvalscenario's mogelijk is en de cognitieve last van geleide interacties wordt verminderd.

- **Didactische setting:** Het scenario is stevig verankerd in de Europese competentiekaders **DigComp 2.2** en **DigCompEdu**, vooral op het gebied van informatievaardigheid, beveiliging en probleemoplossing. In de context van het **SAMR-model** bereikt de leerunit het niveau van **"modificatie" (herontwerp),** omdat de taak (de analyse van aanvallen met realtime AI-feedback) zonder deze technologie niet op dezelfde diepte mogelijk zou zijn. De gekozen lesmethode volgt een **gestructureerd 4-fasenmodel**:

    1. **Oriëntatie:** Theoretische input via een lineaire avatar.
    2. **Levering:** Actief, verkennend leren waarbij leerlingen optreden als **"digitale detectives"** en praktijkzaken onderzoeken (phishing-e-mails, malware-pop-ups).
    3. **Beoordeling:** Probleemoplossende taken met directe AI-feedback.
    4. **Conclusie:** Gezamenlijke reflectie in de groep over de grenzen en mogelijkheden van AI-ondersteuning.

- **Rol van de trainer/docent:** In dit scenario verandert de rol van de docent fundamenteel van de enige kennisoverdrager naar **de facilitator, coach en pedagogisch adviseur**. Specifieke taken zijn onder andere:

    - **Introductie en setting: Introductie van** het onderwerp en uitleg van de rol van de avatar.
    - **AI-interactieondersteuning:** Ondersteuning van leerlingen bij het formuleren van gerichte vragen (**prompt engineering**) voor ChatGPT.
    - **Kwaliteitsborging:** Het uitvoeren van **plausibiliteitscontroles** om ervoor te zorgen dat leerlingen AI-gegenereerde informatie kritisch in twijfel trekken en geen misinterpretaties (hallucinaties) aannemen.
    - **Feedbackgevers:** Moderatie van de uiteindelijke discussie en koppeling van virtuele ervaringen aan echte werkpraktijken.

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. Technologische implementatie

- **AI en avataroplossing:** In dit scenario worden **2D- of 3D-AI-gegenereerde avatars** gebruikt, die voornamelijk **lineaire instructieve inhoud** overbrengen in de vorm van videotutorials. De avatar fungeert als **een speciale visuele gids en mentor** in het leerproces: het introduceert de theoretische concepten van cybersecurity, legt technische termen uit en toont levendig voorbeelden van phishing-e-mails of malware-aanvallen. Daarnaast vervult **ChatGPT** de rol van interactieve **gesprekspartner en "digitale detective"** met wie leerlingen een actieve dialoog kunnen voeren om specifieke dreigingsscenario's in realtime te analyseren.
- **Technische tools:** Een selectie van moderne "low-threshold" tools en standaardhardware wordt gebruikt om het scenario te realiseren:
    - **Avatargeneratie: Synthesia** of **HeyGen** worden gebruikt om snel pratende avatars te creëren vanuit scripts.
    - **Interactieve AI: ChatGPT** (gebaseerd op GPT-4) wordt gebruikt voor scenario-analyse, het beantwoorden van vragen van deelnemers en het assisteren bij het "troubleshooten" van beveiligingsincidenten.
    - **Leerplatform (LMS):** De cursussen worden aangeboden via **Learnpress**, dat de interactieve elementen en video's op een gestructureerde manier samenbrengt.
    - **Hardware:** Leerlingen gebruiken standaard **laptops of pc's** met stabiele internetverbindingen.
    - **Extra bronnen:** Gebruik van **YouTube** om avatarvideo's te hosten en digitale notitieboekjes om resultaten op te slaan.
- **Software hopping-benadering:** Content creatie volgt een **laagdrempelige "software hopping-aanpak"** die de sterke punten van verschillende applicaties combineert zonder dat er gecoderen hoeft te worden. Het proces is onderverdeeld in de volgende stappen:

1. **Tekstoptimalisatie:** Ruwe technische manuscripten van de trainers worden **taalkundig verfijnd met ChatGPT** en omgezet in een didactisch aantrekkelijk script.

2. **Beeld- en videoproductie:** De geoptimaliseerde teksten worden in **Synthesia** geladen om lip-sync video's te renderen met een gekozen avatarpersonage.

3. **Interactieve integratie:** De uiteindelijke video's worden geïntegreerd in het LMS en gekoppeld aan specifieke **prompts voor ChatGPT** . Zo kunnen leerlingen direct na een avatar-uitleg overstappen op een AI-gestuurde casestudy om toe te passen wat ze geleerd hebben in de praktijk.

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. Gedetailleerd lesplan

De uitvoering van deze eenheid is bedoeld om leerlingen in de rol van **"cybersecurityonderzoekers"** te plaatsen. Het proces is verdeeld in de volgende vier fasen:

1. Introductie en inleiding

- **Duur:** 4 minuten.
- **Inhoud:** Basisintroductie tot cybersecurityconcepten en hoe je de twee meest voorkomende dreigingen kunt identificeren: **phishing** en **malware**.
- **Activiteiten:**
    - Leerlingen bekijken een instructievideo waarin een **door AI gegenereerde avatar** (gemaakt met Synthesia) het belang van netwerkbeveiliging uitlegt en de gevaren van online oplichting belicht.
    - De trainer (moderator) introduceert de sessie, legt de **rol van de avatar** als digitale tutor uit en is beschikbaar voor de eerste begripvragen.
- **Media:** Avatarvideo's, gemaakt met **Synthesia** of **HeyGen**.

2. Uitvoering van de taak

- **Duur:** Flexibel (onderdeel van de actieve ontwikkelingsfase).
- **Inhoud:** Praktische analyse van echte aanvalscenario's om kwetsbaarheden te identificeren.
- **Activiteiten:**
    - Leerlingen voeren een **interactief onderzoek uit met behulp van ChatGPT**. Je krijgt specifieke casestudy's, zoals een **nep-Netflix-betalingsverzoek** ("support@netflix-pay.com") of een gemanipuleerde **"Antivirus Defender 3000"** pop-upmelding.
    - De taak is om ChatGPT gerichte vragen te stellen (bijvoorbeeld: "Ik zag een pop-up waarin werd beweerd dat mijn pc geïnfecteerd is – is dat malware?") om de dreiging te verifiëren.
    - De instructeur helpt leerlingen met **prompt engineering** en volgt discussies over de gevonden kenmerken, zoals verdachte URL's of grammaticale fouten.
- **Media: ChatGPT** als interactieve assistent, online notities.

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. Evaluatie / Beoordeling

- **Duur:** 8 minuten.
- **Inhoud:** Toepassing van de verworven kennis op een complexe, reële situatie en mondelinge rechtvaardiging van veiligheidsbeslissingen.
- **Activiteiten:**
    - **CEO-scenario:** Een avatar activeert een taak waarbij leerlingen een dringende sms ontvangen van de "CEO" met het verzoek om een snelle geldovermaking.
    - Leerlingen moeten de afwijkingen identificeren (bijvoorbeeld een iets ander e-mailadres zoals "CEO@yourcornpay.com"), ChatGPT om advies vragen en **hun handelen mondeling aan de docent verantwoorden**.
    - Optioneel kan een interne kennischeck worden gestart door het "**testen"-commando in de chat in te** voeren om een korte quiz met directe feedback te voltooien.

4. Afronding van de sessie

- **Duur:** 8 minuten.
- **Inhoud:** Samenvatting van de belangrijkste bevindingen en reflectie op het leerproces.
- **Activiteiten:**
    - In een gemodereerde **groepsdiscussie** reflecteren deelnemers op de effectiviteit van AI-ondersteuning en de beperkingen van de technologie.
    - Het consolideert dagelijkse beschermingsstrategieën, zoals het inschakelen van tweefactorauthenticatie of het melden van verdachte berichten aan het IT-team.
    - De overdracht naar de praktijk wordt afgerond door menselijke waakzaamheid als de "beste verdediging" te bespreken.

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. Middelen en nevenzaken

1. Video's

De kennisoverdracht is gebaseerd op **AI-avatarvideo's**. Deze bevatten niet alleen technische informatie, maar gebruiken ook memorabele **analogieën** om de concepten te verduidelijken.

- **Fase 1: Cybersecurity beheersen – Phishing & malware herkennen**
    - *Kernboodschap:* Definieer cybersecurity als een praktijk om systemen, netwerken en data te beschermen.
    - *Inhoud:* Introductie tot **phishing** (frauduleuze pogingen om gevoelige informatie te stelen) en **malware** (kwaadaardige software die systemen beschadigt).
    - *Beveiligingsregels:* Waarschuwing voor het openen van bijlagen van verdachte bronnen, het gebruik van actuele antivirussoftware en regelmatige back-ups.
    - *Analogie:* "Zie je computer als een **vesting**. Phishing is als een spion die de wachtpost belt en zich voordoet als generaal om de poort te openen. Malware is als een **houten paard** dat soldaten binnendringt en 's nachts alle deuren op slot doen."
- **Fase 2: Begrijpen en herkennen van cyberdreigingen**
    - *Kernboodschap:* Instructies voor actief speurwerk.
    - *Voorbeelden:* Analyse van een nep-betalingsverzoek **van Netflix** ("support@netflix-pay.com") en een gemanipuleerde pop-up voor de "Antivirus Defender 3000".
    - *Instructies:* Leerlingen worden gevraagd ChatGPT gedetailleerde beschrijvingen van hun observaties te geven om bedreigingen te verifiëren.
- **Fase 3: Worden we aangevallen?!**
    - *Kernboodschap:* Kennis toepassen op complexe scenario's.
    - *Case study 1:* Een dringend sms-bericht van de **CEO** over een geldoverboeking waarbij het e-mailadres iets anders is (bijvoorbeeld CEO@yourcornpay.com).
    - *Casestudy 2:* Een aanval in een online multiplayer-spel getriggerd door een vermeende beveiligingsupdate die resulteert in gewijzigde wachtwoorden.

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

2. Interactieve componenten

Het scenario wordt gekenmerkt door een hoog niveau van interactiviteit dat verder gaat dan alleen videoconsumptie.

- **Interactief ChatGPT-onderzoek:** Leerlingen gebruiken ChatGPT als een **"digitale detective".** Ze voeren specifieke observaties in (bijvoorbeeld: "Ik zag een pop-up waarin werd beweerd dat mijn pc geïnfecteerd is...") en krijgen een beoordeling van de gevaarsituatie van de AI.
- **Kennisquiz**: Binnen de chatomgeving **kan een korte quiz worden gestart** door het commando "test" in te voeren.
    - *Formaat:* 4 vragen met directe feedback over de leervoortgang.
- **Een verbale evaluatie:** Een AI-avatar zet een reflectieperiode in gang waarin leerlingen hun beslissingen mondeling moeten rechtvaardigen tegenover de instructeur.

3. Mediaportfolio

Voor de implementatie werd een portfolio samengesteld van diverse digitale tools:

- **AI-avatartools:** Maak de visuele tutors met **Synthesia** of **HeyGen**.
- **Leerplatform:** De levering gebeurt via het Learnpress LMS.
- **Videohosting:** De voltooide leerunits worden gedocumenteerd als **YouTube-video's** , wat eenvoudige integratie in verschillende VET-platforms mogelijk maakt.
- **Visuele materialen:** Screenshots van echte phishingpogingen en malware-pop-ups dienen als visuele ankerpunten tijdens de uitvoering.