TEASER

Teacher as Avatar

Scenarij poučevanja in učenja

Osnove kibernetske varnosti: Prepoznavanje in preprečevanje kibernetskih groženj

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

Vsebina

I. Glavni podatki in kontekst

- **Naslov scenarija in povzetek:** Scenarij nosi naslov **"Osnove kibernetske varnosti: Prepoznavanje in preprečevanje kibernetskih groženj".** Ponuja poglobljen uvod v prepoznavanje in preprečevanje pogostih digitalnih groženj, s posebnim poudarkom na **phishing poskusih** in **zlonamerni programski opremi**. Učenci se najprej seznanijo s teoretičnimi osnovami preko **avatarja, ustvarjenega z umetno inteligenco,** preden nadaljujejo z interaktivno fazo reševanja problemov **s ChatGPT**. Cilj te kombinacije je ustvariti poglobljeno učno okolje, ki trajnostno krepi varnostno ozaveščenost z vizualno podporo avatarja in neposredno interakcijo z umetno inteligenco.
- **Strokovno področje in ciljna skupina:** Scenarij je umeščen na področje **digitalnih veščin, osnov IT in ozaveščanja o kibernetski** varnosti. Glavna ciljna skupina vključujejo **vajence (od 2. letnika vajeništva),** vajence za poklicno izobraževanje in usposabljanje ter začetnike kariere iz različnih disciplin, kot so programiranje, ekonomija ali finance. Poleg tega je gradivo namenjeno **učiteljem in inštruktorjem VET**, ki želijo posodobiti svoje pedagoške metode z uporabo umetne inteligence in avatarjev. Usposabljanje je zasnovano tako, da je dostopno učencem brez globokega IT znanja, saj omogoča razlago zapletenih pojmov v realnem času z umetno inteligenco.
- **Učni cilji:** Razvoj kompetenc v tem scenariju je razdeljen na tri področja:
    - **Znanje:** Učenci pridobijo sposobnost zanesljivega zaznavanja **phishing in zlonamernih groženj** ter razumevanja osnovnih vzorcev pogostih napadalnih strategij. To vključuje tudi poznavanje različnih vrst napadov, kot so spear phishing, whaling ali izsiljevalska programska oprema.
    - **Veščine:** Naučili se boste kritično analizirati resnične situacije in **prepoznati sumljive elemente** (kot so manipulirane povezave ali napačni e-poštni naslovi). Poleg tega trenirajo sposobnost oblikovanja **specifičnih vprašanj AI**, da bi odpravili nejasnosti v primeru morebitnih napadov.
    - **Kompetence:** Pripravniki lahko svojo ozaveščenost o kibernetski varnosti uporabijo v **resničnih delovnih kontekstih** . Svoje varnostne odločitve lahko upravičijo na podlagi vpogledov, ki jih podpira umetna inteligenca, in razvijejo odgovorno vedenje v digitalnem prostoru.

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. Izobraževalno oblikovanje

- **"Izobraževalno vprašanje":** Osrednji pedagoški izziv tega scenarija je, da se učenci – zlasti tisti brez poglobljenega IT znanja (kot so pripravniki v poslovnem svetu ali financah) – pogosto težko prepoznajo **subtilne digitalne** grožnje in razumejo potreben tehnični besednjak. Scenarij odgovarja na vprašanje: **Kako lahko izboljšamo razumevanje kompleksnih konceptov in okrajšav kibernetske varnosti z interaktivnim, varnim učnim okoljem?.** Uporaba umetne inteligence in avatarjev rešuje ta problem z zagotavljanjem **doslednega in angažiranega prenosa znanja**, kar omogoča varno simulacijo napadalnih scenarijev in zmanjšuje kognitivno breme vodenih interakcij.
- **Didaktično okolje:** Scenarij je trdno zasidran v evropskih okvirih kompetenc **DigComp 2.2** in **DigCompEdu**, zlasti na področjih informacijske pismenosti, varnosti in reševanja problemov. V kontekstu **modela SAMR** učna enota doseže raven **"spremembe" (prenove),** saj naloga (analiza napadov z uporabo povratnih informacij umetne inteligence v realnem času) brez te tehnologije ne bi bila mogoča v enaki globini. Izbrana metoda poučevanja sledi strukturiranemu **štirifaznemu modelu**:
    1. **Orientacija:** Teoretični vhod preko linearnega avatarja.
    2. **Izvedba:** Aktivno, raziskovalno učenje, kjer učenci delujejo kot **"digitalni detektivi"** in preiskujejo resnične primere (phishing e-pošta, pojavna okna z zlonamerno programsko opremo).
    3. **Ocenjevanje:** Naloge reševanja problemov z neposredno povratno informacijo umetne inteligence.
    4. **Zaključek:** Skupna refleksija v skupini o mejah in možnostih podpore UI.
- **Vloga trenerja/učitelja:** V tem primeru se vloga učitelja temeljito spremeni iz edinega prenašalca znanja v **facilitatorja, mentorja in pedagoškega svetovalca**. Specifične naloge vključujejo:
    - **Uvod in okolje: Uvod** v temo in razlaga vloge avatarja.
    - **Podpora interakcijam z umetno inteligenco:** Podpora učencem pri oblikovanju ciljno usmerjenih vprašanj (**inženiring pozivov**) za ChatGPT.
    - **Zagotavljanje kakovosti: Izvajanje preverjanj verjetnosti**, da se zagotovi, da učenci kritično postavljajo pod vprašaj informacije, ustvarjene z umetno inteligenco, in ne sprejemajo napačnih interpretacij (halucinacij).
    - **Ponudnik povratnih informacij**: Moderiranje končne razprave in povezovanje virtualnih izkušenj z resnično delovno prakso.

III. Tehnološka implementacija

- **Rešitev za umetno inteligenco in avatarje:** V tem primeru se **uporabljajo 2D ali 3D avatarji, generirani z umetno inteligenco** , ki predvsem prenašajo **linearno izobraževalno** vsebino v obliki video vodičev. Avatar deluje kot **namenski vizualni vodnik in mentor** v učnem procesu: uvaja teoretične koncepte kibernetske varnosti, razlaga tehnične izraze in živo prikazuje primere phishing e-poštnih sporočil ali napadov z zlonamerno programsko opremo. Poleg tega **ChatGPT** prevzame funkcijo **interaktivnega sogovornika in »digitalnega detektiva«,** s katerim lahko učenci v aktivnem dialogu analizirajo specifične scenarije groženj v realnem času.
- **Tehnična orodja:** Za uresničitev scenarija se uporablja izbor sodobnih "nizkopragovnih" orodij in standardne strojne opreme:
    - **Generiranje avatarjev: Synthesia** ali HeyGen **se uporabljata za hitro ustvarjanje govorečih avatarjev iz skript.**
    - **Interaktivna umetna inteligenca: ChatGPT** (temelji na GPT-4) se uporablja za analizo scenarijev, odgovarjanje na vprašanja udeležencev in pomoč pri "odpravljanju težav" varnostnih incidentov.
    - **Učna platforma (LMS):** Tečaji so na voljo prek **Learnpressa**, ki združuje interaktivne elemente in videoposnetke na strukturiran način.
    - **Strojna oprema:** Učenci uporabljajo standardne **prenosnike ali osebne računalnike** s stabilno internetno povezavo.
    - **Dodatni viri:** Uporaba YouTuba za gostovanje videoposnetkov avatarjev ter digitalnih zvezkov za shranjevanje rezultatov.
- **Pristop skakanja po programski opremi:** Ustvarjanje vsebin sledi **nizkopragovnemu pristopu "skakanja med programsko opremo",** ki združuje prednosti različnih aplikacij brez potrebe po programiranju. Postopek je razdeljen na naslednje korake:

1. **Optimizacija besedila:** Surovi tehnični rokopisi trenerjev so jezikovno izpopolnjeni **s ChatGPT** in pretvorjeni v didaktično privlačno pisavo.

2. **Produkcija slik in videa:** Optimizirana besedila se naložijo v **Synthesio** za upodabljanje videoposnetkov sinhronizacije ustnic z izbranim avatarjem.

3. **Interaktivno povezovanje:** Končni videoposnetki so integrirani v LMS in povezani s specifičnimi pozivi **za ChatGPT** . Na primer, učenci lahko takoj po razlagi avatarja preklopijo na študijo primera, ki jo poganja umetna inteligenca, da uporabijo pridobljeno znanje v praksi.

IV. Podroben učni načrt

Izvedba te enote je zasnovana tako, da udeležence postavi v vlogo **"preiskovalcev kibernetske varnosti".** Postopek je razdeljen na naslednje štiri faze:

1. Uvod in uvod

- **Trajanje:** 4 minute.
- **Vsebina:** Osnovni uvod v koncepte kibernetske varnosti ter kako prepoznati dve najpogostejši grožnji: **ribarjenje** in **zlonamerno programsko opremo**.
- **Dejavnosti:**
    - Učenci si ogledajo učni video, v katerem avatar, **ustvarjen z umetno inteligenco** (ustvarjen s Synthesio), pojasnjuje pomen zaščite omrežja in opozarja na nevarnosti spletnih prevar.
    - Trener (moderator) predstavi sejo, pojasni **vlogo avatarja** kot digitalnega inštruktorja in je na voljo za začetna vprašanja za razumevanje.
- **Mediji:** Avatar videoposnetki, ustvarjeni s pomočjo **Synthesia** ali **HeyGen**.

2. Izvedba naloge

- **Trajanje:** Prilagodljivo (del faze aktivnega razvoja).
- **Vsebina:** Praktična analiza scenarijev napadov v resničnem svetu za prepoznavanje ranljivosti.
- **Dejavnosti:**
    - Učenci izvajajo **interaktivno raziskavo z uporabo ChatGPT**. Prejeli boste specifične študije primerov, kot je lažna **zahteva za plačilo za Netflix** ("support@netflix-pay.com") ali prirejeno **pojavno okno** "Antivirus Defender 3000".
    - Naloga je, da ChatGPT-ju zastavite ciljana vprašanja (npr. "Videla sem pojavno okno, ki trdi, da je moj računalnik okužen – je to zlonamerna programska oprema?") za preverjanje grožnje.
    - Inštruktor pomaga učencem pri **oblikovanju promptov** in spremlja razprave o najdenih funkcijah, kot so sumljivi URL-ji ali slovnične napake.
- **Mediji: ChatGPT** kot interaktivni pomočnik, spletni zapiski.

3. Ocena / Pregled

- **Trajanje:** 8 minut.
- **Vsebina: Uporaba** pridobljenega znanja v zapleteni, resnični situaciji in ustna utemeljitev varnostnih odločitev.
- **Dejavnosti:**
    - **Scenarij direktorja:** Avatar sproži nalogo, kjer učenci prejmejo nujno SMS sporočilo od "direktorja", ki jih prosi k hitremu nakazilu denarja.
    - Učenci morajo prepoznati neskladja (npr. nekoliko drugačen e-poštni naslov, kot je "CEO@yourcornpay.com"), prositi ChatGPT za nasvet in ustno upravičiti **svoja dejanja inštruktorju**.
    - Po želji se lahko notranji preizkus znanja začne z vnosom ukaza **"test" v klepetu,** da zaključite kratek kviz z takojšnjimi povratnimi informacijami.

4. Zaključek seje

- **Trajanje:** 8 minut.
- **Vsebina:** Povzetek najpomembnejših ugotovitev in razmišljanje o učnem procesu.
- **Dejavnosti:**
    - V moderirani skupinski **razpravi** bodo udeleženci razmišljali o učinkovitosti podpore UI in omejitvah tehnologije.
    - Združuje vsakodnevne zaščitne strategije, kot so omogočanje dvofaktorske avtentikacije ali poročanje sumljivih sporočil IT ekipi.
    - Prenos v prakso se zaključi z razpravo o človeški budnosti kot "najboljši obrambi."

V. Viri in zavarovanje

1. Videi

Prenos znanja temelji na **videoposnetkih z AI avatarji**. Te ne vsebujejo le tehničnih informacij, ampak uporabljajo tudi nepozabne **analogije** za pojasnitev konceptov.

- **Faza 1: Obvladovanje kibernetske varnosti – Prepoznavanje phishinga in zlonamerne programske opreme**
    - *Ključno sporočilo:* Kibernetsko varnost opredelite kot prakso za zaščito sistemov, omrežij in podatkov.
    - *Vsebina:* Uvod v **phishing** (goljufive poskuse kraje občutljivih informacij) in **zlonamerno programsko opremo** (zlonamerno programsko opremo, ki škoduje sistemom).
    - *Varnostna pravila:* Opozorilo pred odpiranjem priponk iz sumljivih virov, uporabo posodobljene protivirusne programske opreme in rednimi varnostnimi kopijami.
    - *Primerjava:* "Pomislite na svoj računalnik kot na trdnjavo. Phishing je kot vohun, ki pokliče stražarsko postajo in se pretvarja, da je general, da odpre vrata. Zlonamerna programska oprema je kot lesen **konj**, ki se infiltrira med vojake, ki ponoči zaklepajo vsa vrata."
- **Faza 2: Razumevanje in prepoznavanje kibernetskih groženj**
    - *Glavno sporočilo:* Navodila za aktivno detektivsko delo.
    - *Primeri:* analiza lažnega Netflixovega plačilnega **zahtevka** ("support@netflix-pay.com") in manipuliranega pojavnega okna za "Antivirus Defender 3000".
    - *Navodila:* Učence prosijo, da ChatGPT-ju zagotovijo podrobne opise svojih opažanj za preverjanje groženj.
- **Faza 3: Ali smo pod napadom?!**
    - *Glavno sporočilo:* Uporaba znanja v zapletenih situacijah.
    - *Študija primera 1:* Nujno SMS sporočilo direktorja glede nakazila denarja, kjer je e-poštni naslov nekoliko drugačen (npr. CEO@yourcornpay.com).
    - *Študija primera 2:* Napad v spletni večigralski igri, sprožen zaradi domnevne varnostne posodobitve, ki povzroči spremembo gesel.

2. Interaktivne komponente

Scenarij zaznamuje visoka stopnja interaktivnosti, ki presega zgolj ogled videa.

- **Interaktivna preiskava ChatGPT:** Učenci uporabljajo ChatGPT kot **"digitalnega detektiva".** Vnesejo določena opazovanja (npr. "Videla sem pojavno okno, ki trdi, da je moj računalnik okužen...") in prejmejo oceno nevarnosti od umetne inteligence.
- **Kviz znanja**: V klepetalnem okolju **lahko začnete kratek kviz** z vnosom ukaza "test".
    - *Format:* 4 vprašanja z takojšnjimi povratnimi informacijami o napredku pri učenju.
- **Ustna evalvacija:** AI avatar sproži obdobje razmisleka, v katerem morajo učenci verbalno utemeljiti svoje odločitve inštruktorju.

3. Medijski portfelj

Za implementacijo je bil pripravljen portfelj različnih digitalnih orodij:

- **Orodja za AI avatarje:** Ustvarite vizualne učitelje s **Synthesia** ali **HeyGen**.
- **Učna platforma:** Zagotavljanje poteka prek Learnpress LMS.
- **Gostovanje videov:** Končne učne enote so dokumentirane kot **YouTube videi** , kar omogoča enostavno integracijo v različne platforme za izobraževanje in usposabljanje.
- **Vizualni materiali:** Posnetki zaslona resničnih poskusov phishinga in pojavnih oken z zlonamerno programsko opremo služijo kot vizualne sidrišča med izvajanjem.