TEASER

Teacher as Avatar

Σενάριο διδασκαλίας και μάθησης

Βασικά στοιχεία κυβερνοασφάλειας: Εντοπισμός και πρόληψη απειλών στον κυβερνοχώρο

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

Περιεχόμενα

I. Κύρια δεδομένα και πλαίσιο

- **Τίτλος σεναρίου και περίληψη: Το** σενάριο έχει τίτλο **«Βασικά στοιχεία κυβερνοασφάλειας: Εντοπισμός & Πρόληψη Απειλών στον Κυβερνοχώρο».** Παρέχει μια εις βάθος εισαγωγή στον εντοπισμό και την πρόληψη κοινών ψηφιακών απειλών, με ιδιαίτερη έμφαση στις **απόπειρες phishing** και **το κακόβουλο λογισμικό**. Οι μαθητές εισάγονται πρώτα στα θεωρητικά βασικά από ένα **avatar που δημιουργείται από AI** πριν προχωρήσουν σε μια διαδραστική φάση επίλυσης προβλημάτων **με το ChatGPT.** Ο στόχος αυτού του συνδυασμού είναι να δημιουργήσει ένα καθηλωτικό περιβάλλον μάθησης που ενισχύει βιώσιμα την ευαισθητοποίηση σχετικά με την ασφάλεια μέσω της οπτικής υποστήριξης του avatar και της άμεσης αλληλεπίδρασης με το AI.

- **Επαγγελματικός τομέας και ομάδα-στόχος:** Το σενάριο εντοπίζεται στον τομέα των **ψηφιακών δεξιοτήτων, των βασικών αρχών πληροφορικής και της ευαισθητοποίησης σχετικά με την ασφάλεια στον κυβερνοχώρο**. Η κύρια ομάδα-στόχος περιλαμβάνει **εκπαιδευόμενους (από το 2ο έτος μαθητείας),** μαθητευόμενους ΕΕΚ (Επαγγελματική Εκπαίδευση και Κατάρτιση) καθώς και αρχάριους σταδιοδρομίας από διάφορους κλάδους όπως ο προγραμματισμός, τα οικονομικά ή τα χρηματοοικονομικά. Επιπλέον, το υλικό απευθύνεται σε **δασκάλους και εκπαιδευτές ΕΕΚ** που θέλουν να εκσυγχρονίσουν τις παιδαγωγικές τους μεθόδους μέσω της χρήσης τεχνητής νοημοσύνης και avatars. Η εκπαίδευση έχει σχεδιαστεί για να είναι προσβάσιμη σε μαθητές χωρίς βαθύ υπόβαθρο πληροφορικής, επιτρέποντας την εξήγηση σύνθετων όρων σε πραγματικό χρόνο από την τεχνητή νοημοσύνη.

- **Μαθησιακοί στόχοι:** Η ανάπτυξη ικανοτήτων σε αυτό το σενάριο χωρίζεται σε τρεις τομείς:

    - **Γνώση:** Οι μαθητές αποκτούν την ικανότητα να εντοπίζουν αξιόπιστα **απειλές phishing και κακόβουλου λογισμικού** και να κατανοούν τα υποκείμενα μοτίβα κοινών στρατηγικών επίθεσης. Αυτό περιλαμβάνει επίσης τη γνώση διαφόρων τύπων επιθέσεων, όπως το spear phishing, η φαλαινοθηρία ή το ransomware.

    - **Δεξιότητες:** Θα μάθετε να αναλύετε κριτικά σενάρια πραγματικού κόσμου για να **εντοπίζετε ύποπτα στοιχεία** (όπως παραποιημένους συνδέσμους ή λανθασμένες διευθύνσεις email). Επιπλέον, εκπαιδεύουν την ικανότητα διατύπωσης **συγκεκριμένων ερωτήσεων σε μια τεχνητή νοημοσύνη** προκειμένου να εξαλειφθούν οι ασάφειες σε περίπτωση πιθανών επιθέσεων.

    - **Ικανότητες:** Οι εκπαιδευόμενοι έχουν τη δυνατότητα να εφαρμόσουν την ευαισθητοποίησή τους για την ασφάλεια στον κυβερνοχώρο σε **πραγματικά εργασιακά πλαίσια** . Μπορούν να δικαιολογήσουν τις αποφάσεις τους για την ασφάλεια με βάση τις γνώσεις που υποστηρίζονται από την τεχνητή νοημοσύνη και να αναπτύξουν υπεύθυνη συμπεριφορά στον ψηφιακό χώρο.

II. Εκπαιδευτικός Σχεδιασμός

- **Το «Εκπαιδευτικό Ερώτημα»: Η** κεντρική παιδαγωγική πρόκληση αυτού του σεναρίου είναι ότι οι εκπαιδευόμενοι – ειδικά εκείνοι που δεν έχουν σε βάθος υπόβαθρο πληροφορικής (όπως οι εκπαιδευόμενοι στις επιχειρήσεις ή τα οικονομικά) – συχνά δυσκολεύονται να εντοπίσουν **λεπτές ψηφιακές απειλές** και να κατανοήσουν το απαραίτητο τεχνικό λεξιλόγιο. Το σενάριο απαντά στο ερώτημα: **Πώς μπορεί να βελτιωθεί η κατανόηση πολύπλοκων εννοιών και ακρωνύμιων κυβερνοασφάλειας μέσω ενός διαδραστικού, ασφαλούς περιβάλλοντος μάθησης;**. Η χρήση τεχνητής νοημοσύνης και avatar λύνει αυτό το πρόβλημα **παρέχοντας συνεπή και αφοσιωμένη μεταφορά γνώσης**, επιτρέποντας την ασφαλή προσομοίωση σεναρίων επίθεσης και μειώνοντας τη γνωστική επιβάρυνση των καθοδηγούμενων αλληλεπιδράσεων.

- **Διδακτικό πλαίσιο:** Το σενάριο είναι σταθερά εδραιωμένο στα ευρωπαϊκά πλαίσια ικανοτήτων **DigComp 2.2** και **DigCompEdu**, ειδικά στους τομείς της πληροφοριακής παιδείας, της ασφάλειας και της επίλυσης προβλημάτων. Στο πλαίσιο του **μοντέλου SAMR,** η μονάδα εκμάθησης φτάνει στο επίπεδο της **«τροποποίησης» (επανασχεδιασμός),** καθώς η εργασία (η ανάλυση των επιθέσεων με χρήση ανατροφοδότησης τεχνητής νοημοσύνης σε πραγματικό χρόνο) δεν θα ήταν δυνατή στο ίδιο βάθος χωρίς αυτήν την τεχνολογία. Η επιλεγμένη μέθοδος διδασκαλίας ακολουθεί ένα **δομημένο μοντέλο 4 φάσεων**:

    1. **Προσανατολισμός:** Θεωρητική εισαγωγή μέσω γραμμικού avatar.
    2. **Παράδοση:** Ενεργή, διερευνητική μάθηση όπου οι εκπαιδευόμενοι ενεργούν ως **«ψηφιακοί ντετέκτιβ»** και διερευνούν πραγματικές περιπτώσεις (μηνύματα ηλεκτρονικού ψαρέματος, αναδυόμενα παράθυρα κακόβουλου λογισμικού).
    3. **Εκτίμηση:** Εργασίες επίλυσης προβλημάτων με άμεση ανατροφοδότηση AI.
    4. **Συμπέρασμα:** Συνεργατικός προβληματισμός στην ομάδα σχετικά με τα όρια και τις δυνατότητες υποστήριξης της τεχνητής νοημοσύνης.

- **Ο ρόλος του εκπαιδευτή/εκπαιδευτικού:** Σε αυτό το σενάριο, ο ρόλος του εκπαιδευτικού αλλάζει θεμελιωδώς από τον μοναδικό μεταδότη γνώσης στον **διευκολυντή, τον προπονητή και τον παιδαγωγικό σύμβουλο**. Τα συγκεκριμένα καθήκοντα περιλαμβάνουν:

    - **Εισαγωγή και ρύθμιση: Εισαγωγή** του θέματος και επεξήγηση του ρόλου του avatar.
    - **Υποστήριξη αλληλεπίδρασης AI:** Υποστήριξη των μαθητών στη διατύπωση στοχευμένων ερωτήσεων (**prompt engineering**) στο ChatGPT.
    - **Διασφάλιση ποιότητας:** Διεξαγωγή **ελέγχων αληθοφάνειας** για να διασφαλιστεί ότι οι μαθητές αμφισβητούν κριτικά τις πληροφορίες που δημιουργούνται από την τεχνητή νοημοσύνη και δεν υιοθετούν παρερμηνείες (ψευδαισθήσεις).
    - **Πάροχος ανατροφοδότησης:** Συντονισμός της τελικής συζήτησης και σύνδεση εικονικών εμπειριών με πραγματική εργασιακή πρακτική.

III. Τεχνολογική εφαρμογή

- **Λύση AI και avatar:** Σε αυτό το σενάριο, χρησιμοποιούνται **avatar που δημιουργούνται από 2D ή 3D AI**, τα οποία μεταφέρουν κυρίως **γραμμικό εκπαιδευτικό περιεχόμενο** με τη μορφή εκπαιδευτικών βίντεο. Το avatar λειτουργεί ως **ειδικός οπτικός οδηγός και δάσκαλος στη μαθησιακή διαδικασία**: εισάγει τις θεωρητικές έννοιες της ασφάλειας στον κυβερνοχώρο, εξηγεί τεχνικούς όρους και δείχνει γλαφυρά παραδείγματα μηνυμάτων ηλεκτρονικού ψαρέματος ή επιθέσεων κακόβουλου λογισμικού. Επιπλέον, το **ChatGPT αναλαμβάνει** τη λειτουργία ενός **διαδραστικού συνομιλητή και «ψηφιακού ντετέκτιβ»** με τον οποίο οι μαθητές μπορούν να εισέλθουν σε έναν ενεργό διάλογο για να αναλύσουν συγκεκριμένα σενάρια απειλών σε πραγματικό χρόνο.

- **Τεχνικά εργαλεία:** Για την υλοποίηση του σεναρίου χρησιμοποιείται μια επιλογή σύγχρονων εργαλείων «χαμηλού κατωφλίου» και τυπικού υλικού:

    - **Δημιουργία avatar: To Synthesia** ή το **HeyGen** χρησιμοποιούνται για τη γρήγορη δημιουργία των ομιλούντων avatar από σενάρια.

    - **Διαδραστική τεχνητή νοημοσύνη: Το ChatGPT** (βασισμένο στο GPT-4) χρησιμοποιείται για ανάλυση σεναρίων, απάντηση σε ερωτήσεις των συμμετεχόντων και βοήθεια στην «αντιμετώπιση προβλημάτων» συμβάντων ασφαλείας.

    - **Πλατφόρμα εκμάθησης (LMS):** Τα μαθήματα παρέχονται μέσω του **Learnpress**, το οποίο συγκεντρώνει τα διαδραστικά στοιχεία και τα βίντεο με δομημένο τρόπο.

    - **Υλικό: Οι** μαθητές χρησιμοποιούν τυπικούς **φορητούς υπολογιστές ή υπολογιστές** με σταθερές συνδέσεις στο διαδίκτυο.

    - **Πρόσθετοι πόροι:** Χρήση του **YouTube** για τη φιλοξενία των βίντεο avatar καθώς και ψηφιακών σημειωματάριων για αποθήκευση αποτελεσμάτων.

- **Προσέγγιση αναπήδησης λογισμικού:** Η δημιουργία περιεχομένου ακολουθεί μια **«προσέγγιση αναπήδησης λογισμικού» χαμηλού ορίου** που συνδυάζει τα δυνατά σημεία διαφορετικών εφαρμογών χωρίς την ανάγκη κωδικοποίησης. Η διαδικασία χωρίζεται στα ακόλουθα βήματα:

1. **Βελτιστοποίηση κειμένου:** Τα ακατέργαστα τεχνικά χειρόγραφα των εκπαιδευτών βελτιώνονται γλωσσικά με **το ChatGPT** και μετατρέπονται σε ένα διδακτικά ελκυστικό σενάριο.

2. **Παραγωγή εικόνας και βίντεο:** Τα βελτιστοποιημένα κείμενα φορτώνονται στο **Synthesia** για την απόδοση βίντεο συγχρονισμού χειλιών με έναν επιλεγμένο χαρακτήρα avatar.

3. **Διαδραστική συνένωση:** Τα τελικά βίντεο ενσωματώνονται στο LMS και συνδέονται με συγκεκριμένες **προτροπές για το ChatGPT.** Για παράδειγμα, οι μαθητές μπορούν να μεταβούν σε μια μελέτη περίπτωσης με τεχνητή νοημοσύνη αμέσως μετά από μια εξήγηση avatar για να εφαρμόσουν όσα έμαθαν στην πράξη.

IV. Αναλυτικό Σχέδιο Μαθήματος

Η παράδοση αυτής της ενότητας έχει σχεδιαστεί για να βάλει τους εκπαιδευόμενους στο ρόλο των **«ερευνητών κυβερνοασφάλειας».** Η διαδικασία χωρίζεται στις ακόλουθες τέσσερις φάσεις:

1. Εισαγωγή και προσανατολισμός

- **Διάρκεια:** 4 λεπτά.
- **Περιεχόμενο: Βασική** εισαγωγή στις έννοιες της κυβερνοασφάλειας καθώς και στον τρόπο αναγνώρισης των δύο πιο κοινών απειλών: **phishing** και **κακόβουλου λογισμικού**.
- **Δραστηριότητες:**
    - Οι μαθητές παρακολουθούν ένα εκπαιδευτικό βίντεο στο οποίο ένα **avatar που δημιουργήθηκε από AI** (δημιουργήθηκε με το Synthesia) εξηγεί τη σημασία της προστασίας του δικτύου και υπογραμμίζει τους κινδύνους των διαδικτυακών απατών.
    - Ο εκπαιδευτής (συντονιστής) παρουσιάζει τη συνεδρία, εξηγεί τον **ρόλο του avatar** ως ψηφιακού εκπαιδευτή και είναι διαθέσιμος για ερωτήσεις αρχικής κατανόησης.
- **Πολυμέσα:** Βίντεο avatar, που δημιουργήθηκαν με χρήση **Synthesia** ή **HeyGen**.

2. Εκτέλεση της εργασίας

- **Διάρκεια:** Ευέλικτη (μέρος της ενεργού φάσης ανάπτυξης).
- **Περιεχόμενα:** Πρακτική ανάλυση πραγματικών σεναρίων επιθέσεων για τον εντοπισμό τρωτών σημείων.
- **Δραστηριότητες:**
    - Οι μαθητές διεξάγουν μια **διαδραστική έρευνα χρησιμοποιώντας το ChatGPT.** Θα λάβετε συγκεκριμένες περιπτωσιολογικές μελέτες, όπως ένα ψεύτικο **αίτημα πληρωμής Netflix** ("support@netflix-pay.com") ή μια στημένη **αναδυόμενη ειδοποίηση** "Antivirus Defender 3000".
    - Η εργασία είναι να κάνετε στοχευμένες ερωτήσεις στο ChatGPT (π.χ. "Είδα ένα αναδυόμενο παράθυρο που ισχυρίζεται ότι ο υπολογιστής μου έχει μολυνθεί – είναι κακόβουλο λογισμικό;") για να επαληθεύσετε την απειλή.
    - Ο εκπαιδευτής βοηθά τους μαθητές με **άμεση μηχανική** και παρακολουθεί τις συζητήσεις σχετικά με τα χαρακτηριστικά που βρέθηκαν, όπως ύποπτες διευθύνσεις URL ή γραμματικά λάθη.
- **Πολυμέσα: ChatGPT** ως διαδραστικός βοηθός, διαδικτυακές σημειώσεις.

3. Αξιολόγηση / Ανασκόπηση

- **Διάρκεια:** 8 λεπτά.
- **Περιεχόμενα: Εφαρμογή** των γνώσεων που αποκτήθηκαν σε μια σύνθετη, πραγματική κατάσταση και προφορική αιτιολόγηση των αποφάσεων ασφαλείας.
- **Δραστηριότητες:**
    - **Σενάριο CEO:** Ένα avatar ενεργοποιεί μια εργασία όπου οι μαθητές λαμβάνουν ένα επείγον μήνυμα κειμένου από τον «Διευθύνοντα Σύμβουλο» που τους ζητά να κάνουν μια γρήγορη μεταφορά χρημάτων.
    - Οι εκπαιδευόμενοι πρέπει να εντοπίσουν τις αποκλίσεις (π.χ. μια ελαφρώς διαφορετική διεύθυνση ηλεκτρονικού ταχυδρομείου, όπως "CEO@yourcornpay.com"), να ζητήσουν συμβουλές από το ChatGPT και **να αιτιολογήσουν προφορικά τις ενέργειές τους στον εκπαιδευτή**.
    - Προαιρετικά, μπορεί να ξεκινήσει ένας εσωτερικός έλεγχος γνώσεων εισάγοντας την **εντολή "test" στη συνομιλία** για να ολοκληρώσετε ένα σύντομο κουίζ με άμεση ανατροφοδότηση.

4. Ολοκλήρωση της συνεδρίας

- **Διάρκεια:** 8 λεπτά.
- **Περιεχόμενα:** Σύνοψη των σημαντικότερων ευρημάτων και προβληματισμός σχετικά με τη μαθησιακή διαδικασία.
- **Δραστηριότητες:**
    - Σε μια συντονισμένη **ομαδική συζήτηση,** οι συμμετέχοντες θα προβληματιστούν σχετικά με την αποτελεσματικότητα της υποστήριξης AI και τους περιορισμούς της τεχνολογίας.
    - Ενοποιεί τις καθημερινές στρατηγικές προστασίας, όπως η ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων ή η αναφορά ύποπτων μηνυμάτων στην ομάδα πληροφορικής.
    - Η μεταφορά στην πράξη ολοκληρώνεται με τη συζήτηση της ανθρώπινης επαγρύπνησης ως την «καλύτερη άμυνα».

V. Πόροι και εξασφαλίσεις

1. Βίντεο

Η μεταφορά γνώσης βασίζεται σε **βίντεο avatar AI**. Αυτά όχι μόνο περιέχουν τεχνικές πληροφορίες, αλλά χρησιμοποιούν και αξιομνημόνευτες **αναλογίες** για να διευκρινίσουν τις έννοιες.

- **Φάση 1: Εξοικείωση με την ασφάλεια στον κυβερνοχώρο – Εντοπισμός phishing και κακόβουλου λογισμικού**
    - *Βασικό μήνυμα:* Ορίστε την ασφάλεια στον κυβερνοχώρο ως πρακτική για την προστασία συστημάτων, δικτύων και δεδομένων.
    - *Περιεχόμενο:* Εισαγωγή στο **phishing** (δόλιες απόπειρες κλοπής ευαίσθητων πληροφοριών) και στο **κακόβουλο λογισμικό** (κακόβουλο λογισμικό που καταστρέφει συστήματα).
    - *Κανόνες ασφαλείας:* Προειδοποίηση κατά του ανοίγματος συνημμένων από ύποπτες πηγές, της χρήσης ενημερωμένου λογισμικού προστασίας από ιούς και τακτικών αντιγράφων ασφαλείας.
    - *Αναλογία:* «Σκεφτείτε τον υπολογιστή σας ως **φρούριο**. Το phishing είναι σαν ένας κατάσκοπος που καλεί το φυλάκιο και προσποιείται ότι είναι στρατηγός για να ανοίξει την πύλη. Το κακόβουλο λογισμικό είναι σαν ένα **ξύλινο άλογο** που διεισδύει σε στρατιώτες που κλειδώνουν όλες τις πόρτες τη νύχτα».
- **Φάση 2: Κατανόηση και αναγνώριση των απειλών στον κυβερνοχώρο**
    - *Βασικό μήνυμα:* Οδηγίες για ενεργή εργασία ντετέκτιβ.
    - *Παραδείγματα:* Ανάλυση ενός πλαστού **αιτήματος πληρωμής Netflix** ("support@netflix-pay.com") και ενός παραποιημένου αναδυόμενου παραθύρου για το "Antivirus Defender 3000".
    - *Οδηγίες:* Οι μαθητές καλούνται να παρέχουν στο ChatGPT λεπτομερείς περιγραφές των παρατηρήσεών τους για να επαληθεύσουν τις απειλές.
- **Φάση 3: Δεχόμαστε επίθεση;!**
    - *Βασικό μήνυμα:* Εφαρμογή της γνώσης σε πολύπλοκα σενάρια.
    - *Μελέτη περίπτωσης 1:* Ένα επείγον μήνυμα κειμένου από τον Διευθύνοντα Σύμβουλο σχετικά με μια μεταφορά χρημάτων όπου η διεύθυνση email είναι ελαφρώς διαφορετική (π.χ. CEO@yourcornpay.com).
    - *Μελέτη περίπτωσης 2:* Μια επίθεση σε ένα διαδικτυακό παιχνίδι για πολλούς παίκτες που προκαλείται από μια υποτιθέμενη ενημέρωση ασφαλείας που έχει ως αποτέλεσμα την αλλαγή των κωδικών πρόσβασης.

2. Διαδραστικά στοιχεία

Το σενάριο χαρακτηρίζεται από υψηλό επίπεδο διαδραστικότητας που υπερβαίνει την απλή κατανάλωση βίντεο.

- **Διαδραστική έρευνα ChatGPT:** Οι μαθητές χρησιμοποιούν το ChatGPT ως **«ψηφιακό ντετέκτιβ».** Εισάγουν συγκεκριμένες παρατηρήσεις (π.χ. "Είδα ένα αναδυόμενο παράθυρο που ισχυρίζεται ότι ο υπολογιστής μου έχει μολυνθεί...") και λαμβάνουν μια αξιολόγηση της κατάστασης κινδύνου από την τεχνητή νοημοσύνη.
- **Κουίζ γνώσεων**: Μέσα στο περιβάλλον συνομιλίας, **ένα σύντομο κουίζ μπορεί να ξεκινήσει** εισάγοντας την εντολή "δοκιμή".
    - *Μορφή:* 4 ερωτήσεις με άμεση ανατροφοδότηση σχετικά με την πρόοδο της μάθησης.
- **Λεκτική αξιολόγηση:** Ένα avatar AI πυροδοτεί μια περίοδο προβληματισμού κατά την οποία οι μαθητές πρέπει να αιτιολογήσουν προφορικά τις αποφάσεις τους στον εκπαιδευτή.

3. Χαρτοφυλάκιο πολυμέσων

Για την υλοποίηση δημιουργήθηκε ένα χαρτοφυλάκιο διαφόρων ψηφιακών εργαλείων:

- **Εργαλεία avatar AI:** Δημιουργήστε τους οπτικούς δασκάλους με το **Synthesia** ή το **HeyGen**.
- **Πλατφόρμα εκμάθησης:** Η παροχή γίνεται μέσω του Learnpress LMS.
- **Φιλοξενία βίντεο:** Οι ολοκληρωμένες μαθησιακές ενότητες τεκμηριώνονται ως **βίντεο YouTube** , γεγονός που επιτρέπει την εύκολη ενσωμάτωση σε διάφορες πλατφόρμες ΕΕΚ.
- **Οπτικό υλικό:** Στιγμιότυπα οθόνης από απόπειρες phishing στον πραγματικό κόσμο και αναδυόμενα παράθυρα κακόβουλου λογισμικού χρησιμεύουν ως οπτικά σημεία αγκύρωσης κατά την εκτέλεση.