



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Ηλεκτρονική Μάθηση»
Ακαδημαϊκό έτος 2025-2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΟΥ ΚΩΝΣΤΑΝΤΑΚΗ ΓΕΩΡΓΙΟΥ
(Α.Μ.: 25037)

«e-Course: Αξιοποίηση της Μεθόδου SRL και Υποστηρικτικών Εργαλείων Τεχνητής Νοημοσύνης (AI) σε ένα STEAM Περιβάλλον Μάθησης για την Ανάπτυξη Δεξιοτήτων Κυβερνοασφάλειας σε Φοιτητές Τριτοβάθμιας Εκπαίδευσης»

«e-Course: Integrating the SRL Method and Supportive Artificial Intelligence (AI) Tools in a STEAM Learning Environment for Developing Cybersecurity Skills in Higher Education»

Επιβλέπουσα:

Κα. Φωτεινή Παρασκευά
Καθηγήτρια

Αθήνα, Σεπτέμβριος 2026

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Αυτή η Μεταπτυχιακή Διπλωματική Εργασία υποβάλλεται ως μερική εκπλήρωση των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών στην «Ηλεκτρονική Μάθηση» του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Δηλώνω υπεύθυνα ότι η συγκεκριμένη Μεταπτυχιακή Διπλωματική Εργασία έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει αξιολογηθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό.

Η εργασία αυτή έχοντας εκπονηθεί από εμένα, αντιπροσωπεύει τις προσωπικές μου απόψεις επί του θέματος. Οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης διπλωματικής αναφέρονται στο σύνολό τους, δίνοντας πλήρεις αναφορές στους συγγραφείς, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το Διαδίκτυο.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου. Σε κάθε περίπτωση, αναληθούς ή ανακριβούς δηλώσεως, υπόκειμαι στις συνέπειες που προβλέπονται από τις διατάξεις που προβλέπει η Ελληνική και Κοινοτική Νομοθεσία περί πνευματικής ιδιοκτησίας.

Ο ΔΗΛΩΝ

Ονοματεπώνυμο: Κωνσταντάκης Γεώργιος

Αριθμός Μητρώου: 25037

Υπογραφή:



ΠΕΡΙΛΗΨΗ

Στη σύγχρονη ψηφιακή εποχή, οι φοιτητές τριτοβάθμιας εκπαίδευσης αποτελούν ευάλωτη ομάδα απέναντι σε επιθέσεις phishing, καθώς οι παραδοσιακές εκπαιδευτικές προσεγγίσεις δεν καλύπτουν επαρκώς την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας. Για την κάλυψη του κενού αυτού, η παρούσα εργασία σχεδίασε και ανέπτυξε το ψηφιακό μάθημα «Phishing 360°: Από το Συναίσθημα στα Δεδομένα» στην πλατφόρμα Wix, θεμελιωμένο παιδαγωγικά στη θεωρία της Αυτορρυθμιζόμενης Μάθησης (SRL).

Οι ενότητες και οι δραστηριότητες του μαθήματος διαρθρώνονται στις τρεις φάσεις του μοντέλου: στην προπαρασκευαστική φάση οι φοιτητές θέτουν στόχους και στρατηγικές για τις δραστηριότητες κυβερνοασφάλειας, στην εκτελεστική φάση υλοποιούν τις δραστηριότητες, όπως την ανάλυση σεναρίων phishing, επιτηρώντας την πορεία τους, και στη φάση του αναστοχασμού αξιολογούν το αποτέλεσμα, εντοπίζοντας τους παράγοντες επίτευξης ή μη των στόχων τους.

Το πλαίσιο SRL εντάσσεται σε περιβάλλον μάθησης STEAM, το οποίο συνδυάζει τα πεδία Science, Technology, Engineering, Arts και Mathematics, καλλιεργώντας τη δημιουργικότητα, την επίλυση προβλημάτων και τη συνεργασία μέσα από αυθεντικά σενάρια (case studies) phishing. Παράλληλα, υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης, όπως ψηφιακός βοηθός (AI avatar), ενισχύουν την καθοδήγηση των φοιτητών.

Η εργασία αποτελεί πρόταση σχεδιασμού και δεν περιλαμβάνει εφαρμογή και αξιολόγηση σε πραγματικό δείγμα φοιτητών. Ωστόσο, παρουσιάζεται μεθοδολογικό πλαίσιο για τη μελλοντική αξιολόγησή της, με τρία ερευνητικά ερωτήματα σχετικά με τη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση και την κατανόηση της οπτικής των συνεργατών. Η συμβολή της μελέτης έγκειται στη δημιουργία παιδαγωγικού πλαισίου που συνδυάζει την Αυτορρυθμιζόμενη Μάθηση, το STEAM και υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης, για την καλλιέργεια δεξιοτήτων κυβερνοασφάλειας στην τριτοβάθμια εκπαίδευση.

Λέξεις-Κλειδιά: Αυτορρυθμιζόμενη Μάθηση (SRL), STEAM εκπαίδευση, κυβερνοασφάλεια, phishing, τεχνητή νοημοσύνη στην εκπαίδευση, ψηφιακό μάθημα (e-course), τριτοβάθμια εκπαίδευση.

ABSTRACT

In the contemporary digital era, higher education students constitute a vulnerable group against phishing attacks, as traditional educational approaches do not adequately address the development of cybersecurity skills. To address this gap, the present thesis designed and developed the digital course «Phishing 360°: From Emotion to Data» on the Wix platform, pedagogically grounded in the theory of Self-Regulated Learning (SRL).

The units and activities of the course are structured around the three phases of the model: in the forethought phase, students set goals and strategies for the cybersecurity activities; in the performance phase, they carry out the activities, such as the analysis of phishing scenarios, monitoring their progress; and in the self-reflection phase, they evaluate the outcome, identifying the factors of achievement or non-achievement of their goals.

The SRL framework is embedded within a STEAM learning environment, which combines the fields of Science, Technology, Engineering, Arts and Mathematics, cultivating creativity, problem-solving and collaboration through authentic scenarios (case studies) of phishing. In parallel, supportive Artificial Intelligence tools, such as a digital assistant (AI avatar), enhance the guidance of students.

The thesis constitutes a design proposal and does not include implementation and evaluation on an actual sample of students. However, a methodological framework is presented for its future evaluation, with three research questions concerning cognitive engagement, metacognitive monitoring and perspective taking. The contribution of the study lies in the creation of a pedagogical framework that combines Self-Regulated Learning, STEAM and supportive Artificial Intelligence tools, for the cultivation of cybersecurity skills in higher education.

Keywords: Self-Regulated Learning (SRL), STEAM education, cybersecurity, phishing, artificial intelligence in education, digital course (e-course), higher education.

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο, θα ήθελα να ευχαριστήσω τους ανθρώπους που με συνόδευσαν σε αυτή την πορεία.

Καταρχάς, οφείλω ένα μεγάλο ευχαριστώ στην επιβλέπουσα καθηγήτριά μου, κα. Φωτεινή Παρασκευά, για την εμπιστοσύνη που μου έδειξε από την αρχή και για την ουσιαστική καθοδήγησή της σε κάθε στάδιο αυτής της εργασίας, αλλά και σε όλη τη διάρκεια του μεταπτυχιακού. Η υποστήριξή της δεν με βοήθησε μόνο να ολοκληρώσω αυτή τη μελέτη, αλλά να εξελιχτώ ουσιαστικά, τόσο σε επιστημονικό όσο και σε προσωπικό επίπεδο.

Δεν θα μπορούσα επίσης να παραλείψω τη συμβολή και των υπόλοιπων καθηγητών του Προγράμματος Μεταπτυχιακών Σπουδών, και συγκεκριμένα των κ. Δ. Σάμψων, κ. Σ. Ρετάλη, κ. Π. Καμπύλη και κ. Δ. Γκότζο, οι οποίοι με εφοδίασαν με πολύτιμες γνώσεις, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, συμβάλλοντας σημαντικά στην ακαδημαϊκή αλλά και προσωπική μου πορεία.

Ένα ακόμη μεγάλο ευχαριστώ ανήκει στους γονείς μου, Κωνσταντίνο και Ιωάννα, στον αδερφό μου, Μάρκο, τη νύφη μου Ελευθερία και την ανιψιά μου Ιωάννα που με στήριξαν αδιάκοπα όλα αυτά τα χρόνια. Χωρίς την παρουσία και τη βοήθειά τους, αυτή η προσπάθεια θα ήταν πολύ πιο δύσκολη.

Τέλος, ένα ευχαριστώ σε όσους στάθηκαν δίπλα μου, με τον δικό τους τρόπο, σε αυτό το ταξίδι.

ΠΕΡΙΕΧΟΜΕΝΑ

Συντομογραφίες	13
ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ	15
1.1 Θεωρητική Θεμελίωση της Διπλωματικής Εργασίας.....	15
1.2 Παρουσίαση της Προβληματικής	16
1.3 Στόχος της Διπλωματικής Εργασίας	21
1.4 Καινοτομία της Διπλωματικής Εργασίας	21
1.5 Ερευνητικά Ερωτήματα	22
1.6 Γενική Επισκόπηση της Μεθοδολογίας.....	23
1.7 Οργάνωση της Διπλωματικής Εργασίας.....	24
ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ.....	26
2.1 Εισαγωγή	26
2.2 Αυτορρυθμιζόμενη Μάθηση (SRL).....	26
2.2.1 Κυκλικό μοντέλο του Zimmerman.....	27
2.3 Δείκτες Αξιολόγησης.....	29
2.3.1 Γνωστική Εμπλοκή (cognitive engagement)	29
2.3.2 Μεταγνωστική Παρακολούθηση (metacognitive monitoring).....	31
2.3.3 Κατανόηση της Οπτικής των Άλλων (perspective-taking)	33
2.4 STEAM	36
2.4.1 Ιστορία και εξέλιξη του STEM/STEAM	36
2.4.2 Παιδαγωγική αξία της STEAM	37
2.4.3 STEAM και Κυβερνοασφάλεια.....	38
2.5 Συνεργατικές Στρατηγικές Μάθησης	38
2.5.1 Jigsaw	38
2.5.2 Think-Pair-Share.....	39
2.5.3 Πυραμίδα.....	39
2.5.4 Καταιγισμός Ιδεών (Brainstorming).....	39
2.6 Τεχνικές Μάθησης	39
2.6.1 SCAMPER	39
2.6.2 Think-Aloud.....	40

2.7 Περιβάλλον e-Learning.....	40
2.7.1 Πλατφόρμα Wix	40
2.7.2 Ψηφιακά εργαλεία	40
2.8 Εργαλεία Τεχνητής Νοημοσύνης	42
2.9 Περίληψη	44
ΚΕΦΑΛΑΙΟ 3: ΜΕΘΟΔΟΛΟΓΙΑ	45
3.1 Στόχος ερευνητικής προσέγγισης	45
3.2 Εννοιολογικοί και λειτουργικοί Ορισμοί.....	45
3.3 Τα Ερευνητικά Ερωτήματα	49
3.4 Η περιγραφή της διαδικασίας της έρευνας	49
3.5 Επιλογή στατιστικών κριτηρίων για τις αναλύσεις	55
3.6 Το δείγμα μελέτης.....	56
3.6.1 Οι συμμετέχοντες	56
3.6.2 Οι περιορισμοί της έρευνας	56
3.7 Εκπαιδευτικό υλικό και ροή.....	57
3.7.1 Συνολική ροή του e-course (Μακροσενάριο)	57
3.7.2 Ανάλυση Εκπαιδευτικού Σχεδιασμού (Μικροσενάριο)	60
3.8 Ερευνητικά Περιβάλλοντα.....	125
3.9 Τα ψηφιακά μέσα της έρευνας	125
3.10 Τα Ερευνητικά Μέσα	126
3.10.1 Έλεγχος Δεξιοτήτων (Αρχικός/Τελικός).....	126
3.10.2 Ερωτηματολόγιο Αναστοχασμού	126
3.10.3 Ερωτηματολόγιο Αξιολόγησης Σχεδίου Δράσης.....	126
3.10.4 Ρουμπρίκα Αξιολόγησης Παραδοτέων	127
3.11 Αναμενόμενα Ευρήματα.....	127
ΚΕΦΑΛΑΙΟ 4: ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ.....	128
4.1 Σκοπός του Κεφαλαίου.....	128
4.2 Επίπεδο χρήσης της Τεχνητής Νοημοσύνης (AI Assessment Scale – AIAS)	128
4.3 Συνοπτικός Πίνακας Χρήσης της Τεχνητής Νοημοσύνης.....	129

4.4 Αναλυτική περιγραφή της χρήσης της Τεχνητής Νοημοσύνης	130
4.4.1 Δημιουργία Εικόνων (ChatGPT).....	130
4.4.2 Δημιουργία avatar (Hedra AI)	130
4.4.3 Δημιουργία διαδραστικών εφαρμογών (Lovable AI)	131
4.4.4 Δημιουργία διαδραστικών παρουσιάσεων (Base44 AI)	131
4.4.5 Δημιουργία Βίντεο (NotebookLM).....	132
4.4.6 Αφήγηση (Google AI Studio)	132
4.4.7 Γλωσσική Επιμέλεια (Claude AI)	132
4.5 Ενδεικτικά Prompts	133
4.5.1 Lovable AI	133
4.5.2 NotebookLM	134
4.5.3 Base44 AI	135
4.5.4 ChatGPT	136
4.6 Ανάλυση / Τεκμηρίωση των Αποφάσεων και Παρεμβάσεων.....	136
4.7 Κριτική Αποτίμηση της Χρήσης της Τεχνητής Νοημοσύνης	137
ΚΕΦΑΛΑΙΟ 5: ΑΝΑΜΕΝΟΜΕΝΑ ΑΠΟΤΕΛΕΣΜΑΤΑ & ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ.....	139
5.1 Επισκόπηση Αναμενόμενων Ευρημάτων.....	139
5.2 Συζήτηση - Συμπεράσματα, Περαιτέρω Μελέτη και Έρευνα.....	139
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	141
ΠΑΡΑΡΤΗΜΑ.....	148
A1: Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων (Φάση Forethought).	148
A2: Ερωτηματολόγιο Skills Self-Check (Pre) (Φάση Forethought).	151
A3: Ετεροαξιολόγηση διαγραμμάτων (Ενότητα Engineering-Φάση Performance).	155
A4: Ετεροαξιολόγηση γραφιστικών (Ενότητα Arts-Φάση Performance).	158
A5: Ετεροαξιολόγηση γραφημάτων (Ενότητα Mathematics-Φάση Performance).	160
A6: Ερωτηματολόγιο Αναστοχασμού (Φάση Self-Reflection).	163
A7: Ερωτηματολόγιο Αξιολόγησης σχεδίου δράσης (Φάση Self-Reflection).....	165
A8: Ρουμπρίκα αξιολόγησης παραδοτέων (Google Classroom).....	169
A9: Checklist (Ενότητα Mathematics-Φάση Performance).	170
Σύνδεσμος e-course :	170

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1: Δείκτες Γνωστικής Εμπλοκής	29
Πίνακας 2: Λειτουργίες Μεταγνωστικής Παρακολούθησης ανά Φάση και Αντικείμενο.....	32
Πίνακας 3: Δείκτες Κατανόησης της Οπτικής των Άλλων.....	34
Πίνακας 4: Ορισμός και ταξινόμηση των κλάδων στην προσέγγιση STEAM	37
Πίνακας 5: Εννοιολογικός και λειτουργικός ορισμός της Γνωστικής Εμπλοκής.....	46
Πίνακας 6: Εννοιολογικός και λειτουργικός ορισμός της Μεταγνωστικής Παρακολούθησης	47
Πίνακας 7: Εννοιολογικός και Λειτουργικός Ορισμός της κατανόησης της οπτικής των άλλων.....	48
Πίνακας 8: Κωδικοποιημένοι μαθησιακοί στόχοι του e-course	51
Πίνακας 9: Αντιστοίχιση στόχων με φάσεις εφαρμογής και ερευνητικά ερωτήματα.....	52
Πίνακας 10 Ανάλυση Φάσης I (Forethought)	66
Πίνακας 11: Ανάλυση Ενότητας Science (Φάση II Performance).....	75
Πίνακας 12: Ανάλυση Ενότητας Technology (Φάση II Performance).....	84
Πίνακας 13: Ανάλυση Ενότητας Engineering (Φάση II Performance)	92
Πίνακας 14 : Ανάλυση Ενότητας Arts (Φάση II Performance)	102
Πίνακας 15: Ανάλυση Ενότητας Mathematics (Φάση II Performance).....	110
Πίνακας 16: Ανάλυση Φάσης III (Self-Reflection).....	117
Πίνακας 17: Συνοπτικός Πίνακας Χρήσης της Τεχνητής Νοημοσύνης.....	129

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1: Το κυκλικό μοντέλο των φάσεων SRL.....	28
Σχήμα 2: Βήματα ερευνητικού σχεδιασμού.....	50
Σχήμα 3: Ο κύκλος της Αυτορρυθμιζόμενης Μάθησης στο e-course.....	53
Σχήμα 4: Εκπαιδευτικός σχεδιασμός e-course	61
Σχήμα 5: Ροή δραστηριοτήτων Φάσης I (Forethought).....	66
Σχήμα 6: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Science.....	74
Σχήμα 7: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Technology	83
Σχήμα 8: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Engineering.....	92
Σχήμα 9: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Arts.....	102
Σχήμα 10: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Mathematics	110
Σχήμα 11: Ροή δραστηριοτήτων Φάσης III (Self-Reflection).....	116

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Εισαγωγική Σελίδα (Home Page).....	62
Εικόνα 2: Timeline.....	63
Εικόνα 3: Road Map.....	65
Εικόνα 4: Εισαγωγικό Βίντεο (Φάση Forethought).....	67
Εικόνα 5: Threat Map	68
Εικόνα 6: Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων.....	69
Εικόνα 7: Καθορισμός Στόχων (Φάση Forethought).....	71
Εικόνα 8: Καταιγισμός Ιδεών	71
Εικόνα 9: Word Check (Σταυρόλεξο).....	72
Εικόνα 10: Κουίζ Γνώσεων (Forethought).....	73
Εικόνα 11: Εισαγωγικό βίντεο: «Η ψυχολογία της Κοινωνικής Μηχανικής»	76
Εικόνα 12: Διαδραστικός εννοιολογικός χάρτης	77
Εικόνα 13: Διαχείριση Χρόνου & Ρυθμού Μάθησης.....	78
Εικόνα 14: Simulation Spear-phishing Case Study I.....	79
Εικόνα 15: Δραστηριότητα Ανάλυσης ύποπτου email (Πυραμίδα).....	80
Εικόνα 16: Κουίζ Κατανόησης θεωρίας (Science).....	82
Εικόνα 17: Θεωρητική Παρουσίαση Ενότητας Technology	85
Εικόνα 18: Interactive Book (Lumi).....	86
Εικόνα 19: Μελέτη Περιεχομένου & Εξάσκηση (Technology)	87
Εικόνα 20: Τεχνική Επιθεώρηση Case Study II	88
Εικόνα 21: Επιθεώρηση URL με τη στρατηγική Think-Pair-Share	89
Εικόνα 22: Κουίζ Κατανόησης θεωρίας (Technology)	90
Εικόνα 23: Καθορισμός νέων στόχων	91
Εικόνα 24: Εισαγωγικό Βίντεο (Engineering).....	93
Εικόνα 25: Διάγραμμα Ακολουθίας	94

Εικόνα 26: Ατομική Μελέτη (Engineering).....	95
Εικόνα 27: Ανάθεση σε Ομάδες Ειδικών (Jigsaw)	96
Εικόνα 28: Αναζήτηση διευκρινήσεων στο Claude AI	97
Εικόνα 29: Δραστηριότητα Οπτικής Επίθεσης (Case Study III)	98
Εικόνα 30: Κουίζ Κατανόησης Θεωρίας (Engineering).....	100
Εικόνα 31: Καταγραφή Μαθησιακής Πορείας με το εργαλείο Evernote	101
Εικόνα 32: Θεωρητική Επίδειξη (Arts).....	103
Εικόνα 33: Ατομική Μελέτη (Arts).....	105
Εικόνα 34: Σενάριο Οπτικής Εξαπάτησης	106
Εικόνα 35: Δραστηριότητα Ανάλυσης Σχεδιασμού (Think-Pair-Share)	107
Εικόνα 36: Κουίζ Κατανόησης Θεωρίας (Arts).....	109
Εικόνα 37: Θεωρητική Παρουσίαση (Mathematics).....	111
Εικόνα 38: Ιδεοθύελλα νέων δεικτών (Τεχνική SCAMPER).....	113
Εικόνα 39: Ιστόγραμμα Total_Risk (SPSS).....	114
Εικόνα 40: Εισαγωγικό Βίντεο (Self-Reflection)	118
Εικόνα 41: Escape Room (Genially).....	119
Εικόνα 42: Ερωτηματολόγιο Αναστοχασμού	120
Εικόνα 43: Σχεδιασμός Επόμενων Βημάτων	121
Εικόνα 44: Ερωτηματολόγιο Αξιολόγησης Σχεδίου Δράσης	122
Εικόνα 45: Παραλαβή Πιστοποιητικού Παρακολούθησης	123
Εικόνα 46: Communication Station	124

Συντομογραφίες

Συντομογραφία	Επεξήγηση
AIAS	AI Assessment Scale
H5P	HTML5 Package
HITL	Human in the Loop
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Interactive, Constructive, Active, Passive
KPI	Key Performance Indicator
LMS	Learning Management System
PDF	Portable Document Format
PSD2	Payment Services Directive 2
RQ	Research Question (Ερευνητικό Ερώτημα)
RSA	Rivest–Shamir–Adleman
SLD	Second-Level Domain
SMS/MMS	Short/Multimedia Messaging Service
SPSS	Statistical Package for the Social Sciences
SRL	Self-Regulated Learning (Αυτορρυθμιζόμενη Μάθηση)

Συντομογραφία	Επεξήγηση
STEAM	Science, Technology, Engineering, Arts, Mathematics
STEM	Science, Technology, Engineering, Mathematics
TLD	Top-Level Domain
URL	Uniform Resource Locator
ΚΣ	Κοινωνικό-Συναισθηματικός Στόχος
ΜΓΣ	Μεταγνωστικός Στόχος
ΜΔΕ	Μεταπτυχιακή Διπλωματική Εργασία
ΜΣ	Μαθησιακός Στόχος

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Θεωρητική Θεμελίωση της Διπλωματικής Εργασίας

Οι συνεχείς κοινωνικές και τεχνολογικές μεταβολές έχουν διαφοροποιήσει τις απαιτήσεις της σύγχρονης εκπαίδευσης. Πέρα από την απόκτηση γνώσεων σε επιμέρους γνωστικά αντικείμενα, οι εκπαιδευόμενοι χρειάζεται να αναπτύσσουν ένα ευρύτερο σύνολο ικανοτήτων και στάσεων, ώστε να μπορούν να ανταποκρίνονται σε σύνθετες και μεταβαλλόμενες συνθήκες. Οι ικανότητες αυτές χαρακτηρίζονται ως δεξιότητες του 21^{ου} αιώνα και έχουν εφαρμογή σε διαφορετικά μαθησιακά, επαγγελματικά και κοινωνικά περιβάλλοντα (Voogt & Roblin, 2012).

Οι δεξιότητες του 21^{ου} αιώνα συνδέονται στενά με τις ψηφιακές δεξιότητες, στις οποίες περιλαμβάνονται η διαχείριση πληροφορίας, η επικοινωνία, η συνεργατικότητα, η δημιουργική σκέψη, η κριτική ικανότητα και η επίλυση προβλημάτων. Επιπρόσθετα, εντάσσονται σε αυτές η ηθική επίγνωση, η προσαρμοστικότητα, η ικανότητα αυτοκαθοδήγησης και η διαρκής μάθηση (Van Laar et al., 2017).

Οι ψηφιακές, πληροφοριακές και επικοινωνιακές δεξιότητες αφορούν την ικανότητα των εκπαιδευομένων να αποκτούν πρόσβαση στην ψηφιακή πληροφορία, να την αξιολογούν, να τη διαμοιράζονται και να τη μεταδίδουν αποτελεσματικά (Siddiq et al., 2016).

Με βάση τα παραπάνω, ως θεωρητικό θεμέλιο της παρούσας εργασίας ορίζεται η Αυτορρυθμιζόμενη Μάθηση (Self-Regulated Learning-SRL). Σύμφωνα με αυτήν, ο εκπαιδευόμενος συμμετέχει ενεργά στη διαχείριση της μάθησής του, θέτοντας στόχους, παρακολουθώντας την πορεία του και αναστοχαζόμενος πάνω σε αυτήν (Zimmerman, 2002). Η συγκεκριμένη θεωρία αποτελεί το βασικό παιδαγωγικό πλαίσιο για την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας στην παρούσα διπλωματική εργασία.

Στη σύγχρονη ψηφιακή πραγματικότητα, η ανάπτυξη ψηφιακών δεξιοτήτων συνδέεται άμεσα με την κυβερνοασφάλεια. Η ασφαλής αξιοποίηση της τεχνολογίας αποτελεί βασική προϋπόθεση για τη συμμετοχή των φοιτητών σε ψηφιακά περιβάλλοντα. Ειδικότερα στο ακαδημαϊκό πλαίσιο, η κυβερνοασφάλεια δεν περιορίζεται στις τεχνικές γνώσεις, αλλά περιλαμβάνει και την επίγνωση, την υπεύθυνη συμπεριφορά και την ικανότητα αναγνώρισης απειλών, όπως το phishing και η κοινωνική μηχανική.

Οι φοιτητές αποτελούν ιδιαίτερα ευάλωτη ομάδα, επειδή χρησιμοποιούν καθημερινά ψηφιακές υπηρεσίες, διαδικτυακές πλατφόρμες και ακαδημαϊκούς λογαριασμούς. Για τον λόγο αυτό, η ενσωμάτωση της κυβερνοασφάλειας στην εκπαιδευτική διαδικασία κρίνεται απαραίτητη (Khader et al., 2021). Μελέτη σε ακαδημαϊκό περιβάλλον έδειξε ότι οι χρήστες εξακολουθούν να είναι ευάλωτοι σε μηνύματα phishing, ακόμη και όταν διαθέτουν υψηλό επίπεδο τεχνολογικής εξοικείωσης. Το συγκεκριμένο εύρημα αναδεικνύει την ανάγκη για εκπαιδευτικές παρεμβάσεις και δράσεις ενημέρωσης σχετικά με το phishing και την ασφαλή χρήση ψηφιακών υπηρεσιών (Diaz et al., 2020).

1.2 Παρουσίαση της Προβληματικής

Η ευρεία χρήση ψηφιακών υπηρεσιών, διαδικτυακών πλατφορμών, ηλεκτρονικού ταχυδρομείου και ακαδημαϊκών λογαριασμών στην τριτοβάθμια εκπαίδευση καθιστά την κυβερνοασφάλεια κρίσιμο πεδίο ανάπτυξης δεξιοτήτων για τους φοιτητές.

Το phishing αποτελεί χαρακτηριστική μορφή απειλής, επειδή δεν εκμεταλλεύεται μόνο τεχνικές αδυναμίες, αλλά και ανθρώπινους παράγοντες. Σε αυτούς περιλαμβάνονται η περιορισμένη γνώση, η έλλειψη πόρων και υποστήριξης, η χαμηλή αντίληψη του κινδύνου, οι παγιωμένες συμπεριφορές στον χώρο της εργασίας και ο εφησυχασμός των χρηστών. Η ανάπτυξη δεξιοτήτων κυβερνοασφάλειας δεν αρκεί να βασίζεται μόνο στη μετάδοση γνώσεων. Χρειάζεται επίσης να καλλιεργεί την κριτική αξιολόγηση, τη λήψη αποφάσεων και τον αναστοχασμό κατά την επεξεργασία ύποπτων ψηφιακών μηνυμάτων (Desolda et al., 2022; Diaz et al., 2020; Waqas et al., 2023).

Η εκπαίδευση απέναντι στο phishing φαίνεται ωστόσο να είναι πιο ουσιαστική όταν δεν περιορίζεται σε γενική ενημέρωση, αλλά περιλαμβάνει ενεργές μορφές μάθησης, πρακτική εξάσκηση, ανατροφοδότηση και σύνδεση της γνώσης με πραγματικές ή προσομοιωμένες καταστάσεις. Η ανάγκη αυτή συνδέεται άμεσα με τον σχεδιασμό μαθησιακών δραστηριοτήτων στις οποίες οι εκπαιδευόμενοι αναλύουν σενάρια, εντοπίζουν ύποπτες ενδείξεις κοινωνικής μηχανικής, αξιολογούν την αξιοπιστία ψηφιακών μηνυμάτων και αναστοχάζονται πάνω στις αποφάσεις τους (Arachchilage & Love, 2014; Kumaraguru et al., 2007; Marshall et al., 2024).

Σε αυτή τη βάση, η αυτορρυθμιζόμενη μάθηση προσφέρει ένα παιδαγωγικό πλαίσιο μέσα στο οποίο ο εκπαιδευόμενος αναλαμβάνει ενεργό ρόλο στη ρύθμιση της μάθησης και της συμπεριφοράς του. Η διαδικασία αυτή περιλαμβάνει τον καθορισμό στόχων, την επιλογή κατάλληλων στρατηγικών, τον έλεγχο της μαθησιακής πορείας και την αποτίμηση των ενεργειών που πραγματοποιήθηκαν (Zimmerman, 2002).

Το μοντέλο του Zimmerman περιγράφει την Αυτορρυθμιζόμενη Μάθηση ως κυκλική διαδικασία τριών σταδίων: τη φάση της προετοιμασίας, που εμπεριέχει την ανάλυση του έργου, τη στοχοθεσία και τον στρατηγικό σχεδιασμό, τη φάση της εκτέλεσης, κατά την οποία εφαρμόζονται στρατηγικές αυτοελέγχου και αυτοπαρακολούθησης, και το στάδιο του αναστοχασμού όπου πραγματοποιείται αυτοαξιολόγηση της μαθησιακής πορείας, εντοπισμός δυσκολιών και σημείων προς βελτίωση, και ανάλογη προσαρμογή των επόμενων μαθησιακών ενεργειών (Panadero, 2017; Zimmerman, 2002).

Στα διαδικτυακά περιβάλλοντα μάθησης, η SRL αποκτά καθοριστική σημασία, δεδομένου ότι οι εκπαιδευόμενοι χρειάζεται να οργανώνουν και να ρυθμίζουν με αυτονομία τον χρόνο, τις μεθόδους και τον ρυθμό μελέτης τους.

Στα διαδικτυακά περιβάλλοντα η ικανότητα αυτορρύθμισης επηρεάζει ουσιαστικά τη μαθησιακή πορεία. Για τη διερεύνησή της έχει σχεδιαστεί το εργαλείο Online Self-Regulated Learning Questionnaire (OSLQ), το οποίο εξετάζει τη στοχοθεσία, την οργάνωση του περιβάλλοντος μελέτης, τις στρατηγικές υλοποίησης του έργου, τη διαχείριση του χρόνου, την αναζήτηση βοήθειας και την αυτοαξιολόγηση (Barnard et al., 2009). Αντίστοιχα, μία συστηματική ανασκόπηση στην τριτοβάθμια διαδικτυακή εκπαίδευση έδειξε ότι οι φοιτητές που έχουν καλύτερη μαθησιακή επίδοση είναι αυτοί που αξιοποιούν συγκεκριμένες στρατηγικές διαχείρισης χρόνου και ρυθμού μάθησης, έχουν αναπτύξει μεταγνωστικές ικανότητες και ασκούν κριτική πάνω στη μαθησιακή τους πορεία (Broadbent & Poon, 2015).

Η σύνδεση της αυτορρύθμισης με την κυβερνοασφάλεια γίνεται πιο σαφής όταν εξεταστεί ο τρόπος με τον οποίο οι εκπαιδευόμενοι επεξεργάζονται πληροφορίες σε πραγματικές συνθήκες phishing. Σε πρόσφατη μελέτη εξετάζεται η σχέση της αυτορρύθμισης, της επεξεργασίας πληροφορίας και της ευαλωτότητας σε phishing επιθέσεις, με τα ευρήματα να δείχνουν ότι η επίδραση της αυτορρύθμισης περνά έμμεσα μέσα από τον τρόπο επεξεργασίας πληροφορίας, είτε συστηματικό είτε ευρετικό, ο οποίος τελικά καθορίζει σε μεγάλο βαθμό πόσο είναι ευάλωτος ο χρήστης σε επιθέσεις phishing (Waqas et al., 2023).

Στο πλαίσιο αυτό, η SRL φαίνεται να δίνει στους φοιτητές τη δυνατότητα να θέτουν στόχους, να παρατηρούν τον τρόπο με τον οποίο σκέφτονται καθώς αναλύουν ύποπτα μηνύματα, να σταθμίζουν τα δεδομένα προτού καταλήξουν σε μια κρίσιμη απόφαση, και να αναστοχάζονται πάνω στις επιλογές τους όταν οι δραστηριότητες έχουν πλέον ολοκληρωθεί (Waqas et al., 2023; Zimmerman, 2002).

Η υιοθέτηση ενός STEAM περιβάλλοντος μάθησης ανταποκρίνεται στην ανάγκη διεπιστημονικής προσέγγισης σύνθετων ζητημάτων, καθώς το STEAM συνδυάζει τα πεδία Science, Technology, Engineering, Arts και Mathematics, επιδιώκοντας τη διασύνδεσή τους μέσω δραστηριοτήτων που καλλιεργούν τη δημιουργικότητα, την επίλυση προβλημάτων, την καινοτομία, τη συνεργασία και την επικοινωνία. Η σχετική βιβλιογραφία επισημαίνει ότι το STEAM δεν αποτελεί απλή προσθήκη των τεχνών στα STEM πεδία, αλλά ένα πλαίσιο που μπορεί να οργανωθεί με διεπιστημονικό, διαθεματικό ή ενσωματωμένο τρόπο, ανάλογα με τον σχεδιασμό της μαθησιακής δραστηριότητας (Perignat & Katz-Buonincontro, 2019). Το εννοιολογικό μοντέλο διδασκαλίας STEAM αναδεικνύει ότι η μαθησιακή διαδικασία δεν οφείλει να επικεντρώνεται αποκλειστικά στη μετάδοση γνώσεων προς μία κατεύθυνση. Αντίθετα, οφείλει να διασυνδέει διαφορετικά γνωστικά πεδία, να θεμελιώνεται σε αυθεντικά προβλήματα και να ενδυναμώνει την ενεργό συμμετοχή των εκπαιδευομένων (Quigley et al., 2017).

Η σύνδεση του STEAM με την Αυτορρυθμιζόμενη Μάθηση είναι σημαντική, επειδή τα STEAM έργα προϋποθέτουν διερεύνηση, σχεδιασμό, δημιουργία, επίλυση προβλημάτων και αναστοχασμό. Οι εκπαιδευόμενοι δεν αρκεί να απομνημονεύουν πληροφορίες, αλλά χρειάζεται να εφαρμόζουν στρατηγικές μάθησης, να συνεργάζονται, να κρίνουν τις επιλογές τους και να ενισχύουν στοιχεία της αυτορρύθμισης, όπως η αυτοαποτελεσματικότητα, το ενδιαφέρον και η παρακολούθηση της μαθησιακής τους πορείας (López Carrillo et al., 2024). Ωστόσο, η εφαρμογή του STEAM σε συνδυασμό με την Αυτορρυθμιζόμενη Μάθηση παραμένει πεδίο που χρειάζεται περαιτέρω διερεύνηση. Η σχετική βιβλιογραφία δείχνει ότι υπάρχει αυξημένο ενδιαφέρον για τη σύνδεση των STEAM δραστηριοτήτων με τη μεταγνώση, την αυτορρύθμιση και την ακαδημαϊκή επίδοση. Αναδεικνύεται ωστόσο η ανάγκη περαιτέρω διερεύνησης του τρόπου με τον οποίο οι μαθησιακές δραστηριότητες, τα εργαλεία αξιολόγησης και τα ψηφιακά περιβάλλοντα μπορούν να υποστηρίξουν ουσιαστικά την καλλιέργεια δεξιοτήτων SRL σε πλαίσια STEAM (García-Senín et al., 2022; López Carrillo et al., 2024).

Στην τριτοβάθμια εκπαίδευση, τα εργαλεία Τεχνητής Νοημοσύνης μπορούν να υποστηρίξουν διάφορες πτυχές της μάθησης, όπως την εξατομίκευση, την αξιολόγηση και την παρακολούθηση της προόδου των φοιτητών. Η σχετική βιβλιογραφία αναφέρει επίσης εφαρμογές που αφορούν την πρόβλεψη και την επεξεργασία μαθησιακών δεδομένων, τα προσαρμοστικά περιβάλλοντα και τα ευφυή συστήματα διδασκαλίας (Zawacki-Richter et al., 2019).

Ωστόσο, η βιβλιογραφία τονίζει και την ανάγκη τα εργαλεία Τεχνητής Νοημοσύνης να μην αξιοποιούνται αποκομμένα από παιδαγωγικές θεωρίες, αλλά να συνδέονται ουσιαστικά με τον εκπαιδευτικό σχεδιασμό και τους μαθησιακούς στόχους (X. Chen et al., 2020; Zawacki-Richter et al., 2019). Έρευνα σε ψηφιακούς βοηθούς που υποστηρίζουν την αυτορρυθμιζόμενη μάθηση δείχνει ότι η υπάρχουσα βιβλιογραφία επικεντρώνεται κυρίως στη ρύθμιση της γνωστικής διάστασης της μάθησης (Martins et al., 2024). Ομοίως, ο AI βοηθός του παρόντος e-course εστιάζει επίσης στη γνωστική και διαδικαστική υποστήριξη του φοιτητή, παρέχοντας προκαθορισμένο περιεχόμενο, αναλυτικές οδηγίες υλοποίησης, καθοδηγούμενα βήματα και θεωρητική υποστήριξη σε κάθε δραστηριότητα.

Οι βασικοί δείκτες που διατρέχουν την παρούσα διπλωματική εργασία είναι η γνωστική εμπλοκή (cognitive engagement), η μεταγνωστική παρακολούθηση (metacognitive monitoring) και η κατανόηση της οπτικής των άλλων μελών της ομάδας (perspective taking). Η γνωστική εμπλοκή αφορά το βάθος με το οποίο ο εκπαιδευόμενος επεξεργάζεται το περιεχόμενο και εξετάζει κριτικά τα δεδομένα μιας δραστηριότητας (Redmond et al., 2018). Η μεταγνωστική παρακολούθηση εντάσσεται στη φάση εκτέλεσης (performance) του μοντέλου SRL, και αφορά τη συνειδητή παρατήρηση της σκέψης και της μαθησιακής πορείας (Zimmerman, 2002). Η κατανόηση της οπτικής των άλλων μελών αφορά την αξιοποίηση των απόψεων και της ειδίκευσης των συνεργατών για την επίλυση ενός κοινού προβλήματος (Hesse et al., 2015). Οι δείκτες αυτοί αξιοποιούνται στον σχεδιασμό του e-course, ώστε οι δραστηριότητες SRL, το STEAM περιβάλλον και τα υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης να συνδέονται με συγκεκριμένες δεξιότητες προς ανάπτυξη στους φοιτητές.

Οι δείκτες αυτοί αποτελούν υποδιαστάσεις ευρύτερων εννοιολογικών οικογενειών: η εμπλοκή διακρίνεται σε κοινωνική, γνωστική, συμπεριφορική, συνεργατική και συναισθηματική (Redmond et al., 2018). Η μεταγνώση διακρίνεται στις φάσεις σχεδιασμού, παρακολούθησης και αξιολόγησης (Zimmerman, 2002). Η συνεργασία διακρίνεται σε κοινωνικές δεξιότητες όπως συμμετοχή, κατανόηση της οπτικής των άλλων, κοινωνική ρύθμιση και γνωστικές δεξιότητες όπως ρύθμιση του έργου και οικοδόμηση της γνώσης (Hesse et al., 2015). Η παρούσα εργασία εστιάζει αντίστοιχα στη γνωστική εμπλοκή μέσω ανάλυσης Case Studies phishing (Chi & Wylie, 2014; Hobert et al., 2023), στη μεταγνωστική παρακολούθηση (μέσω στρατηγικών αυτοπαρατήρησης) (Akamatsu et al., 2019), και στην κατανόηση της οπτικής των άλλων μέσω συνεργατικών στρατηγικών Jigsaw, Πυραμίδας, Think-Pair-Share και Brainstorming (Çelik & Akay, 2025; Cochon Drouet et al., 2023; Esfandiari & Knight, 2013; Mouw et al., 2020; Sembert et al., 2021). Οι τρεις αυτοί δείκτες λειτουργούν ως μετρήσιμα KPIs στο πλαίσιο του e-course, ώστε η συμβολή του μαθήματος να αποτιμηθεί συγκεκριμένα.

Με βάση την προηγούμενη θεωρητική τεκμηρίωση, η παρούσα διπλωματική εργασία προσανατολίζεται στη διαμόρφωση ενός μαθησιακού περιβάλλοντος που συνδυάζει την Αυτορρυθμιζόμενη Μάθηση με τη διεπιστημονική προσέγγιση STEAM για την καλλιέργεια δεξιοτήτων κυβερνοασφάλειας σε φοιτητές τριτοβάθμιας εκπαίδευσης. Η μαθησιακή διαδικασία δεν αποσκοπεί αποκλειστικά στην απόκτηση γνώσεων σχετικά με το phishing, αλλά και στην κριτική ανάλυση ψηφιακών απειλών, στη συνειδητή παρακολούθηση της μαθησιακής πορείας και στη συνεργατική λήψη τεκμηριωμένων αποφάσεων. Στη βάση αυτή, προκύπτει η ανάγκη σχεδιασμού μιας εκπαιδευτικής παρέμβασης όπου το SRL λειτουργεί ως παιδαγωγικό μοντέλο, το STEAM ως διεπιστημονικό μαθησιακό πλαίσιο, και τα εργαλεία Τεχνητής Νοημοσύνης ως συμπληρωματικά μέσα υποστήριξης της μάθησης (García-Senín et al., 2022; López Carrillo et al., 2024; Zawacki-Richter et al., 2019; Zimmerman, 2002).

1.3 Στόχος της Διπλωματικής Εργασίας

Στόχος αυτής της διπλωματικής εργασίας είναι ο σχεδιασμός και η ανάπτυξη ενός ηλεκτρονικού μαθήματος με τίτλο «Phishing 360°: Από το Συναίσθημα στα Δεδομένα», με θεματικό αντικείμενο την κυβερνοασφάλεια και συγκεκριμένα την αναγνώριση και αντιμετώπιση επιθέσεων phishing. Το μάθημα αξιοποιεί τη μέθοδο της Αυτορρυθμιζόμενης Μάθησης (SRL), ένα STEAM περιβάλλον μάθησης και υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης, εστιάζοντας στη γνωστική εμπλοκή (cognitive engagement), τη μεταγνωστική παρακολούθηση (metacognitive monitoring) και την κατανόηση της οπτικής των άλλων μελών της ομάδας (perspective taking) των φοιτητών τριτοβάθμιας εκπαίδευσης.

1.4 Καινοτομία της Διπλωματικής Εργασίας

Η καινοτομία της παρούσας εργασίας συνίσταται στην ανάπτυξη ενός e-course κυβερνοασφάλειας, στο οποίο η εκπαίδευση για το phishing εντάσσεται σε ένα ενιαίο παιδαγωγικό πλαίσιο που συνδυάζει την Αυτορρυθμιζόμενη Μάθηση, το STEAM και υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης.

Το e-course αξιοποιεί σενάρια προσομοίωσης phishing, μέσα από τα οποία οι φοιτητές καλούνται να εντοπίσουν ύποπτα ψηφιακά μηνύματα, να αναλύσουν τεχνικά και κοινωνικά στοιχεία της επίθεσης phishing, να καταλήξουν σε τεκμηριωμένες αποφάσεις και να αναστοχαστούν πάνω στις στρατηγικές που εφάρμοσαν (Desolda et al., 2022; Marshall et al., 2024).

Η πρωτοτυπία της εργασίας εντοπίζεται επίσης στη σύνδεση της αυτορρυθμιζόμενης μάθησης με συγκεκριμένες δραστηριότητες αυτοπαρακολούθησης, στοχοθεσίας, αυτοαξιολόγησης και αναστοχασμού μέσα σε ένα STEAM περιβάλλον μάθησης. Με αυτόν τον τρόπο, η κυβερνοασφάλεια δεν προσεγγίζεται από τους φοιτητές αποκλειστικά ως τεχνικό ζήτημα, αλλά ως πεδίο που προϋποθέτει γνωστική εμπλοκή, μεταγνωστική παρακολούθηση και κατανόηση της οπτικής των συνεργατών (García-Senín et al., 2022; López Carrillo et al., 2024; Panadero, 2017; Zimmerman, 2002).

Η αξιοποίηση εργαλείων Τεχνητής Νοημοσύνης λειτουργεί επίσης υποστηρικτικά και ενισχύει τον παιδαγωγικό σχεδιασμό, καθώς συνδέεται με την παροχή καθοδήγησης και υποστήριξης κατά την ανάλυση phishing περιστατικών. Επομένως, η παρούσα διπλωματική εργασία προτείνει ένα ολοκληρωμένο μαθησιακό πλαίσιο για την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας σε φοιτητές τριτοβάθμιας εκπαίδευσης, συνδυάζοντας παιδαγωγική τεκμηρίωση, διαθεματική μάθηση και σύγχρονα ψηφιακά εργαλεία (X. Chen et al., 2020; Zawacki-Richter et al., 2019).

Παρατηρείται αυξανόμενο ενδιαφέρον για τη σύνδεση SRL και STEAM (García-Senín et al., 2022; López Carrillo et al., 2024), ωστόσο εντοπίζεται η ανάγκη περαιτέρω μελέτης του τρόπου με τον οποίο αυτά μπορούν να συνδυαστούν ουσιαστικά με ψηφιακά εργαλεία σε συγκεκριμένα γνωστικά πεδία (García-Senín et al., 2022). Αντίστοιχα, στο πεδίο της κυβερνοασφάλειας ειδικότερα, πρόσφατη συστηματική ανασκόπηση επισημαίνει ότι η ουσιαστική ενσωμάτωση εργαλείων Τεχνητής Νοημοσύνης στην εκπαίδευση κυβερνοασφάλειας απαιτεί νέους παιδαγωγικούς σχεδιασμούς, κάτι που παραμένει σχετικά ανεπαρκώς μελετημένο (Tian, 2025). Η παρούσα εργασία στοχεύει να καλύψει αυτό το διπλό κενό, προτείνοντας ένα ενιαίο σενάριο όπου το SRL, το STEAM και η Τεχνητή Νοημοσύνη λειτουργούν συμπληρωματικά για την καλλιέργεια μετρήσιμων δεξιοτήτων κυβερνοασφάλειας.

1.5 Ερευνητικά Ερωτήματα

Με βάση τον στόχο της παρούσας διπλωματικής εργασίας, διαμορφώνονται τα ακόλουθα ερευνητικά ερωτήματα:

RQ1: Σε ποιο βαθμό το e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα» συμβάλλει στην ενίσχυση της γνωστικής εμπλοκής (cognitive engagement) των φοιτητών κατά την ανάλυση των Case Studies phishing;

RQ2: Σε ποιο βαθμό το e-course συμβάλλει στην ενίσχυση της μεταγνωστικής παρακολούθησης (monitoring) των φοιτητών κατά την εκτέλεση των δραστηριοτήτων;

RQ3: Σε ποιο βαθμό το e-course συμβάλλει στην κατανόηση της οπτικής των άλλων μελών της ομάδας (perspective taking) κατά τις συνεργατικές δραστηριότητες;

1.6 Γενική Επισκόπηση της Μεθοδολογίας

Η μεθοδολογία της παρούσας εργασίας οργανώνεται σε τρία διαδοχικά στάδια: τον εκπαιδευτικό σχεδιασμό (design), την ανάπτυξη (development) και την προτεινόμενη αξιολόγηση του ηλεκτρονικού μαθήματος. Στο στάδιο του σχεδιασμού τεκμηριώνεται θεωρητικά η ένταξη των αρχών της Αυτορρυθμιζόμενης Μάθησης και του STEAM στους μαθησιακούς στόχους. Στο στάδιο της ανάπτυξης πραγματοποιείται η υλοποίηση του e-course στην πλατφόρμα Wix, μέσα από δομημένες δραστηριότητες, σενάρια phishing και υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης. Τέλος, διαμορφώνεται η πρόταση για μελλοντική αξιολόγηση του μαθήματος, δεδομένου ότι η παρούσα εργασία δεν περιλαμβάνει εφαρμογή του σε πραγματικό δείγμα φοιτητών.

Η παρούσα διπλωματική εργασία επικεντρώνεται στον σχεδιασμό και την ανάπτυξη του e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα», το οποίο υλοποιείται στην πλατφόρμα Wix. Το μάθημα στηρίζεται στην Αυτορρυθμιζόμενη Μάθηση (SRL) (Zimmerman, 2002), δομείται ως περιβάλλον STEAM (Perignat & Katz-Buonincontro, 2019), και αξιοποιεί υποστηρικτικά εργαλεία Τεχνητής Νοημοσύνης, τα οποία συνδέονται με βελτιωμένα μαθησιακά αποτελέσματα και ενισχυμένα κίνητρα των φοιτητών (Garzón et al., 2025), στοχεύοντας παράλληλα στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας σε φοιτητές τριτοβάθμιας εκπαίδευσης, πεδίο που αναγνωρίζεται ως κρίσιμο στη σύγχρονη ακαδημαϊκή εκπαίδευση (Alammari et al., 2022).

Η μεθοδολογική προσέγγιση περιλαμβάνει τον εκπαιδευτικό σχεδιασμό του e-course, την ανάπτυξη των μαθησιακών δραστηριοτήτων και την πρόταση πλαισίου μελλοντικής αξιολόγησης. Η αξιολόγηση αυτή μπορεί να στηριχθεί σε μικτή μεθοδολογία, με συνδυασμό ποσοτικών και ποιοτικών δεδομένων, εξετάζοντας τη συμβολή του μαθήματος στους φοιτητές ως προς την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας μέσω των τριών δεικτών: της γνωστικής εμπλοκής, της μεταγνωστικής παρακολούθησης και της κατανόησης της οπτικής των συνεργατών (Guetterman et al., 2015).

Σε επίπεδο μελλοντικής εφαρμογής, μπορεί να αξιοποιηθεί σχεδιασμός μίας ομάδας με αρχικές και τελικές μετρήσεις, όπως περιγράφεται αναλυτικά στο Κεφάλαιο 3. Η αξιολόγηση μπορεί επιπλέον να εμπλουτιστεί με παρατήρηση της μαθησιακής διαδικασίας, ανάλυση των παραδοτέων και απαντήσεις των φοιτητών που βασίζονται σε αναστοχασμό, ώστε να αποτυπωθεί με πιο ολοκληρωμένο τρόπο η πορεία της μάθησής τους (Guetterman et al., 2015; Nowell et al., 2017).

1.7 Οργάνωση της Διπλωματικής Εργασίας

Η διάρθρωση της διπλωματικής εργασίας περιλαμβάνει πέντε κεφάλαια, μέσω των οποίων αναπτύσσονται διαδοχικά το θεωρητικό υπόβαθρο, ο σχεδιασμός και η ανάπτυξη του e-course, καθώς και το προτεινόμενο πλαίσιο αξιολόγησής του.

Στο πρώτο κεφάλαιο παρουσιάζεται το γενικό πλαίσιο της εργασίας, οι δεξιότητες του 21^{ου} αιώνα, η προβληματική που συνδέεται με την ανάγκη ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην τριτοβάθμια εκπαίδευση, ο στόχος, η καινοτομία, τα ερευνητικά ερωτήματα, η γενική επισκόπηση της μεθοδολογίας και η οργάνωση της διπλωματικής εργασίας.

Στο δεύτερο κεφάλαιο αναπτύσσεται η βιβλιογραφική επισκόπηση. Ειδικότερα εξετάζονται η Αυτορρυθμιζόμενη μάθηση (SRL), οι δείκτες αξιολόγησης, η διεπιστημονική προσέγγιση STEAM, οι συνεργατικές στρατηγικές μάθησης, τεχνικές μάθησης όπως το SCAMPER και Think-Aloud, το περιβάλλον Wix και τα υποστηρικτικά ψηφιακά εργαλεία, καθώς και τα εργαλεία Τεχνητής Νοημοσύνης που αξιοποιήθηκαν στην εκπαιδευτική διαδικασία.

Στο τρίτο κεφάλαιο παρουσιάζεται η μεθοδολογική προσέγγιση της εργασίας. Περιγράφονται οι εννοιολογικοί και λειτουργικοί ορισμοί των υπό εξέταση εννοιών, τα ερευνητικά ερωτήματα, η ερευνητική διαδικασία καθώς και ο αναλυτικός σχεδιασμός και η ανάπτυξη του ηλεκτρονικού μαθήματος «Phishing 360°: Από το Συναίσθημα στα Δεδομένα», η δομή του στο περιβάλλον Wix, οι φάσεις SRL, οι STEAM δραστηριότητες, τα σενάρια κυβερνοασφάλειας και τα ψηφιακά εργαλεία που χρησιμοποιήθηκαν για τις ανάγκες του e-course.

Στο τέταρτο κεφάλαιο παρουσιάζεται αναλυτικά η περιγραφή και η αξιολόγηση των εργαλείων Τεχνητής Νοημοσύνης που αξιοποιήθηκαν στο πλαίσιο του σεναρίου, καθώς και το επίπεδο χρήσης τους σύμφωνα με την κλίμακα AIAS.

Στο πέμπτο κεφάλαιο παρουσιάζεται επισκόπηση των βασικών σημείων της εργασίας, τα συμπεράσματα, οι περιορισμοί του σχεδιασμού, καθώς και προτάσεις για μελλοντική έρευνα, τόσο ως προς την εφαρμογή και αξιολόγηση του e-course σε πραγματικό εκπαιδευτικό πλαίσιο όσο και ως προς ευρύτερα ζητήματα που αναδεικνύει η βιβλιογραφία στο πεδίο και δεν έχουν εξεταστεί στο πλαίσιο της παρούσας διπλωματικής εργασίας.

ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Εισαγωγή

Το τρέχον κεφάλαιο εστιάζει στην ανασκόπηση της βιβλιογραφίας γύρω από το θεωρητικό υπόβαθρο στο οποίο βασίστηκε η ανάπτυξη του συγκεκριμένου e-course.

Σε πρώτο στάδιο, αναλύεται η Αυτορρυθμιζόμενη Μάθηση (SRL), δίνοντας ιδιαίτερη βαρύτητα στο κυκλικό μοντέλο του Zimmerman. Έπειτα, εξετάζονται οι τρεις δείκτες αξιολόγησης που εφαρμόζονται στο εκπαιδευτικό σενάριο. Επιπρόσθετα, παρουσιάζεται το θεωρητικό πλαίσιο της μεθοδολογίας STEAM και η διασύνδεσή της με τον τομέα της κυβερνοασφάλειας. Έπειτα, αναπτύσσονται οι συνεργατικές στρατηγικές μάθησης και οι τεχνικές SCAMPER και Think-Aloud. Η ενότητα ολοκληρώνεται με την ανάλυση της τεχνολογικής υποδομής που χρησιμοποιήθηκε, περιλαμβάνοντας την πλατφόρμα Wix και τα εργαλεία τεχνητής νοημοσύνης που συνέβαλαν στην παραγωγή του περιεχομένου του σεναρίου.

2.2 Αυτορρυθμιζόμενη Μάθηση (SRL)

Η αυτορρυθμιζόμενη μάθηση συνιστά αντικείμενο μελέτης της εκπαιδευτικής ψυχολογίας, εστιάζοντας στον ενεργό ρόλο που αναλαμβάνει ο εκπαιδευόμενος στη δική του πορεία μάθησης. Πρόκειται για μια ενεργή διαδικασία οικοδόμησης της γνώσης, κατά την οποία ο εκπαιδευόμενος θέτει στόχους, και επιχειρεί να παρατηρεί, να τροποποιεί και να κατευθύνει τη γνωστική, παρακινητική και συμπεριφορική του λειτουργία, λαμβάνοντας υπόψη τόσο τους στόχους αυτούς όσο και τα χαρακτηριστικά του περιβάλλοντος (Pintrich, 2000). Εναλλακτικά, περιγράφεται ως η κατάσταση κατά την οποία ο εκπαιδευόμενος εμπλέκεται ενεργά στη διαμόρφωση της μελέτης του, επιτηρεί τα δικά του κίνητρα και τους στόχους, χρησιμοποιεί τους διαθέσιμους πόρους και συμμετέχει ενεργά στη λήψη αποφάσεων που αφορούν τη μάθησή του (Bandura, 1986).

Ορίζεται επίσης ως η ικανότητα του εκπαιδευόμενου να εμπλέκεται στη μαθησιακή διαδικασία σε γνωστικό, μεταγνωστικό, παρακινητικό και συμπεριφορικό επίπεδο (Zimmerman, 1989).

Για να χαρακτηριστεί μια μαθησιακή διαδικασία ως αυτορρυθμιζόμενη, επισημαίνονται τρία κρίσιμα στοιχεία: η χρήση στρατηγικών αυτορρύθμισης από τον εκπαιδευόμενο, οι αντιλήψεις του για τη δική του αυτοαποτελεσματικότητα, και η δέσμευσή του στους ακαδημαϊκούς του στόχους (Zimmerman, 1989).

Το θεωρητικό υπόβαθρο της αυτορρύθμισης εντοπίζεται στη θεωρία κοινωνικής μάθησης, όπου διατυπώνεται η αρχή της τριαδικής αμοιβαιότητας (Bandura, 1986). Βάσει αυτής της αρχής, η μαθησιακή διαδικασία καθορίζεται από την αμοιβαία επίδραση τριών παραγόντων: του ατόμου, με τα διανοητικά και συναισθηματικά του χαρακτηριστικά, της συμπεριφοράς του, μέσω της αυτοπαρατήρησης και της αυτοαξιολόγησης, και του περιβάλλοντος, κοινωνικού και φυσικού. Η σχέση αυτή δεν είναι συμμετρική, καθώς ανάλογα με την περίπτωση κάποιος από τους τρεις παράγοντες μπορεί να επιδρά περισσότερο στη μάθηση από τους άλλους δύο (Bandura, 1986).

2.2.1 Κυκλικό μοντέλο του Zimmerman

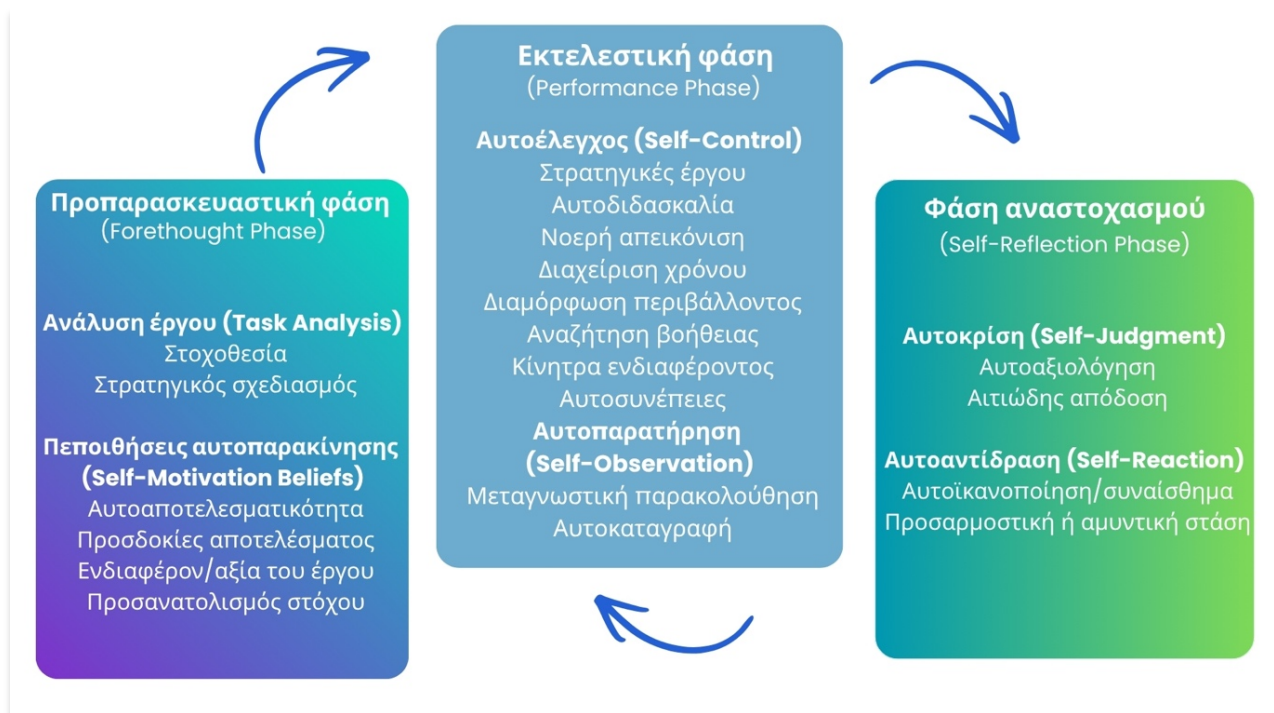
Για την ερμηνεία της αυτορρύθμισης έχουν διατυπωθεί θεωρητικά μοντέλα, με επικρατέστερα το μοντέλο του Pintrich και το κυκλικό μοντέλο του Zimmerman (Zimmerman & Moylan, 2009). Η παρούσα εργασία υιοθετεί ως κύριο θεωρητικό μοντέλο το δεύτερο, λόγω της σαφήνειας και της άμεσης εφαρμοσιμότητάς του σε ψηφιακά μαθησιακά σενάρια.

Το κυκλικό μοντέλο απαρτίζεται από τρεις διαδοχικές φάσεις, όπου τα αποτελέσματα της τελευταίας τροφοδοτούν εκ νέου την πρώτη, επιτρέποντας στον εκπαιδευόμενο να ενισχύει προοδευτικά την ικανότητά του για αυτορρύθμιση (Panadero, 2017).

Στην προπαρασκευαστική φάση, ο εκπαιδευόμενος αναλύει τι ακριβώς χρειάζεται να επιτύχει, ορίζοντας σαφείς στόχους και αποφασίζοντας ποιες στρατηγικές θα ακολουθήσει για την προσέγγιση του έργου του. Παράλληλα, ενεργοποιούνται τα κίνητρά του, με κυρίαρχο στοιχείο την πεποίθησή του για την ικανότητά του να επιτύχει (Panadero, 2017).

Στην εκτελεστική φάση, ο εκπαιδευόμενος υλοποιεί όσα είχε σχεδιάσει, κατανέμοντας τον χρόνο και την προσπάθειά του, ενώ ταυτόχρονα καταγράφει και επιτηρεί την πορεία του σε σχέση με τον αρχικό στόχο (Panadero, 2017).

Στη φάση του αναστοχασμού, ο εκπαιδευόμενος αξιολογεί το τελικό αποτέλεσμα σε αντιπαραβολή με όσα είχε αρχικά σχεδιάσει, εντοπίζει τους παράγοντες που οδήγησαν στην επίτευξη ή μη των αρχικών του στόχων, και βιώνει μια αντίστοιχη συναισθηματική αντίδραση που διαμορφώνει την προσέγγισή του στον επόμενο κύκλο μάθησης (Panadero, 2017). Οι τρεις αυτές φάσεις απεικονίζονται στο σχήμα που ακολουθεί (Zimmerman & Moylan, 2009).



Σχήμα 1: Το κυκλικό μοντέλο των φάσεων SRL

Σημείωση. Προσαρμογή από (Zimmerman & Moylan, 2009).

2.3 Δείκτες Αξιολόγησης

Η αξιολόγηση της αποτελεσματικότητας ενός εκπαιδευτικού σεναρίου δεν μπορεί να στηριχθεί μόνο στον σχεδιασμό του, αλλά απαιτεί συγκεκριμένους, μετρήσιμους δείκτες που να αντικατοπτρίζουν τις δεξιότητες που το σενάριο επιδιώκει να καλλιεργήσει. Στο παρόν e-course αξιοποιούνται τρεις δείκτες αξιολόγησης.

2.3.1 Γνωστική Εμπλοκή (cognitive engagement)

Η γνωστική εμπλοκή αναφέρεται στον βαθμό στον οποίο ο εκπαιδευόμενος επεξεργάζεται σε βάθος το περιεχόμενο της μάθησης, εφαρμόζει στρατηγικές ανάλυσης και κριτικής σκέψης, συνδέει διαφορετικές πληροφορίες και τεκμηριώνει τις αποφάσεις του, αντί να παραμένει σε μια απλή, επιφανειακή εκτέλεση της δραστηριότητας (Redmond et al., 2018; Shi et al., 2026). Πρόκειται για μία από τις κεντρικές διαστάσεις της μαθησιακής εμπλοκής που έχουν καθιερωθεί στη διεθνή βιβλιογραφία, μαζί με τη συμπεριφορική και τη συναισθηματική διάσταση (Fredricks et al., 2004). Για την πληρέστερη κατανόηση και μέτρησή της, η γνωστική εμπλοκή αναλύεται σε δείκτες ποσότητας και δείκτες ποιότητας (Halverson & Graham, 2019), όπως αποτυπώνονται στον κάτωθι Πίνακα.

Πίνακας 1: Δείκτες Γνωστικής Εμπλοκής

Παράγοντες	Δείκτες
Παράγοντες Ποσότητας	Προσοχή
	Προσπάθεια και Επιμονή
	Χρόνος επί του έργου
Παράγοντες Ποιότητας	Γνωστικές και Μεταγνωστικές Στρατηγικές
	Βαθιά Συγκέντρωση και Απορρόφηση
	Ατομικό Ενδιαφέρον και Περιέργεια

Σημείωση. Προσαρμογή από (Halverson & Graham, 2019)

Η μέτρηση της γνωστικής εμπλοκής παραμένει επίσης ενεργό ερευνητικό πεδίο, καθώς τα εργαλεία που έχουν αναπτυχθεί έως τώρα διαφέρουν σημαντικά μεταξύ τους ως προς τη μεθοδολογική τους προσέγγιση. Το University Student Engagement Inventory ξεχωρίζει ως ένα από τα πιο εκτενώς επικυρωμένα εργαλεία αυτοαναφοράς, καθώς περιλαμβάνει ξεχωριστή διάσταση αφιερωμένη αποκλειστικά στη γνωστική εμπλοκή. Αξιοσημείωτο είναι ότι έχει δοκιμαστεί σε φοιτητικούς πληθυσμούς διαφορετικών χωρών με σταθερά ευρήματα ως προς την αξιοπιστία και την εγκυρότητά του (Marôco, 2026). Παράλληλα, πρόσφατη έρευνα διερεύνησε κατά πόσο δεδομένα συμπεριφοράς μέσα σε περιβάλλον online μάθησης, όπως ο χρόνος πρόσβασης στο υλικό ή ο αριθμός των διαλειμμάτων, μπορούν να προβλέψουν τη γνωστική εμπλοκή έτσι όπως τη δηλώνουν οι ίδιοι οι φοιτητές. Τα αποτελέσματα έδειξαν ότι τα δεδομένα συμπεριφοράς εξηγούν μόνο ένα μικρό έως μέτριο ποσοστό της διακύμανσης στην αυτοαναφερόμενη εμπλοκή (Winter et al., 2024). Τα ευρήματα αυτά υποδηλώνουν ότι, η μέτρηση της γνωστικής εμπλοκής παραμένει μεθοδολογικά σύνθετη, με την αυτοαναφορά και τα αντικειμενικά δεδομένα συμπεριφοράς να αποτυπώνουν εν μέρει διαφορετικές απόψεις της ίδιας έννοιας.

Πρόσφατη έρευνα έδειξε ότι ένα καλά σχεδιασμένο online μάθημα ενισχύει τόσο τη βαθιά όσο και την επιφανειακή γνωστική εμπλοκή των φοιτητών, μέσω παραγόντων όπως η ακαδημαϊκή αυτοαντίληψη και η βίωση κατάστασης ροής κατά τη μελέτη (Shi et al., 2025). Στο πλαίσιο ενός σεναρίου κυβερνοασφάλειας, η ικανότητα αυτή αποκτά ιδιαίτερη σημασία, καθώς η αναγνώριση μιας επίθεσης phishing προϋποθέτει αυτού του είδους τη σε βάθος ανάλυση και αξιολόγηση των στοιχείων, και όχι μια βιαστική, επιφανειακή κρίση.

Η σύνδεση της γνωστικής εμπλοκής με το πλαίσιο της Αυτορρυθμιζόμενης Μάθησης αποτελεί αντικείμενο αυξανόμενου ερευνητικού ενδιαφέροντος τα τελευταία χρόνια. Ένα πρόσφατο ενοποιημένο μοντέλο καταγράφει τον τρόπο με τον οποίο μεταβάλλεται η γνωστική εμπλοκή του εκπαιδευόμενου κατά τη διάρκεια της στοχοθεσίας, της εκτέλεσης και του αναστοχασμού, ενσωματώνοντας παράλληλα τη συνεχή παρακολούθηση της προόδου καθώς και την αξιοποίηση της ανατροφοδότησης. Με τον τρόπο αυτό αναδεικνύεται ότι ο βαθμός γνωστικής εμπλοκής επηρεάζει την αυτορρύθμιση, ενώ ταυτόχρονα η ίδια η αυτορρύθμιση καθοδηγεί και ενισχύει την γνωστική εμπλοκή (Alam & Mohanty, 2024).

Παρά τη θεωρητική αυτή σύγκλιση, συστηματική ανασκόπηση πέντε ετών σε περιβάλλοντα μεικτής μάθησης της τριτοβάθμιας εκπαίδευσης διαπίστωσε πως οι γνωστικές στρατηγικές παραμένουν λιγότερο μελετημένες συγκριτικά με τη διαχείριση πόρων και τις μεταγνωστικές στρατηγικές, αναδεικνύοντας έτσι την ανάγκη για περαιτέρω διερεύνησή τους στο συγκεκριμένο πεδίο (Luo & Zhou, 2024). Ιδιαίτερα σημαντική είναι και μια πρόσφατη μελέτη σε μεταπτυχιακούς φοιτητές, η οποία, αξιοποιώντας το πλαίσιο ICAP της γνωστικής εμπλοκής, διαπίστωσε ότι όσοι διαθέτουν υψηλότερη ικανότητα αυτορρύθμισης εμπλέκονται πιο ενεργά με την ανατροφοδότηση που λαμβάνουν κατά τη διάρκεια ενός μαθήματος αν και η εμπλοκή αυτή δεν συνδέθηκε πάντα άμεσα με καλύτερη τελική επίδοση (Uzun et al., 2025).

Οι παραπάνω μελέτες συγκλίνουν σε ένα βασικό συμπέρασμα: η γνωστική εμπλοκή δεν είναι απλώς παράλληλη με την αυτορρύθμιση, αλλά αλληλένδετη μαζί της, ενώ παραμένει πεδίο που χρειάζεται περαιτέρω εμπειρική τεκμηρίωση, ιδίως σε εφαρμοσμένα πλαίσια όπως η κυβερνοασφάλεια. Αυτό ενισχύει την επιλογή της ως δείκτη αξιολόγησης στο παρόν e-course, όπου η ανάλυση σεναρίων phishing απαιτεί ακριβώς αυτόν τον συνδυασμό βαθιάς γνωστικής επεξεργασίας και συνειδητής αυτορρύθμισης.

2.3.2 Μεταγνωστική Παρακολούθηση (metacognitive monitoring)

Η μεταγνωστική παρακολούθηση αφορά τη συνειδητή παρατήρηση και τον έλεγχο της κατανόησης, της προόδου και των στρατηγικών του εκπαιδευόμενου κατά την εκτέλεση ενός μαθησιακού έργου. Στη φάση της εκτέλεσης του μοντέλου της Αυτορρυθμιζόμενης Μάθησης, ο εκπαιδευόμενος παρακολουθεί την πορεία του, αναγνωρίζει δυσκολίες και προσαρμόζει τις ενέργειές του όταν χρειάζεται (Wagener, 2016). Πρόσφατη έρευνα σε φοιτητές εξ αποστάσεως εκπαίδευσης επιβεβαιώνει ότι η μεταγνωστική παρακολούθηση συνδέεται σταθερά με την ακαδημαϊκή επίδοση σε αυτού του είδους τα περιβάλλοντα μάθησης (Xue & Khalid, 2026). Η ικανότητα αυτή αποκτά ιδιαίτερη βαρύτητα στην αναγνώριση απειλών phishing, καθώς οι χρήστες συχνά εμφανίζουν αδύναμη σύνδεση ανάμεσα στην αυτοπεποίθησή τους και την πραγματική τους ικανότητα να διακρίνουν ένα ύποπτο μήνυμα (Canfield et al., 2019).

Η σύγχρονη βιβλιογραφία δείχνει ότι η ίδια η μέτρηση της μεταγνωστικής παρακολούθησης παραμένει ζήτημα υπό συνεχή διερεύνηση, καθώς διακρίνονται δύο βασικές οικογένειες δεικτών. Η πρώτη αφορά τις στρατηγικές παρακολούθησης, δηλαδή αυτοαναφορικές κλίμακες μέσω των οποίων ο εκπαιδευόμενος δηλώνει σε ποιο βαθμό ελέγχει την αποτελεσματικότητα της μελέτης του και την κατανόησή του. Η δεύτερη αφορά τις κρίσεις παρακολούθησης, δηλαδή τις άμεσες εκτιμήσεις της επίδοσης, που μπορούν να διαμορφωθούν είτε ως προβλέψεις πριν από μια δραστηριότητα, είτε ως ταυτόχρονες αξιολογήσεις κατά τη διάρκειά της, είτε ως εκ των υστέρων αποτιμήσεις μετά την ολοκλήρωσή της. Έρευνα σε φοιτητές τριτοβάθμιας εκπαίδευσης έδειξε ότι οι δύο αυτοί τύποι δεικτών συσχετίζονται μόνο ελαφρά μεταξύ τους, γεγονός που υποδηλώνει ότι αποτυπώνουν διαφορετικές πτυχές της ίδιας διεργασίας (Händel et al., 2023).

Η οργάνωση αυτή γίνεται ακόμα πιο σαφής όταν οι δύο διαστάσεις, η φάση και το αντικείμενο, εξεταστούν διασταυρωτικά. Ο παρακάτω Πίνακας αποτυπώνει τις τέσσερις επιμέρους λειτουργίες που προκύπτουν από αυτή τη διασταύρωση, με ενδεικτικά παραδείγματα μεταγνωστικής συμπεριφοράς για την καθεμία (Händel et al., 2023).

Πίνακας 2: Λειτουργίες Μεταγνωστικής Παρακολούθησης ανά Φάση και Αντικείμενο

	Προετοιμασία		Εξέταση	
	Διαδικασία	Ανάκληση	Διαδικασία	Ανάκληση
Ορισμός	Παρακολούθηση αποτελεσματικότητας της μαθησιακής προσέγγισης.	Παρακολούθηση κατανόησης.	Παρακολούθηση επεξεργασίας της εξέτασης.	Παρακολούθηση ορθότητας δοθεισών απαντήσεων.
Ενδεικτική Συμπεριφορά Παρακολούθησης	Έλεγχος αν η διαδικασία μελέτης που χρησιμοποιήθηκε είναι αποτελεσματική.	Έλεγχος αν το περιεχόμενο της μελέτης έγινε κατανοητό.	Έλεγχος αν όλα τα ερωτήματα έχουν απαντηθεί.	Έλεγχος αν μια δοθείσα απάντηση είναι σωστή.

Σημείωση. Προσαρμογή από (Händel et al., 2023).

Η διάσταση αυτή ανάμεσα σε αντικειμενικούς και υποκειμενικούς δείκτες επιβεβαιώνεται και από πιο πρόσφατες μελέτες. Έρευνα σε ενήλικες συμμετέχοντες έδειξε ότι η υποκειμενική εκτίμηση συχνά παραπλανά, καθώς όσοι δήλωναν στα ερωτηματολόγια υψηλή μεταγνωστική ικανότητα αποδείχθηκαν στην πραγματικότητα λιγότερο ακριβείς στις αντικειμενικές τους εκτιμήσεις (Double, 2025).

Σε μελέτη με φοιτητές κατά την ανάγνωση κειμένου, οι άμεσες εκτιμήσεις που υπέβαλαν οι ίδιοι την ώρα της μελέτης δεν σχετίστηκαν με τα γενικά ερωτηματολόγια, ενώ ήταν οι μόνες που προέβλεψαν την πραγματική τους επίδοση (Seban et al., 2025).

Τα ευρήματα αυτά ενισχύουν την άποψη ότι η μεταγνωστική παρακολούθηση δεν πρέπει να αντιμετωπίζεται ως ενιαία και ομοιογενής ικανότητα, αλλά ως πολυδιάστατη διεργασία, της οποίας η ακριβής αποτύπωση εξαρτάται σε μεγάλο βαθμό από τη μέθοδο μέτρησης που επιλέγεται. Στο πλαίσιο της αναγνώρισης απειλών phishing, η διάκριση αυτή αποκτά πρακτική σημασία, καθώς η αίσθηση επάρκειας που έχει ο χρήστης για τον εαυτό του δεν συμπίπτει πάντα με την πραγματική του ικανότητα να διακρίνει ένα ύποπτο μήνυμα, γεγονός που ενισχύει την ανάγκη για πιο άμεσους και επαληθεύσιμους δείκτες αξιολόγησης της μεταγνωστικής επίδοσης.

2.3.3 Κατανόηση της Οπτικής των Άλλων (perspective-taking)

Η ικανότητα να κατανοεί κανείς την οπτική των άλλων αφορά τη δυνατότητα του εκπαιδευμένου να προσεγγίζει ένα ζήτημα λαμβάνοντας υπόψη τη θέση και τη συνεισφορά των συνεργατών του, προσαρμόζοντας ανάλογα τον τρόπο σκέψης και επικοινωνίας του (Hesse et al., 2015). Η θετική αλληλεξάρτηση των μελών μιας ομάδας ωθεί τον εκπαιδευόμενο να λαμβάνει υπόψη τις συνεισφορές των άλλων προκειμένου να συμβάλλει στην επίτευξη ενός κοινού στόχου (Johnson & Johnson, 2009). Στις συνεργατικές δραστηριότητες του σεναρίου, η ικανότητα αυτή αναδεικνύεται όταν ο εκπαιδευόμενος συγκρίνει τις δικές του παρατηρήσεις με εκείνες των συνεργατών του, ώστε να διαμορφώσει μια πιο ολοκληρωμένη εικόνα του προβλήματος.

Στη σύγχρονη βιβλιογραφία, η λήψη οπτικής, γνωστή και ως perspective-taking, περιγράφεται ως μια σύνθετη διεργασία που βοηθά στη γεφύρωση διαφορετικών αντιλήψεων κατά την επικοινωνία (Vaassen et al., 2026). Παράλληλα, ευρήματα πειραματικής μελέτης αποδεικνύουν ότι η διαδικασία αυτή συμβάλλει στη μείωση της γνωστικής συγχώνευσης και στην ενίσχυση της αυτοσυμπόνιας του ατόμου (Boland et al., 2021). Επιπλέον, σχετική έρευνα υπογραμμίζει ότι η ενεργός κατανόηση της προοπτικής του άλλου συμβάλλει στη μείωση στερεοτυπικών αντιλήψεων και προκαταλήψεων ανάμεσα σε διαφορετικές ομάδες, ενισχύοντας παράλληλα τα επίπεδα εμπιστοσύνης (Hutchings et al., 2021).

Για τη συστηματική αξιολόγηση της ικανότητας λήψης οπτικής (perspective-taking), πρόσφατη έρευνα προτείνει την οργάνωση της ικανότητας αυτής σε τρεις αλληλένδετους δείκτες που καλύπτουν τη γνωστική διάσταση, τη συναισθηματική διάσταση και τη διάσταση κινήτρων, όπως αποτυπώνεται στον κάτωθι Πίνακα (Harriss et al., 2025).

Πίνακας 3: Δείκτες Κατανόησης της Οπτικής των Άλλων

Διαστάσεις	Δείκτες	Περιγραφή
Γνωστική Διάσταση	Κριτικός Αναστοχασμός (Critical Reflection)	Εντοπισμός και αμφισβήτηση των προσωπικών παραδοχών, προκαταλήψεων και υποσυνείδητων παραδοχών κατά την επικοινωνία.
Συναισθηματική Διάσταση	Μετατόπιση Οπτικής (Perspective Shift)	Ενσυναισθητική εμπλοκή και αναγνώριση των συναισθημάτων, των αναγκών και του υπόβαθρου του άλλου.
Διάσταση Κινήτρων	Εφαρμογή Νέων Οπτικών (Application of New Perspectives)	Μετάφραση της νέας κατανόησης σε συγκεκριμένες επικοινωνιακές στρατηγικές και προσαρμογή της συμπεριφοράς στην πράξη.

Σημείωση. Προσαρμογή από (Harriss et al., 2025).

Παράλληλα με τη γνωστική εμπλοκή και τη μεταγνωστική παρακολούθηση, η μέτρηση της ικανότητας κατανόησης της οπτικής των άλλων εξακολουθεί να αποτελεί ανοιχτό ερευνητικό ζήτημα. Μια συστηματική ανασκόπηση εξήντα μελετών διαπίστωσε πως τα διαθέσιμα εργαλεία μέτρησης στηρίζονται σχεδόν αποκλειστικά σε αυτοαναφορά, ενώ ελάχιστα ανεξάρτητα και ψυχομετρικά επικυρωμένα εργαλεία είναι διαθέσιμα, γεγονός που αναδεικνύει την ανάγκη ανάπτυξης νέων μέσων μέτρησης (Leijenaar et al., 2025). Προς αυτή την κατεύθυνση κινείται πρόσφατη έρευνα που ανέπτυξε και επικύρωσε, μέσα από πέντε διαδοχικές μελέτες, ένα νέο εργαλείο μέτρησης της ικανότητας ενσωμάτωσης της οπτικής άλλων σε διεπιστημονικές συνεργασίες, το οποίο οργανώνει την ικανότητα αυτή σε δύο διαστάσεις, τη συνειδητή θεώρηση της γνώσης του συνεργάτη και την αφομοίωση ή προσαρμογή σε αυτήν (Salazar Campo & Lant, 2025). Τα ευρήματα αυτά επιβεβαιώνουν ότι, όπως και στις προηγούμενες δύο ικανότητες, η μέτρηση της κατανόησης της οπτικής των άλλων εξελίσσεται ενεργά, με την επιστημονική κοινότητα να αναζητά πιο αξιόπιστα και ειδικά προσαρμοσμένα εργαλεία αξιολόγησης.

Στο πλαίσιο του παρόντος e-course για την κυβερνοασφάλεια, η καλλιέργεια των παραπάνω δεικτών αποκτά ιδιαίτερη σημασία. Η αποτελεσματική αναγνώριση μιας απειλής phishing δεν περιορίζεται στην τεχνική εξέταση ενός μηνύματος, αλλά προϋποθέτει ότι ο χρήστης κατανοεί τον τρόπο σκέψης, τα κίνητρα και τις τακτικές ψυχολογικής χειραγώγησης που επιστρατεύει ο επιτιθέμενος. Παράλληλα, κατά τις συνεργατικές δραστηριότητες του μαθήματος, οι εκπαιδευόμενοι καλούνται να αναγνωρίσουν τις δικές τους προκαταλήψεις και να διακρίνουν καθαρά ανάμεσα στην αρχική πρόθεση μιας επικοινωνίας και στον πραγματικό αντίκτυπο στον παραλήπτη. Αυτή η συνειδητοποίηση επιτρέπει στους εκπαιδευόμενους να αμφισβητούν τις αυθαίρετες παραδοχές τους, να διορθώνουν επικοινωνιακά λάθη και να αναπτύσσουν μια πιο σφαιρική και κριτική στάση απέναντι στις ψηφιακές απειλές.

2.4 STEAM

2.4.1 Ιστορία και εξέλιξη του STEM/STEAM

Ο όρος STEM προέκυψε στις Ηνωμένες Πολιτείες τη δεκαετία του 1990, ως συντομογραφία των όρων Science, Technology, Engineering, Mathematics, με σκοπό τη συνένωση αυτών των τεσσάρων επιστημονικών περιοχών σε ένα ενοποιημένο εκπαιδευτικό πλαίσιο (Sokolova et al., 2025). Η εκπαίδευση STEM γνώρισε σημαντική ανάπτυξη, ως απάντηση στην ανάγκη για διεπιστημονική, τεχνολογικά προσανατολισμένη μάθηση. Αξίζει να σημειωθεί ότι η εξέλιξή της δεν σταμάτησε εκεί, με μεταγενέστερες προσαρμογές να προσθέτουν την Τέχνη, διαμορφώνοντας το STEAM (Gavrilas & Kotsis, 2025).

Η ενσωμάτωση των Τεχνών (ARTS) εισήχθη τυπικά το 2008 από την ερευνήτρια Georgette Yakman. Η προσέγγιση αυτή δεν αποτέλεσε απλώς την προσθήκη μιας νέας γνωστικής περιοχής, αλλά απέβλεπε στη συγκρότηση ενός ολοκληρωμένου συστήματος όπου η τέχνη γεφυρώνει την τεχνολογική εξειδίκευση με την ανθρώπινη βιωματική πλευρά (Yakman, 2008). Μολονότι ο όρος STEAM χρησιμοποιείται εκτενώς, η ερευνητική κοινότητα δεν έχει διαμορφώσει μια κοινή προσέγγιση σχετικά με το τι ακριβώς συνιστά η ενσωμάτωση των Τεχνών, με έρευνες να επισημαίνουν ότι η δημιουργικότητα στο πλαίσιο του STEAM σπάνια μετριέται συστηματικά (Perignat & Katz-Buonincontro, 2019).

Στο πλαίσιο αυτό, προσδιορίστηκε ο τρόπος με τον οποίο κάθε επιμέρους κλάδος ορίζεται και ταξινομείται εντός της προσέγγισης STEAM, όπως συνοψίζεται στον κάτωθι Πίνακα (Yakman, 2008).

Πίνακας 4: Ορισμός και ταξινόμηση των κλάδων στην προσέγγιση STEAM

Κλάδος	Ορισμός	Υποπεδία
Επιστήμες	Ό,τι υπάρχει στη φύση και πώς επηρεάζεται.	Φυσική, Βιολογία, Χημεία, Γεωεπιστήμες, Επιστήμη του Διαστήματος, Βιοχημεία.
Τεχνολογία	Ό, τι είναι ανθρωπογενές.	Φύση της Τεχνολογίας, Τεχνολογία και Κοινωνία, Σχεδιασμός, Ιατρική, Γεωργία, Βιοτεχνολογία, Κατασκευές, Βιομηχανία, Πληροφορική, Επικοινωνίες, Μεταφορές, Ενέργεια.
Μηχανική	Η χρήση δημιουργικότητας και λογικής, βασισμένη στα μαθηματικά και τις επιστήμες, με την τεχνολογία ως συνδετικό κρίκο.	Αεροδιαστημική, Αρχιτεκτονική, Χημική, Πολιτική, Πληροφορική, Ηλεκτρολογική, Βιομηχανική/Συστημάτων, Μηχανολογική, Ναυπηγική.
Μαθηματικά	Δεν παρέχεται ξεχωριστός εννοιολογικός ορισμός στο πρωτότυπο κείμενο.	Αριθμοί και Πράξεις, Άλγεβρα, Γεωμετρία, Μέτρηση, Ανάλυση Δεδομένων και Πιθανότητες, Επίλυση Προβλημάτων.
Τέχνες	Πώς η κοινωνία εξελίσσεται, επικοινωνείται και γίνεται κατανοητή, με τα ήθη και τα έθιμά της.	Φυσική Αγωγή, Καλές Τέχνες, Χειροτεχνία, Γλώσσα, Φιλελεύθερες Τέχνες.

Σημείωση. Προσαρμογή από (Yakman, 2008).

2.4.2 Παιδαγωγική αξία της STEAM

Σύμφωνα με τις βιβλιογραφικές πηγές, το μοντέλο STEAM συμβάλλει καθοριστικά στην καλλιέργεια προηγμένων ικανοτήτων, συμπεριλαμβανομένης της κριτικής ανάλυσης, της αντιμετώπισης προβλημάτων και της ικανότητας σύνδεσης θεωρητικής γνώσης με την πρακτική εφαρμογή (Yulianti et al., 2024). Η διεπιστημονική φύση της προσέγγισης ωθεί τον εκπαιδευόμενο να επεξεργάζεται το περιεχόμενο σε βάθος, συνδυάζοντας πληροφορίες από διαφορετικά γνωστικά πεδία για την επίτευξη ενός συγκεκριμένου στόχου. Έρευνα σε φοιτητές μαθημάτων STEAM έδειξε ότι το επίπεδο ακαδημαϊκής εμπλοκής τους συνδέεται άμεσα με το επίπεδο κριτικής σκέψης που επιδεικνύουν κατά την επεξεργασία ενός προβλήματος (Sha et al., 2021).

2.4.3 STEAM και Κυβερνοασφάλεια

Η διεπιστημονική λογική της STEAM έχει αρχίσει να εφαρμόζεται και στο πεδίο της κυβερνοασφάλειας, καθώς η κατανόηση απειλών όπως το phishing δεν απαιτεί μόνο τεχνική γνώση, αλλά και δεξιότητες ανάλυσης, δημιουργικής σκέψης και επικοινωνίας που καλλιεργεί η προσέγγιση STEAM. Η ένταξη της κυβερνοεπιστήμης μέσα στο ευρύτερο πλαίσιο STEM/STEAM προτείνεται ως τρόπος ώστε οι εκπαιδευόμενοι να αποκτούν όχι μόνο τεχνικές δεξιότητες, αλλά και ικανότητα κριτικής αξιολόγησης κινδύνων στο ψηφιακό περιβάλλον (Spencer, 2024). Παράλληλα, διαδραστικές και παιχνιδοποιημένες παιδαγωγικές προσεγγίσεις, συγγενείς με τη λογική της STEAM, έχουν εφαρμοστεί με επιτυχία στη διδασκαλία εννοιών κυβερνοασφάλειας, συμπεριλαμβανομένης της αναγνώρισης μηνυμάτων phishing, ενισχύοντας την κατανόηση και τη διατήρηση της γνώσης των εκπαιδευομένων (Arduin & Costé, 2026).

2.5 Συνεργατικές Στρατηγικές Μάθησης

Οι συνεργατικές στρατηγικές μάθησης αξιοποιούνται στο παρόν e-course ως εργαλείο ενίσχυσης της αλληλεπίδρασης μεταξύ των φοιτητών και της συλλογικής επεξεργασίας γνώσης. Στο σενάριο αξιοποιούνται τέσσερις τέτοιες στρατηγικές: το Jigsaw, το Think-Pair-Share, η Πυραμίδα και ο Καταιγισμός Ιδεών.

2.5.1 Jigsaw

Κατά την εφαρμογή της στρατηγικής Jigsaw, οι συμμετέχοντες οργανώνονται σε «ομάδες ειδικών» προκειμένου να μελετήσουν αυτόνομα ένα συγκεκριμένο τμήμα του εκπαιδευτικού υλικού. Ακολούθως, εντάσσονται ξανά στις αρχικές τους ομάδες με σκοπό να μοιραστούν και να ενοποιήσουν τις νέες γνώσεις τους (Kekeba et al., 2024). Πρόσφατη συστηματική ανασκόπηση και μετα-ανάλυση 69 μελετών επιβεβαιώνει ότι το Jigsaw έχει γενικά θετική επίδραση στην ακαδημαϊκή επίδοση, ωστόσο η αποτελεσματικότητά του επηρεάζεται από στοιχεία όπως η πολυπλοκότητα του περιεχομένου και η σωστή προετοιμασία των ομάδων ειδικών (Cochon Drouet et al., 2023).

2.5.2 Think-Pair-Share

Στη στρατηγική Think-Pair-Share, ο φοιτητής επεξεργάζεται αρχικά ατομικά μια ερώτηση, στη συνέχεια συζητά τις σκέψεις του με έναν συνεργάτη και τέλος μοιράζεται τα πορίσματα με την ολομέλεια της τάξης. Η δομή αυτή ενισχύει τη συμμετοχή μέσα στην τάξη, καθώς η ενδιαμέση φάση της συζήτησης σε ζευγάρια λειτουργεί προστατευτικά για φοιτητές που διστάζουν να μιλήσουν απευθείας μπροστά σε όλη την ομάδα (Mundelsee & Jurkowski, 2021), ενώ σε ψηφιακά περιβάλλοντα η στρατηγική έχει προσαρμοστεί επιτυχώς μέσω δομημένης συνεργασίας μεταξύ φοιτητών (Sembert et al., 2021).

2.5.3 Πυραμίδα

Η στρατηγική της Πυραμίδας ακολουθεί λογική σταδιακής διεύρυνσης, από το άτομο σε μικρές ομάδες και στη συνέχεια σε ολοένα μεγαλύτερες, επιτρέποντας στους φοιτητές να συγκρίνουν και να συνθέτουν διαφορετικές απόψεις σε κάθε στάδιο. Έρευνα σε εκπαιδευόμενους διαπίστωσε βελτίωση στις μαθησιακές τους επιδόσεις, όταν εφαρμόστηκε η συγκεκριμένη τεχνική σε ομαδικές συζητήσεις (Duraman et al., 2015).

2.5.4 Καταιγισμός Ιδεών (Brainstorming)

Ο Καταιγισμός Ιδεών ενθαρρύνει την ελεύθερη έκφραση ιδεών χωρίς άμεση κριτική, με στόχο τη συλλογική παραγωγή πολλαπλών πιθανών λύσεων σε ένα πρόβλημα. Πρόσφατη μετα-ανάλυση επιβεβαιώνει τη θετική επίδραση της τεχνικής τόσο στην ακαδημαϊκή επίδοση όσο και στη δημιουργική σκέψη των εκπαιδευομένων (Çelik & Akay, 2025).

2.6 Τεχνικές Μάθησης

Το e-course αξιοποιεί επιπλέον δύο τεχνικές που ενισχύουν τη δημιουργική και τη μεταγνωστική σκέψη του φοιτητή: το SCAMPER και το Think-Aloud.

2.6.1 SCAMPER

Το SCAMPER είναι τεχνική δημιουργικής σκέψης που καθοδηγεί τον χρήστη μέσα από μια σειρά στοχευμένων ερωτήσεων, οι οποίες αντιστοιχούν στα γράμματα του ακρωνυμίου: υποκατάσταση, συνδυασμός, προσαρμογή, τροποποίηση, άλλη χρήση, απαλοιφή και αντιστροφή, με στόχο την εξέταση ενός προβλήματος από πολλαπλές οπτικές γωνίες (Serrat, 2017). Έρευνα σε φοιτητές μηχανικής επιβεβαιώνει τη θετική επίδραση της τεχνικής στην ενίσχυση της δημιουργικής τους σκέψης (Bui et al., 2025).

2.6.2 Think-Aloud

Το Think-Aloud είναι τεχνική κατά την οποία ο εκπαιδευόμενος εκφράζει φωναχτά ή γραπτά τη σκέψη του καθώς επεξεργάζεται ένα πρόβλημα, καθιστώντας ορατή τη νοητική διαδικασία που κανονικά παραμένει εσωτερική (Coiro, 2011). Έρευνα που εφάρμοσε το πρωτόκολλο Think-Aloud σε εκπαιδευόμενους κατά την επίλυση προβλήματος επιβεβαιώνει ότι η φωναχτή έκφραση της σκέψης αναδεικνύει με σαφήνεια τις γνωστικές και μεταγνωστικές διεργασίες που ο εκπαιδευόμενος ακολουθεί (Bouiri et al., 2023).

2.7 Περιβάλλον e-Learning

2.7.1 Πλατφόρμα Wix

Το e-course αναπτύχθηκε στην πλατφόρμα Wix, η οποία λειτούργησε ως το βασικό εικονικό μαθησιακό περιβάλλον της παρέμβασης. Το Wix είναι πλατφόρμα δημιουργίας ιστοσελίδων που βασίζεται στη λογική drag-and-drop, χωρίς να απαιτεί προχωρημένες γνώσεις προγραμματισμού. Μελέτη περίπτωσης σε φοιτητές χωρίς προηγούμενη εμπειρία προγραμματισμού επιβεβαίωσε ότι το Wix επιτρέπει την ολοκλήρωση ενός πλήρους εκπαιδευτικού ιστότοπου μέσα σε σύντομο χρονικό διάστημα (Madiyah et al., 2024), ενώ πρακτική εφαρμογή έχει δείξει ότι η αξιοποίησή του υποστηρίζει αποτελεσματικά την αυτορρυθμιζόμενη μάθηση σε ψηφιακά περιβάλλοντα (Dharma & Septiana, 2023).

2.7.2 Ψηφιακά εργαλεία

Ως υποστηρικτικά εργαλεία Web 2.0 επιλέχθηκαν συγκεκριμένες εφαρμογές που εξυπηρετούν ξεχωριστούς παιδαγωγικούς σκοπούς, όπως:

Padlet: διαδικτυακός, εικονικός πίνακας ανακοινώσεων και συνεργασίας (Padlet, 2026). Χρησιμοποιήθηκε στο σενάριο ως χώρος ανάρτησης στόχων, ιδεών και ανατροφοδότησης μεταξύ των φοιτητών.

Trello: εργαλείο διαχείρισης έργων και οργάνωσης εργασιών βασισμένο σε πίνακες και κάρτες (Trello, 2026). Χρησιμοποιήθηκε στο σενάριο για τη διαχείριση χρόνου των φοιτητών σε κάθε STEAM ενότητα της φάσης Performance.

Evernote: ψηφιακή εφαρμογή σημειώσεων και οργάνωσης (Evernote, 2026) που χρησιμοποιήθηκε στο σενάριο για την αυτοκαταγραφή της μαθησιακής πορείας στο ημερολόγιο αναστοχασμού.

Canva: εργαλείο γραφιστικής σχεδίασης (Canva, 2026) που αξιοποιήθηκε για τον σχεδιασμό γραφιστικών και mockup στις δραστηριότητες οπτικής εξαπάτησης του σεναρίου. Επίσης χρησιμοποιήθηκε από τον συγγραφέα για την επεξεργασία φωτογραφιών και διαγραμμάτων που παρουσιάζονται στην παρούσα διπλωματική.

Mentimeter: πλατφόρμα διαδραστικών παρουσιάσεων (Mentimeter, 2026). Χρησιμοποιήθηκε στο σενάριο στη δραστηριότητα καταιγισμού ιδεών στη φάση Forethought.

Genially: πλατφόρμα διαδραστικού ψηφιακού περιεχομένου (Genially, 2026), όπως παρουσιάσεις, infographics, διαδραστικές εικόνες, κουίζ και εκπαιδευτικά παιχνίδια. Χρησιμοποιήθηκε στο σενάριο για την υλοποίηση του τελικού Escape Room στη φάση του Αναστοχασμού (Self-Reflection).

Lumi: πρόγραμμα ανοιχτού κώδικα για τη δημιουργία και επεξεργασία διαδραστικού εκπαιδευτικού υλικού (H5P) (Lumi, 2026). Χρησιμοποιήθηκε στο σενάριο για τη δημιουργία κουίζ κατανόησης της θεωρίας και για τη δημιουργία σεναρίων διακλάδωσης σε κάθε ενότητα STEAM της φάσης Performance.

Lucidchart: διαδικτυακή εφαρμογή (cloud-based tool) για τη δημιουργία διαγραμμάτων και την οπτικοποίηση δεδομένων (Lucidchart, 2026). Χρησιμοποιήθηκε από τους φοιτητές για τον σχεδιασμό τεχνικών διαγραμμάτων ακολουθίας μιας επίθεσης phishing στην ενότητα Engineering της φάσης Performance.

Fillout: εργαλείο δημιουργίας διαδραστικών φορμών και λιστών ελέγχου (Fillout, 2026). Χρησιμοποιήθηκε στο σενάριο για τη δημιουργία ενός checklist ελέγχου της προόδου των φοιτητών στην ενότητα Mathematics της φάσης Performance.

Google Forms: εργαλείο δημιουργίας ερωτηματολογίων (Google, 2026d). Χρησιμοποιήθηκε για τη συλλογή δεδομένων αυτοαξιολόγησης, ετεροαξιολόγησης και τελικού αναστοχασμού στο σενάριο.

Google Docs: διαδικτυακός επεξεργαστής κειμένου (Google, 2026c). Χρησιμοποιήθηκε στο σενάριο για την παροχή γραπτών οδηγιών και θεωρητικού υλικού.

Google Classroom: πλατφόρμα διαχείρισης μαθήματος (LMS) της Google (Google, 2026b). Χρησιμοποιήθηκε στο σενάριο ως το κεντρικό σημείο ανάθεσης, παράδοσης και αξιολόγησης των εργασιών των φοιτητών.

SPSS: στατιστικό λογισμικό ανάλυσης δεδομένων (IBM, 2026). Χρησιμοποιήθηκε στο σενάριο για τον έλεγχο αξιοπιστίας (Cronbach's alpha) και τη συσχέτιση μεταβλητών στο πλαίσιο της δραστηριότητας της στατιστικής ανάλυσης ερωτηματολογίου, στην ενότητα Mathematics της φάσης Performance.

DaVinci Resolve: λογισμικό επεξεργασίας βίντεο (Blackmagic Design, 2026). Χρησιμοποιήθηκε για την επεξεργασία και το μοντάζ των εκπαιδευτικών βίντεο του σεναρίου.

Pixabay: διαδικτυακή πλατφόρμα δωρεάν, ελεύθερων πνευματικών δικαιωμάτων εικόνων, βίντεο και μουσικής (Pixabay, 2026), η οποία χρησιμοποιήθηκε στο σενάριο ως πηγή μουσικής υπόκρουσης για τα εκπαιδευτικά βίντεο.

2.8 Εργαλεία Τεχνητής Νοημοσύνης

Στο παρόν e-course αξιοποιήθηκαν επιλεκτικά εργαλεία τεχνητής νοημοσύνης, με αποκλειστικά υποστηρικτικό ρόλο στη δημιουργία περιεχομένου, καθώς κάθε δημιουργημένο περιεχόμενο εξετάστηκε και τροποποιήθηκε από τον συγγραφέα πριν από την οριστική του ένταξη στη σελίδα.

Hedra AI: εργαλείο δημιουργίας ψηφιακών avatar με κίνηση προσώπου (Hedra, 2026). Χρησιμοποιήθηκε στο σενάριο για τη δημιουργία του avatar της ψηφιακής βοηθού «Σοφία», η οποία παρουσιάζει προκαθορισμένο, σεναριακά γραμμένο περιεχόμενο. Η χρήση οπτικών avatar σε εκπαιδευτικό πλαίσιο έχει συνδεθεί με ενίσχυση του ενδιαφέροντος και της παρακίνησης των εκπαιδευομένων (Baylor, 2011; Fink et al., 2024).

Google AI Studio: πλατφόρμα της Google για ανάπτυξη εφαρμογών τεχνητής νοημοσύνης (Google, 2026a). Χρησιμοποιήθηκε στο σενάριο για τη μετατροπή κειμένου σε ομιλία (text-to-speech) στα εκπαιδευτικά βίντεο. Η ενσωμάτωση εργαλείων Google AI σε υπηρεσίες πληροφόρησης και εκπαίδευσης συζητείται ως πρακτική εφαρμογή τεχνητής νοημοσύνης με πρακτικό όφελος στην παραγωγή περιεχομένου (K.C & Aravind, 2024).

Lovable AI: εργαλείο δημιουργίας ψηφιακού περιεχομένου και διαδραστικών εφαρμογών (Lovable, 2026). Χρησιμοποιήθηκε για τη δημιουργία του rule-based chatbot οδηγιών της Σοφίας στην αρχική σελίδα (Home Page), όπου παρουσιάζονται πληροφορίες για το e-course μέσω προκαθορισμένων ερωτήσεων και απαντήσεων, καθώς και για τη δημιουργία ενός θεωρητικού διαγράμματος ακολουθίας στην ενότητα Engineering της φάσης Performance. Έρευνα σε φοιτητές τριτοβάθμιας εκπαίδευσης εξέτασε την αποδοχή rule-based εκπαιδευτικών chatbot ως εναλλακτικής μορφής υποστήριξης, με ενθαρρυντικά αποτελέσματα ως προς τη χρηστικότητα και την αντιληπτή χρησιμότητά τους (Güldal & Dinçer, 2025).

Base44 AI: εργαλείο δημιουργίας διαδραστικών ψηφιακών εφαρμογών (Base44, 2026). Χρησιμοποιήθηκε στο σενάριο για τη δημιουργία διαδραστικών σελίδων, όπως το Timeline, ο διαδραστικός χάρτης phishing στη φάση Forethought και ο εννοιολογικός χάρτης στην ενότητα Science της φάσης Performance.

NotebookLM: εργαλείο της Google για σύνθεση περιεχομένου με τεχνητή νοημοσύνη (Google, 2026e). Χρησιμοποιήθηκε για τη δημιουργία ενός εκπαιδευτικού βίντεο στην ενότητα Science της φάσης Performance. Πρόσφατη μελέτη σε πλαίσιο τριτοβάθμιας εκπαίδευσης περιγράφει τη δυνατότητά του να λειτουργεί ως προσωπικός βοηθός μελέτης, συνοψίζοντας σημειώσεις και διευκρινίζοντας έννοιες μέσα από το υλικό του μαθήματος (Reyna, 2025).

Claude AI: συνομιλητικό εργαλείο τεχνητής νοημοσύνης (Anthropic, 2026). Χρησιμοποιείται από τους φοιτητές ως πηγή διευκρινίσεων κατά τη μελέτη τους στις ομάδες ειδικών. Η χρήση AI chatbots σε εκπαιδευτικό πλαίσιο έχει μελετηθεί ως εργαλείο υποστήριξης της μάθησης, με οφέλη στην άμεση πρόσβαση σε πληροφορίες αλλά και προκλήσεις ως προς την ακρίβεια του περιεχομένου (Davar et al., 2025).

ChatGPT: συνομιλητικό εργαλείο τεχνητής νοημοσύνης (OpenAI, 2026). Χρησιμοποιήθηκε στο σενάριο για τη δημιουργία φωτογραφιών που ενσωματώθηκαν στο περιβάλλον του Wix.

2.9 Περίληψη

Το παρόν κεφάλαιο παρουσίασε τους θεωρητικούς πυλώνες στους οποίους θεμελιώνεται η διαμόρφωση του e-course. Η Αυτορρυθμιζόμενη Μάθηση, μέσω του κυκλικού μοντέλου του Zimmerman, προσέφερε τον δομικό σκελετό του σεναρίου. Οι τρεις δείκτες αξιολόγησης, η γνωστική εμπλοκή, η μεταγνωστική παρακολούθηση και η κατανόηση της οπτικής των συνεργατών, αντιστοιχούν στο SRL, στη STEAM και στις συνεργατικές στρατηγικές, συνδέοντάς τα με τους στόχους αξιολόγησης της παρέμβασης. Η STEAM συνδέθηκε επιπλέον με το πεδίο της κυβερνοασφάλειας, αναδεικνύοντας τη διεπιστημονική της αξία για την κατανόηση απειλών όπως το phishing. Το τεχνολογικό οικοσύστημα, με κεντρικό άξονα το Wix και υποστηρικτικά εργαλεία Web 2.0 και τεχνητής νοημοσύνης, παρείχε το πλαίσιο υλοποίησης όλων των παραπάνω θεωρητικών αρχών σε ένα ενιαίο, ασύγχρονο μαθησιακό περιβάλλον.

ΚΕΦΑΛΑΙΟ 3: ΜΕΘΟΔΟΛΟΓΙΑ

3.1 Στόχος ερευνητικής προσέγγισης

Στόχος της παρούσας εργασίας είναι ο σχεδιασμός και η ανάπτυξη ενός ηλεκτρονικού μαθήματος κυβερνοασφάλειας, το οποίο θα βοηθήσει τους φοιτητές να αναγνωρίζουν και να αντιμετωπίζουν επιθέσεις phishing, μέσα από θεωρητική εκπαίδευση, τεχνική ανάλυση, σχεδιασμό διαγραμμάτων, οπτική αναγνώριση παραπλάνησης και ανάλυση δεδομένων.

Για την υλοποίηση αυτού του στόχου, το μάθημα αξιοποιεί το μοντέλο της αυτορρυθμιζόμενης μάθησης (SRL), την προσέγγιση STEAM και υποστηρικτικά εργαλεία τεχνητής νοημοσύνης.

3.2 Εννοιολογικοί και λειτουργικοί Ορισμοί

Τρία ερευνητικά ερωτήματα δίνουν τους βασικούς δείκτες της μελέτης, τη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση και την κατανόηση της οπτικής των άλλων μελών της ομάδας. Οι εννοιολογικοί και λειτουργικοί ορισμοί παρουσιάζονται αναλυτικά στη συνέχεια.

Ο εννοιολογικός ορισμός περιγράφει το θεωρητικό περιεχόμενο κάθε δείκτη με βάση την επιστημονική βιβλιογραφία, ενώ ο λειτουργικός ορισμός προσδιορίζει τις ενέργειες των φοιτητών και τις δραστηριότητες του e-course που θα χρησιμοποιηθούν για την αξιολόγησή τους. Αξίζει να σημειωθεί ότι καθώς δεν έχει γίνει ακόμη εφαρμογή σε πραγματικό δείγμα φοιτητών, πρόκειται για ένα προτεινόμενο πλαίσιο μελλοντικής αξιολόγησης.

Πίνακας 5: Εννοιολογικός και λειτουργικός ορισμός της Γνωστικής Εμπλοκής

Εννοιολογικός Ορισμός	Λειτουργικός Ορισμός
Η γνωστική εμπλοκή αναφέρεται στον βαθμό στον οποίο ο εκπαιδευόμενος επεξεργάζεται σε βάθος το μαθησιακό περιεχόμενο, εφαρμόζει στρατηγικές ανάλυσης και κριτικής σκέψης, συνδέει διαφορετικές πληροφορίες και τεκμηριώνει τις αποφάσεις του, αντί να μένει σε επιφανειακή εκτέλεση της δραστηριότητας (Redmond et al., 2018; Shi et al., 2026).	Ο δείκτης της γνωστικής εμπλοκής μετριέται από το κατά πόσο ο φοιτητής: • Εφαρμόζει κατάλληλες τεχνικές, εργαλεία και μεθόδους για τον έλεγχο, την επαλήθευση και τη μέτρηση απειλών phishing. • Αναλύει στοιχεία, δεδομένα και δείκτες σχετικούς με το phishing, εντοπίζοντας αδυναμίες ή συσχετίσεις και εξάγοντας τεκμηριωμένα συμπεράσματα. • Αξιολογεί την επικινδυνότητα και την τρωτότητα σε επιθέσεις phishing, με βάση ποιοτικά και ποσοτικά στοιχεία. • Σχεδιάζει τεχνικά διαγράμματα, οπτικά δολώματα και γραφήματα αναπαράστασης στατιστικών δεδομένων. Η γνωστική εμπλοκή μετριέται σε δραστηριότητες όπως: • Το Content Study-Practice στην ενότητα Technology. • Η Επιθεώρηση URL στην ενότητα Technology και η ανάλυση ύποπτου email στην ενότητα Science. • Η αξιολόγηση επικινδυνότητας στις ενότητες Science και Mathematics. • Ο σχεδιασμός διαγράμματος ακολουθίας στην ενότητα Engineering, το Design Lab στην ενότητα Arts, και ο σχεδιασμός γραφημάτων στο SPSS στην ενότητα Mathematics. Ο δείκτης αυτός συνδέεται με το ερευνητικό ερώτημα RQ1.

Πίνακας 6: Εννοιολογικός και λειτουργικός ορισμός της Μεταγνωστικής Παρακολούθησης

Εννοιολογικός Ορισμός	Λειτουργικός Ορισμός
Η μεταγνωστική παρακολούθηση αφορά τη συνειδητή παρατήρηση και τον έλεγχο της κατανόησης, της προόδου και των στρατηγικών του εκπαιδευόμενου κατά την εκτέλεση ενός μαθησιακού έργου. Στη φάση της εκτέλεσης του μοντέλου της Αυτορρυθμιζόμενης Μάθησης, ο εκπαιδευόμενος παρακολουθεί την πορεία του, αναγνωρίζει δυσκολίες και προσαρμόζει τις ενέργειές του όταν χρειάζεται (Wagener, 2016; Zimmerman, 2002).	Ο δείκτης της μεταγνωστικής παρακολούθησης μετριέται από το κατά πόσο ο φοιτητής: • Παρακολουθεί και καταγράφει την πρόοδό του σε σχέση με τους στόχους της δραστηριότητας. • Αναγνωρίζει λάθη και δυσκολίες που χρειάζονται βελτίωση. • Διαχειρίζεται τον χρόνο και τα επιμέρους βήματα της εργασίας του. • Προσαρμόζει τις στρατηγικές του και αναστοχάζεται πάνω στις ενέργειες και αποφάσεις του όταν αυτές δεν αποδίδουν. Η μεταγνωστική παρακολούθηση μετριέται σε δραστηριότητες όπως: • Η διαχείριση χρόνου μέσω του Trello και η αυτοκαταγραφή μέσω του Evernote σε όλες τις ενότητες STEAM. • Η Αρχική και Τελική Αυτοαξιολόγηση Δεξιοτήτων (Skills Self-Check Pre/Post) στις φάσεις Forethought και Self-Reflection. • Ο Τελικός αναστοχασμός στη φάση Self-Reflection. Ο δείκτης αυτός συνδέεται με το ερευνητικό ερώτημα RQ2.

Πίνακας 7: Εννοιολογικός και Λειτουργικός Ορισμός της κατανόησης της οπτικής των άλλων

Εννοιολογικός Ορισμός	Λειτουργικός Ορισμός
Η κατανόηση της οπτικής των άλλων μελών της ομάδας αναφέρεται στην ικανότητα του εκπαιδευομένου να εξετάζει ένα πρόβλημα λαμβάνοντας υπόψη τη θέση και τις συνεισφορές των συνεργατών του και να προσαρμόζει ανάλογα τη σκέψη και την επικοινωνία του (Hesse et al., 2015).	Ο δείκτης της κατανόησης της οπτικής των άλλων μετريέται από το κατά πόσο ο φοιτητής: • Ακούει τις απόψεις των συνεργατών του, αναγνωρίζοντας ότι μπορεί να διαθέτουν διαφορετικές πληροφορίες ή ειδίκευση. • Συγκρίνει τη δική του ερμηνεία με των άλλων, αιτιολογώντας τη συμφωνία ή τη διαφωνία του. • Ενσωματώνει χρήσιμα στοιχεία από τις απόψεις των άλλων στην τελική λύση. • Συμβάλλει στη διαμόρφωση μιας κοινής και τεκμηριωμένης ομαδικής απόφασης. Η κατανόηση της οπτικής των άλλων μετρίεται σε δραστηριότητες όπως: • Η στρατηγική Jigsaw στην Engineering και το συνεργατικό στάδιο της Πυραμίδας στη Science. • Τα συνεργατικά στάδια του Think-Pair-Share στην Technology και στην Arts, και το Brainstorming στη φάση Forethought. • Οι δραστηριότητες Peer Evaluation/Assessment στις ενότητες Engineering, Arts και Mathematics. Ο δείκτης αυτός συνδέεται με το ερευνητικό ερώτημα RQ3.

3.3 Τα Ερευνητικά Ερωτήματα

Με βάση τον στόχο της παρούσας ερευνητικής προσέγγισης, διαμορφώνονται τα ακόλουθα ερευνητικά ερωτήματα, τα οποία αντιστοιχούν στους τρεις βασικούς δείκτες που εξετάζονται στο πλαίσιο του e-course.

- **RQ1:** Σε ποιο βαθμό το e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα» συμβάλλει στην ενίσχυση της γνωστικής εμπλοκής (cognitive engagement) των φοιτητών κατά την ανάλυση των Case Studies phishing;
- **RQ2:** Σε ποιο βαθμό το e-course συμβάλλει στην ενίσχυση της μεταγνωστικής παρακολούθησης (metacognitive monitoring) των φοιτητών κατά την εκτέλεση των δραστηριοτήτων;
- **RQ3:** Σε ποιο βαθμό το e-course συμβάλλει στην κατανόηση της οπτικής των άλλων μελών της ομάδας (perspective taking) κατά τις συνεργατικές δραστηριότητες;

3.4 Η περιγραφή της διαδικασίας της έρευνας

Η παρούσα εργασία οργανώνεται ως διαδικασία σχεδιασμού και ανάπτυξης ενός ασύγχρονου ηλεκτρονικού μαθήματος κυβερνοασφάλειας και όχι ως εφαρμοσμένη έρευνα σε πραγματικό δείγμα φοιτητών. Η διαδικασία εστιάζει στη θεωρητική θεμελίωση, στον παιδαγωγικό και τεχνολογικό σχεδιασμό του e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα» και στη διαμόρφωση ενός πλαισίου για τη μελλοντική αξιολόγησή του. Το μάθημα απευθύνεται σε φοιτητές, αναπτύσσεται στην πλατφόρμα Wix και έχει διάρκεια επτά εβδομάδων, με συνολικό φόρτο εργασίας δεκατεσσάρων ωρών και ενδεικτική απασχόληση δύο ωρών ανά εβδομάδα.

Η διαδικασία μάθησης πραγματοποιείται εξ ολοκλήρου ασύγχρονα. Οι φοιτητές μελετούν το διδακτικό υλικό, εκτελούν τις ατομικές και ομαδικές δραστηριότητες και καταγράφουν την πρόοδό τους σε εβδομαδιαία βάση και προχωρούν στον δικό τους ρυθμό. Ο εκπαιδευτικός διατηρεί ρόλο επίβλεψης και οργάνωσης, χωρίς να απαιτείται η παρουσία του κατά την πραγματοποίηση των δραστηριοτήτων. Τα εργαλεία τεχνητής νοημοσύνης αξιοποιούνται υποστηρικτικά, όπου προβλέπεται από τον σχεδιασμό, για την παροχή οδηγιών και σημαντικών επεξηγήσεων.

Η διαδικασία του σχεδιασμού περιλαμβάνει έξι διαδοχικά βήματα. Αρχικά πραγματοποιείται η θεωρητική τεκμηρίωση του προβλήματος και προσδιορίζεται η ανάγκη ανάπτυξης δεξιοτήτων αναγνώρισης και αντιμετώπισης επιθέσεων phishing. Στη συνέχεια καθορίζονται ο σκοπός, οι τρεις ερευνητικοί δείκτες και τα αντίστοιχα ερευνητικά ερωτήματα. Ακολουθεί η διατύπωση των μαθησιακών στόχων και των λειτουργικών ορισμών. Έπειτα οργανώνεται ο εκπαιδευτικός σχεδιασμός με βάση τις φάσεις της Αυτορρυθμιζόμενης Μάθησης και τις πέντε ενότητες STEAM, συμπεριλαμβανομένων των συνεργατικών στρατηγικών. Ακολουθεί ο σχεδιασμός των επιμέρους δραστηριοτήτων και η ανάπτυξη του ψηφιακού περιβάλλοντος στο Wix. Το τελευταίο στάδιο αφορά στη διαμόρφωση του πλαισίου μελλοντικής εφαρμογής και αξιολόγησης.

Τα βήματα του ερευνητικού σχεδιασμού παρουσιάζονται στο κάτωθεν σχήμα.



Σχήμα 2: Βήματα ερευνητικού σχεδιασμού

Οι μαθησιακοί στόχοι κωδικοποιούνται, ώστε να αποτυπώνεται με σαφήνεια η σχέση ανάμεσα στις επιδιωκόμενες γνώσεις και δεξιότητες, στις δραστηριότητες του e-course και στα ερευνητικά ερωτήματα. Οι στόχοι ΜΣ-1 έως ΜΣ-6 ακολουθούν την ταξινομία του Bloom από την αναγνώριση έως τη δημιουργία, ενώ ο στόχος ΜΓΣ-1 αφορά τη μεταγνωστική παρακολούθηση και ο στόχος ΚΣ-1 τη συνεργατική δράση και την κατανόηση της οπτικής των άλλων.

Πίνακας 8: Κωδικοποιημένοι μαθησιακοί στόχοι του e-course

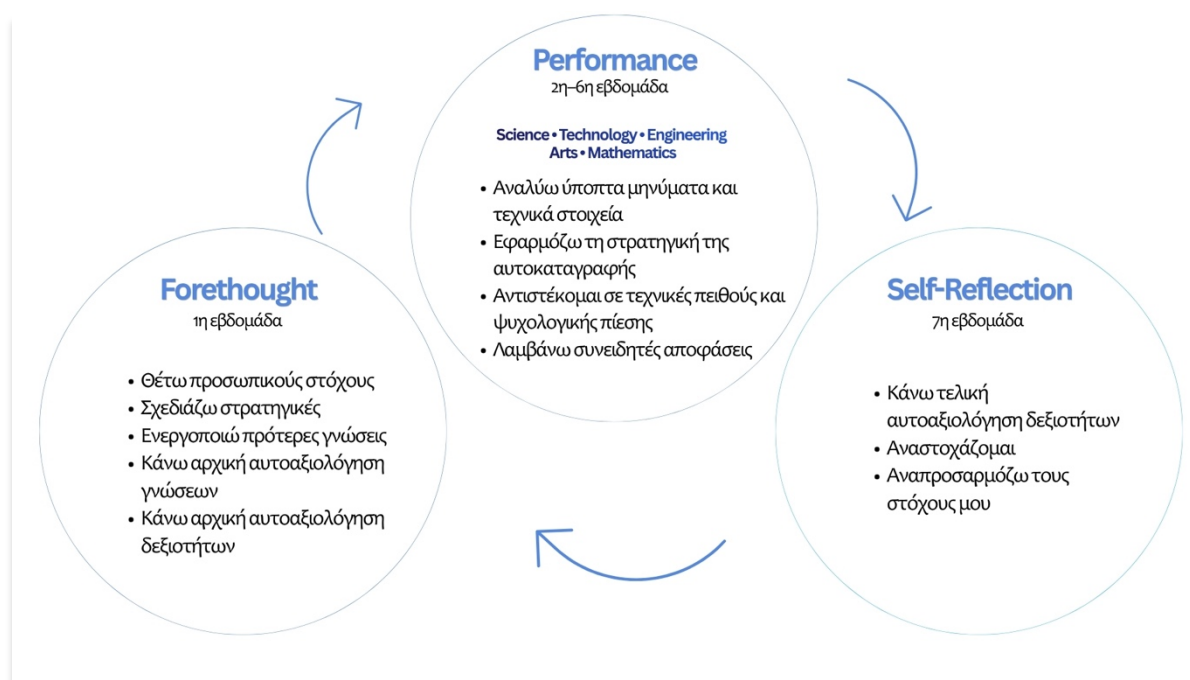
Κωδικός στόχου	Περιγραφή στόχου
ΜΣ-1 (Remember)	Να αναγνωρίζουν και να κατονομάζουν τις βασικές αρχές, τα εργαλεία και τους τεχνικούς όρους μιας επίθεσης phishing.
ΜΣ-2 (Understand)	Να κατανοούν τη μεθοδολογία και τη λειτουργία των επιμέρους σταδίων μιας επίθεσης phishing.
ΜΣ-3 (Apply)	Να εφαρμόζουν τις κατάλληλες τεχνικές, εργαλεία και μεθόδους για τον έλεγχο, την επαλήθευση και τη μέτρηση απειλών phishing.
ΜΣ-4 (Analyze)	Να αναλύουν στοιχεία, δεδομένα και δείκτες σχετικούς με το phishing, εντοπίζοντας αδυναμίες ή συσχετίσεις και εξάγοντας τεκμηριωμένα συμπεράσματα.
ΜΣ-5 (Evaluate)	Να αξιολογούν την επικινδυνότητα και την τρωτότητα σε επιθέσεις phishing, με βάση ποιοτικά και ποσοτικά δεδομένα.
ΜΣ-6 (Create)	Να σχεδιάζουν και να κατασκευάζουν τεχνικά διαγράμματα, οπτικά δολώματα και γραφήματα αναπαράστασης στατιστικών δεδομένων.
ΜΓΣ-1 (Μεταγνωστικός)	Να παρακολουθούν συνειδητά τη μαθησιακή τους πορεία, εντοπίζοντας δυσκολίες και προσαρμόζοντας τις στρατηγικές τους κατά τη διάρκεια της εκτέλεσης των δραστηριοτήτων, καθώς και να αυτοαξιολογούνται και να διαμορφώνουν πλάνο μελλοντικών στόχων βασισμένο στον αναστοχασμό τους.
ΚΣ-1 (Κοινωνικο-συναισθηματικός Στόχος)	Να συνεργάζονται αποτελεσματικά σε ομαδικές δραστηριότητες, κατανοώντας και αξιοποιώντας τις διαφορετικές οπτικές των συνεργατών τους.

Η αντιστοίχιση των στόχων με τις φάσεις και τις δραστηριότητες εξασφαλίζει ότι κάθε ερευνητικός δείκτης συνδέεται με συγκεκριμένες μαθησιακές ενέργειες. Οι στόχοι γνώσης και κατανόησης λειτουργούν ως προαπαιτούμενο υπόβαθρο, ενώ οι στόχοι εφαρμογής, ανάλυσης, αξιολόγησης και δημιουργίας συνδέονται κυρίως με τη γνωστική εμπλοκή. Η μεταγνωστική παρακολούθηση ενεργοποιείται μέσα από εργαλεία καταγραφής και αναστοχασμού, ενώ η κατανόηση της οπτικής των άλλων καλλιεργείται μέσα από τις συνεργατικές στρατηγικές.

Πίνακας 9: Αντιστοίχιση στόχων με φάσεις εφαρμογής και ερευνητικά ερωτήματα

Κωδικός Στόχου	Κύρια φάση / Δραστηριότητα	Σχετιζόμενο RQ
ΜΣ-1	Θεωρητική παρουσίαση, εισαγωγικά βίντεο και κουίζ γνώσεων στη φάση Forethought και στις ενότητες STEAM.	-
ΜΣ-2	Θεωρητική παρουσίαση και κουίζ κατανόησης της θεωρίας σε κάθε ενότητα STEAM.	-
ΜΣ-3	Δοκιμή πραγματικών ιστοσελίδων σε εργαλεία ελέγχου στη δραστηριότητα Πρακτική Μελέτη-Εφαρμογή στην ενότητα Technology καθώς και εφαρμογή τύπων υπολογισμού στη δραστηριότητα Πρακτική Μελέτη-Εφαρμογή και ανάλυση δεδομένων στο SPSS στην ενότητα Mathematics.	RQ1
ΜΣ-4	Επιθεώρηση URL στην ενότητα Technology, ανάλυση ύποπτου email στην ενότητα Science, και ανάλυση δεδομένων στο SPSS στην ενότητα Mathematics.	RQ1
ΜΣ-5	Ερωτήσεις αξιολόγησης επικινδυνότητας στη δραστηριότητα Ατομική Μελέτη της ενότητας Science, και ερωτήσεις αξιολόγησης επικινδυνότητας στην ενότητα Mathematics.	RQ1
ΜΣ-6	Εργαστήριο σχεδιασμού στην ενότητα Arts, σχεδιασμός γραφημάτων στην ενότητα Mathematics, σχεδιασμός διαγράμματος ακολουθίας στην ενότητα Engineering.	RQ1
ΜΓΣ-1	Καθορισμός στόχων στη φάση Forethought, διαχείριση του χρόνου μέσω του Trello σε όλες τις ενότητες STEAM, αυτοκαταγραφή της προόδου μέσω του Evernote σε όλες τις ενότητες STEAM, αρχική και τελική αυτοαξιολόγηση δεξιοτήτων στις φάσεις Forethought και Self-Reflection, σχεδιασμός επόμενων βημάτων στη φάση Self-Reflection.	RQ2
ΚΣ-1	Στρατηγική Jigsaw με ομάδες ειδικών στην ενότητα Engineering, συνεργατικό στάδιο της στρατηγικής της Πυραμίδας στην ενότητα Science, συνεργατικά στάδια της στρατηγικής Think-Pair-Share στις ενότητες Technology και Arts, συνεργατικός καταγισμός ιδεών στη φάση Forethought, αξιολόγηση από ομοτίμους στις ενότητες Engineering, Arts και Mathematics.	RQ3

Η συνολική ροή του e-course βασίζεται στον κυκλικό χαρακτήρα της Αυτορρυθμιζόμενης Μάθησης. Στη φάση Forethought (Προπαρασκευαστική Φάση), η οποία αντιστοιχεί στην πρώτη εβδομάδα, οι φοιτητές γνωρίζουν το περιβάλλον και τον σκοπό του μαθήματος, ενεργοποιούν τις πρότερες γνώσεις τους για το phishing, συμπληρώνουν το pre-test και διαμορφώνουν προσωπικούς μαθησιακούς στόχους. Στη φάση Performance (Εκτελεστική Φάση), από τη δεύτερη έως την έκτη εβδομάδα, προσεγγίζουν το phishing μέσα από τις πέντε διαδοχικές ενότητες STEAM, εφαρμόζουν στρατηγικές ανάλυσης και επίλυσης προβλημάτων, συνεργάζονται και παρακολουθούν συστηματικά την πρόοδό τους. Στη φάση Self-Reflection (Φάση Αναστοχασμού), κατά την έβδομη εβδομάδα, συμπληρώνουν το post-test, αξιολογούν τη μαθησιακή τους πορεία και αναστοχάζονται στις δεξιότητες που ανέπτυξαν. Η διάρθρωση αυτή ακολουθεί τις τρεις κυκλικές φάσεις του μοντέλου (Zimmerman, 2002).



Σχήμα 3: Ο κύκλος της Αυτορρυθμιζόμενης Μάθησης στο e-course

Στο πλαίσιο της ροής του e-course, αξιοποιούνται συγκεκριμένες συνεργατικές στρατηγικές μάθησης: το Jigsaw στην ενότητα Engineering, η Πυραμίδα στην ενότητα Science, το Think-Pair-Share στις ενότητες Technology και Arts, και το Brainstorming στη φάση Forethought.

Η φάση **Performance (Εκτελεστική Φάση)** οργανώνεται σε πέντε διαδοχικές ενότητες, μία για κάθε περιοχή του STEAM.

Στην ενότητα **Science** οι φοιτητές διερευνούν την ψυχολογία της κοινωνικής μηχανικής και τον τρόπο με τον οποίο η εμπιστοσύνη, το συναίσθημα και η ανθρώπινη συμπεριφορά αξιοποιούνται για την παραπλάνηση του χρήστη.

Στην ενότητα **Technology** αναλύουν ύποπτα μηνύματα, συνδέσμους και τεχνικά στοιχεία, ώστε να εντοπίζουν τις ενδείξεις μιας επίθεσης phishing.

Στην ενότητα **Engineering** οργανώνουν τη ροή μιας προσομοιωμένης επίθεσης, σχεδιάζουν τεχνικά διαγράμματα και κατανοούν τη λειτουργία μιας ψηφιακής παγίδας.

Στην ενότητα **Arts** εξετάζουν τον ρόλο της εικόνας, του σχεδιασμού και της οπτικής πειθούς στη δημιουργία παραπλανητικών μηνυμάτων και οπτικών δολωμάτων.

Στην ενότητα **Mathematics** επεξεργάζονται εικονικά δεδομένα ερωτηματολογίου στο SPSS, ελέγχουν αξιοπιστία και συσχέτιση μεταβλητών, και δημιουργούν τα κατάλληλα γραφήματα.

Με αυτόν τον τρόπο, το STEAM ενσωματώνεται οργανικά στη φάση της εκτέλεσης και συνδέεται με τους τρεις ερευνητικούς δείκτες. Η χρονική κατανομή των επτά εβδομάδων οργανώνει τη μετάβαση από τον προσανατολισμό και τη στοχοθεσία στην ενεργή διερεύνηση και, τέλος, στον αναστοχασμό. Κάθε εβδομάδα αντιστοιχεί σε δύο περίπου ώρες ασύγχρονης μελέτης και δραστηριοτήτων. Η 1η εβδομάδα αφιερώνεται στη φάση Forethought, οι εβδομάδες 2–6 στις ενότητες Science, Technology, Engineering, Arts και Mathematics αντίστοιχα και η 7η εβδομάδα στη φάση Self-Reflection. Αυτή η χρονική οργάνωση επιτρέπει στους φοιτητές να προσεγγίσουν το phishing από διαφορετικές επιστημονικές οπτικές, ολοκληρώνοντας τον κύκλο με αναστοχασμό πάνω στη μαθησιακή τους πορεία και αξιολόγηση τόσο της τελικής τους επίδοσης όσο και του ίδιου του εκπαιδευτικού σεναρίου.

3.5 Επιλογή στατιστικών κριτηρίων για τις αναλύσεις

Καθώς το e-course δεν εφαρμόζεται πραγματικά στο πλαίσιο αυτής της εργασίας, δεν έχει νόημα η χρήση πολύπλοκων στατιστικών επαγωγικών ελέγχων. Αντ' αυτού, σε περίπτωση πραγματικής εφαρμογής, η αξιολόγηση θα μπορούσε να στηριχθεί σε περιγραφική στατιστική, δηλαδή στην εξαγωγή ποσοστών για κάθε ερευνητικό ερώτημα (RQ1, RQ2, RQ3) μέσω του Ελέγχου Δεξιοτήτων (pre/post-test), το οποίο περιλαμβάνει ξεχωριστή υποκλίμακα για κάθε έναν από τους τρεις δείκτες, επιτρέποντας τη σύγκριση αρχικής και τελικής βαθμολογίας ανά δείκτη.

Παράλληλα, σε περίπτωση μελλοντικής εφαρμογής του σεναρίου σε πραγματικό δείγμα φοιτητών, θα μπορούσε προαιρετικά να αξιοποιηθεί πιο εκτενής στατιστική ανάλυση. Οι μετρήσεις της αρχικής και της τελικής αξιολόγησης δεξιοτήτων θα μπορούσαν να συγκριθούν μέσω κριτηρίου paired samples t-test, συνοδευόμενου από τον υπολογισμό του μεγέθους επίδρασης Cohen's d, ώστε να τεκμηριωθεί όχι μόνο η στατιστική σημαντικότητα αλλά και το πρακτικό μέγεθος τυχόν βελτίωσης (Lakens, 2013; Rietveld & Van Hout, 2017).

Επιπλέον, δεδομένου ότι ο έλεγχος δεξιοτήτων αποτελείται από πολλαπλές δηλώσεις ανά δείκτη, θα ήταν σκόπιμος ο έλεγχος της εσωτερικής συνέπειας κάθε υποκλίμακας γνωστικής εμπλοκής, μεταγνωστικής παρακολούθησης και κατανόησης της οπτικής των άλλων μέσω του συντελεστή Cronbach's alpha (Gialamas, 2024). Συμπληρωματικά, θα μπορούσε να αξιοποιηθεί δείγμα ειδικών όπως εκπαιδευτικών ή ερευνητών στο πεδίο της κυβερνοασφάλειας και της εκπαιδευτικής τεχνολογίας, στο οποίο θα μπορούσε να δοθεί το σενάριο προς αξιολόγηση μέσω πρόσθετων μετρήσεων, παρέχοντας δεδομένα για την περαιτέρω τεκμηρίωση της ποιότητας του σχεδιασμού.

Τα παραπάνω κριτήρια αποτελούν προτεινόμενο πλαίσιο ανάλυσης για ενδεχόμενη μελλοντική εφαρμογή του σεναρίου.

3.6 Το δείγμα μελέτης

3.6.1 Οι συμμετέχοντες

Η προτεινόμενη εφαρμογή του e-course απευθύνεται σε φοιτητές τριτοβάθμιας εκπαίδευσης, οι οποίοι αποτελούν ιδιαίτερα ευάλωτη ομάδα απέναντι σε επιθέσεις phishing, καθώς η καθημερινότητά τους περιλαμβάνει εκτεταμένη χρήση ψηφιακών υπηρεσιών, ακαδημαϊκών λογαριασμών και διαδικτυακών πλατφορμών (Khader et al., 2021). Παράλληλα, το επίπεδο αυτονομίας και ψηφιακού γραμματισμού που διαθέτουν τους καθιστά κατάλληλους για την παρακολούθηση ενός ασύγχρονου μαθήματος που απαιτεί αυτορρύθμιση και ατομική διαχείριση του ρυθμού μελέτης.

Ως δείγμα προτείνεται ένα ήδη υπάρχον τμήμα ή εργαστηριακή ομάδα 25 έως 30 φοιτητών. Το μέγεθος αυτό επαρκεί για να εξαχθούν ενδεικτικά ποσοστά ανά δείκτη, χωρίς να δημιουργεί δυσκολία στην παρακολούθηση των δραστηριοτήτων στην πράξη.

Η προσέγγιση αυτή αντιστοιχεί σε δειγματοληψία ευκολίας (Etikan et al., 2016), αφού δεν απαιτεί τυχαία επιλογή αλλά αξιοποιεί ένα τμήμα που ήδη λειτουργεί. Προϋπόθεση συμμετοχής αποτελεί η ενήμερη συγκατάθεση των φοιτητών, με εγγυημένη ανωνυμία και προστασία των προσωπικών τους δεδομένων σε κάθε στάδιο της έρευνας.

3.6.2 Οι περιορισμοί της έρευνας

Ο βασικότερος περιορισμός της παρούσας εργασίας αποτελεί το γεγονός ότι μένει στο επίπεδο του σχεδιασμού, χωρίς να έχει δοκιμαστεί σε πραγματικές συνθήκες τάξης. Ό,τι αναφέρεται στη συνέχεια αφορά το πόσο καλά θεμελιωμένο είναι παιδαγωγικά και θεωρητικά το σενάριο και όχι το κατά πόσο αποδεδειγμένα λειτουργεί στην πράξη.

Επιπλέον, ο προτεινόμενος σχεδιασμός μιας ομάδας με μετρήσεις πριν και μετά την παρέμβαση δεν περιλαμβάνει ομάδα ελέγχου, γεγονός που περιορίζει την αιτιώδη ερμηνεία τυχόν βελτίωσης, καθώς δεν μπορεί να αποκλειστεί η επίδραση άλλων παραγόντων εκτός του e-course.

Αξίζει επιπλέον να σημειωθεί ότι ένα τμήμα 25-30 φοιτητών είναι πολύ μικρό για να βγουν συμπεράσματα που να ισχύουν για όλους τους φοιτητές τριτοβάθμιας εκπαίδευσης γενικότερα, κάτι που όποιος εφαρμόσει το σενάριο στο μέλλον θα πρέπει να το έχει υπόψη του.

Η παρακολούθηση του e-course απαιτεί σταθερή πρόσβαση σε υπολογιστή ή tablet με σύνδεση στο διαδίκτυο, ενώ προϋποτίθεται και βασική εξοικείωση των φοιτητών με τα ψηφιακά εργαλεία που αξιοποιούνται, όπως το Trello, το Evernote, το Padlet, το Canva, το Mentimeter και το Genially. Τέλος, ο ασύγχρονος χαρακτήρας του μαθήματος απαιτεί προσωπική πειθαρχία των φοιτητών για την ολοκλήρωση των επτά εβδομάδων εντός των προτεινόμενων χρονικών ορίων.

3.7 Εκπαιδευτικό υλικό και ροή

Στην παρούσα ενότητα αναλύεται το εκπαιδευτικό υλικό και η ροή του e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα», σε δύο επιμέρους υποενότητες. Η πρώτη (3.7.1) περιγράφει συνολικά τη ροή του σεναρίου, δίνοντας μια αφηγηματική εικόνα του τρόπου με τον οποίο συνδέονται οι επτά εβδομάδες με τις τρεις φάσεις της Αυτορρυθμιζόμενης Μάθησης. Η δεύτερη (3.7.2) εστιάζει σε κάθε δραστηριότητα ξεχωριστά, εξηγώντας πώς υλοποιείται μέσα από στρατηγικές αυτορρύθμισης ή συνεργατικές στρατηγικές μάθησης, ποια ψηφιακά εργαλεία και εργαλεία Τεχνητής Νοημοσύνης την υποστηρίζουν, και με ποιον τρόπο αξιολογείται.

3.7.1 Συνολική ροή του e-course (Μακροσενάριο)

Πριν την είσοδο στο ίδιο το εκπαιδευτικό μοντέλο, το e-course περιλαμβάνει τέσσερις σελίδες πλοήγησης, οι οποίες λειτουργούν υποστηρικτικά και δεν εντάσσονται στις τρεις φάσεις της Αυτορρυθμιζόμενης Μάθησης. Στην αρχική σελίδα (Home Page), ο φοιτητής παρακολουθεί σύντομο βίντεο με τον ψηφιακό AI οδηγό «Σοφία» και επιλέγει ανάμεσα σε δύο κατευθύνσεις: τις οδηγίες χρήσης του e-course ή την απευθείας είσοδο σε αυτό. Η σελίδα χρονοδιαγράμματος (Timeline) τον ενημερώνει διαδραστικά για το περιεχόμενο και τους στόχους κάθε εβδομάδας, ενώ η σελίδα οδικού χάρτη (Road Map) αποτυπώνει οπτικά ολόκληρη τη διαδρομή του σεναρίου, προσφέροντας άμεση πρόσβαση σε κάθε επιμέρους φάση. Τέλος, η σελίδα «Communication Station» λειτουργεί ως χώρος επικοινωνίας μεταξύ των φοιτητών και ανατροφοδότησης από τον διδάσκοντα, μέσω δύο αντίστοιχων ενοτήτων συζήτησης.

Το e-course «Phishing 360^ο: Από το Συναίσθημα στα Δεδομένα» αναπτύσσεται σε επτά εβδομάδες, συνολικής διάρκειας δεκατεσσάρων ωρών. Κατά την πρώτη εβδομάδα, η οποία αντιστοιχεί στη φάση **Forethought (Προπαρασκευαστική Φάση)**, οι φοιτητές παρακολουθούν αρχικά ένα εισαγωγικό βίντεο που τους γνωρίζει με το περιβάλλον και τον σκοπό του μαθήματος, και στη συνέχεια εξερευνούν έναν διαδραστικό χάρτη phishing, ο οποίος τους εισάγει στις βασικές μορφές της απειλής. Συμπληρώνουν μια αρχική φόρμα αυτοαξιολόγησης γνώσεων, και στη συνέχεια θέτουν τους προσωπικούς τους μαθησιακούς στόχους μέσα από δραστηριότητα καθορισμού στόχων στο Padlet. Ακολουθεί μια ομαδική δραστηριότητα καταιγισμού ιδεών, καθώς και δραστηριότητα με παιχνίδια αναγνώρισης phishing, όπου οι φοιτητές αναλύουν ατομικά σενάρια απειλών. Η φάση ολοκληρώνεται με ένα κουίζ γνώσεων για το phishing και με τη συμπλήρωση της Αρχικής αξιολόγησης Δεξιοτήτων, ενός ερωτηματολογίου που αποτυπώνει την αρχική αυτοαντίληψη των φοιτητών ως προς τη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση και την κατανόηση της οπτικής των άλλων.

Από τη δεύτερη έως την έκτη εβδομάδα εκτείνεται η φάση **Performance (Εκτελεστική Φάση)**, κατά την οποία το phishing προσεγγίζεται διαδοχικά μέσα από τις πέντε επιστημονικές οπτικές της προσέγγισης STEAM: την Επιστήμη, την Τεχνολογία, τη Μηχανική, τις Τέχνες και τα Μαθηματικά. Στην ενότητα Επιστήμης οι φοιτητές μελετούν την ψυχολογία της κοινωνικής μηχανικής και τον τρόπο με τον οποίο οι επιθέσεις phishing αξιοποιούν την εμπιστοσύνη, το συναίσθημα και την ανθρώπινη συμπεριφορά για να παραπλανήσουν τον χρήστη. Στην ενότητα Τεχνολογίας οι φοιτητές αναλύουν ύποπτα μηνύματα, συνδέσμους και τεχνικά στοιχεία, ώστε να κατανοήσουν πώς εντοπίζονται οι βασικές ενδείξεις μιας επίθεσης phishing. Στην ενότητα Μηχανικής οι φοιτητές οργανώνουν τη ροή μιας προσομοιωμένης επίθεσης, σχεδιάζουν τεχνικά διαγράμματα και διερευνούν τη λειτουργία μιας ψηφιακής παγίδας μέσα σε ασφαλές εκπαιδευτικό περιβάλλον. Στην ενότητα Τεχνών οι φοιτητές εξετάζουν τον ρόλο της εικόνας, του σχεδιασμού και της οπτικής πειθούς στη δημιουργία παραπλανητικών μηνυμάτων και ψηφιακών δολωμάτων. Στην ενότητα Μαθηματικών επεξεργάζονται εικονικά δεδομένα ερωτηματολογίου στο SPSS, ελέγχουν αξιοπιστία και συσχέτιση μεταβλητών, και δημιουργούν τα κατάλληλα γραφήματα.

Στη φάση **Self-Reflection (Φάση Αναστοχασμού)**, κατά την έβδομη εβδομάδα, οι φοιτητές ολοκληρώνουν το πρόγραμμα μέσω τελικού διαδραστικού τεστ στο Genially (Escape Room), για την επικύρωση των γνώσεων που απέκτησαν. Στη συνέχεια, συμπληρώνουν ένα ερωτηματολόγιο αναστοχασμού πάνω στη μαθησιακή πορεία και τις επιλογές τους και μετά καταγράφουν στο Padlet τους επόμενους μαθησιακούς στόχους τους. Ακολουθεί το post-test μέσω της τελικής αξιολόγησης δεξιοτήτων, ώστε να αξιολογήσουν την πρόοδό τους και την επίτευξη των στόχων τους σε σύγκριση με το αρχικό pre-test που συμπλήρωσαν στη φάση 1 (Forethought). Η φάση κλείνει με τη συμπλήρωση ερωτηματολογίου αξιολόγησης του σχεδίου δράσης, και ολοκληρώνεται με την απονομή πιστοποιητικού παρακολούθησης, το οποίο αναγνωρίζει την επιτυχή ολοκλήρωση του προγράμματος από τους φοιτητές.

Σε όλη τη διάρκεια του σεναρίου, οι δραστηριότητες συνδέονται με τους ακόλουθους κωδικοποιημένους μαθησιακούς στόχους:

Γνωστικοί Μαθησιακοί Στόχοι

ΜΣ-1: Να αναγνωρίζουν και να κατονομάζουν τις βασικές αρχές, τα εργαλεία και τους τεχνικούς όρους μιας επίθεσης phishing.

ΜΣ-2: Να κατανοούν τη μεθοδολογία και τη λειτουργία των επιμέρους σταδίων μιας επίθεσης phishing.

ΜΣ-3: Να εφαρμόζουν τις κατάλληλες τεχνικές, εργαλεία και μεθόδους για τον έλεγχο, την επαλήθευση και τη μέτρηση απειλών phishing.

ΜΣ-4: Να αναλύουν τα στοιχεία, δεδομένα και δείκτες σχετικούς με το phishing, εντοπίζοντας αδυναμίες ή συσχετίσεις και εξάγοντας τεκμηριωμένα συμπεράσματα.

ΜΣ-5: Να αξιολογούν την επικινδυνότητα και την τρωτότητα σε επιθέσεις phishing, με βάση ποιοτικά και ποσοτικά δεδομένα.

ΜΣ-6: Να σχεδιάζουν και να κατασκευάζουν τεχνικά διαγράμματα, οπτικά δολώματα και γραφήματα αναπαράστασης στατιστικών δεδομένων.

Μεταγνωστικός Στόχος

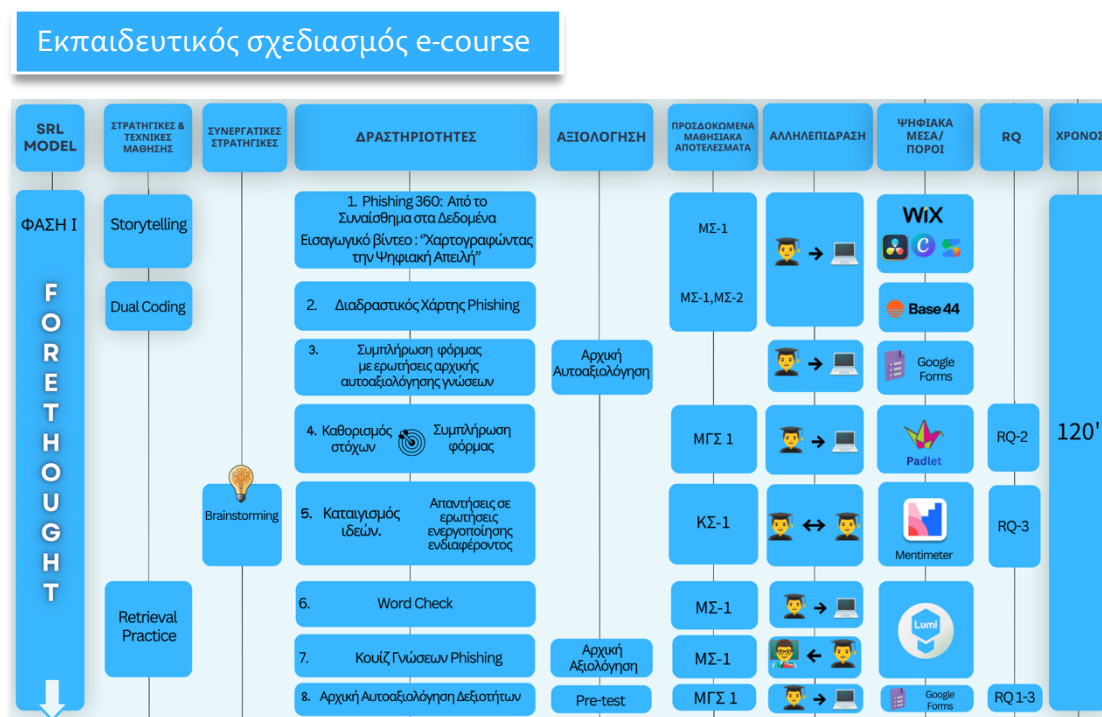
ΜΓΣ-1: Να παρακολουθούν συνειδητά τη μαθησιακή τους πορεία, εντοπίζοντας δυσκολίες και προσαρμόζοντας τις στρατηγικές τους κατά τη διάρκεια της εκτέλεσης των δραστηριοτήτων, καθώς και να αυτοαξιολογούνται και να διαμορφώνουν πλάνο μελλοντικών στόχων βασισμένο στον αναστοχασμό τους.

Κοινωνικό-Συναισθηματικός Στόχος

ΚΣ-1: Να συνεργάζονται αποτελεσματικά σε ομαδικές δραστηριότητες, κατανοώντας και αξιοποιώντας τις διαφορετικές οπτικές των συνεργατών τους.

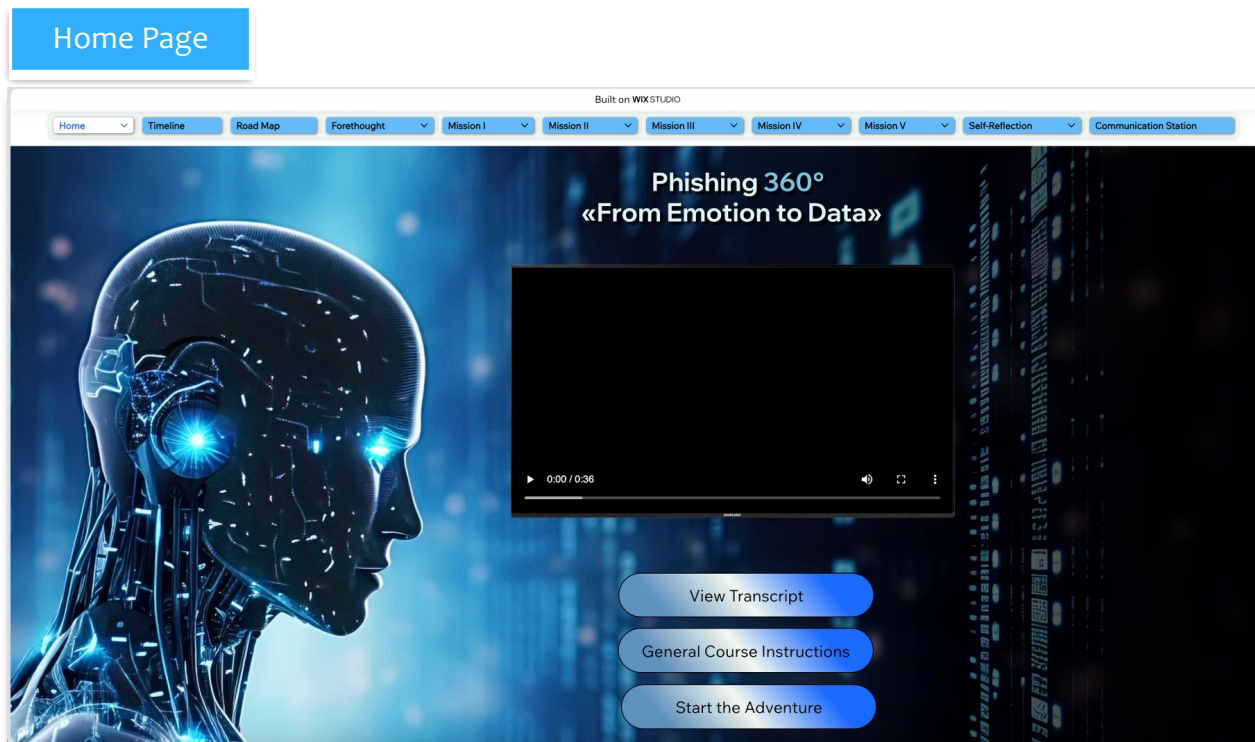
3.7.2 Ανάλυση Εκπαιδευτικού Σχεδιασμού (Μικροσενάριο)

Το σενάριο αναπτύχθηκε στην ψηφιακή πλατφόρμα Wix, ακολουθώντας την προσέγγιση STEAM σε συνδυασμό με το μοντέλο της αυτορρυθμιζόμενης μάθησης. Το σενάριο περιλαμβάνει συνεργατικές στρατηγικές όπως το Jigsaw, το Think-Pair-Share, την Πυραμίδα και τον Καταιγισμό ιδεών και είναι σχεδιασμένο για πλήρως ασύγχρονη παρακολούθηση. Σύνδεσμος e-course: <https://gkonstantakis.wixstudio.com/education>



SRL MODEL	ΣΤΡΑΤΗΓΙΚΕΣ & ΤΕΧΝΙΚΕΣ ΜΑΘΗΣΗΣ	ΣΥΝΕΡΓΑΤΙΚΕΣ ΣΤΡΑΤΗΓΙΚΕΣ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΑΞΙΟΛΟΓΗΣΗ	ΠΡΟΣΔΟΚΩΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ	ΑΛΛΗΛΕΠΙΔΡΑΣΗ	ΨΗΦΙΑΚΑ ΜΕΣΑ/ ΠΟΡΟΙ	RQ	ΧΡΟΝΟΣ
ΦΑΣΗ II P E R F O R M A N C E ↓	Concrete Examples Dual Coding Scaffolding Retrieval Practice Reflective Learning Diaries	Pyramid 1. Ατομική μελέτη 2. Σύγκριση των λύσεων και πρόταση νέων 3. Παρουσίαση τελικής λύσης	9. Ενότητα: S-Science (Η Ψυχολογία της Κοινωνικής Μηχανικής) 9. Εισαγωγικό Βίντεο 9.1 Διαδραστικός εννοιολογικός χάρτης 9.2 Ατομική Μελέτη 9.3 Διαχείριση χρόνου & ρυθμού μάθησης 9.4 Case study I (Simulation spear-phishing) 9.5 Ανάλυση ύποπτου email 9.6 Συχνές Ερωτήσεις & Διευκρινίσεις 9.7 Οδηγός Κατανόησης Θεωρίας 9.8 Αυτοκαταγραφή	Διαμορφωτική Αξιολόγηση	ΜΣ-1 ΜΣ-2 ΜΓΣ-1 ΜΣ-4 ΜΣ-5 ΚΣ-1 ΜΓΣ-1	→ ↔ ↔ ↔ ↔ →	NotebookLM Base 44 Trello Google Docs Lumi Padlet Claude AI Evernote	RQ1 RQ2 RQ3	120'
	Concrete Examples Think Aloud Dual Coding Retrieval Practice Reflective Learning Diaries Στοχοθεσία	Think Pair Share	10. Ενότητα T-Technology Τεχνικά μέσα και επικοινωνία-phishing 10. Θωρηκτική Παρουσίαση 10.1 Μελέτη Περιεχομένου και Εξάσκηση 10.2 Διαχείριση Χρόνου 10.3 Case study II (Τεχνικός Έλεγχος) 10.4 Επιθεώρηση URL 10.5 Κουίζ Κατανόησης Θεωρίας 10.6 Αυτοκαταγραφή 10.7 Καθορισμός νέων στόχων	Διαμορφωτική Αξιολόγηση	ΜΣ-1 ΜΣ-2 ΜΓΣ-1 ΜΓΣ-2 ΜΣ-3 ΜΣ-4 ΚΣ-1 ΜΓΣ-1	→ ↔ ↔ ↔ ↔ →	Wix Google Docs Padlet Trello Lumi Evernote Padlet	RQ1 RQ2 RQ3	120'
	Dual Coding Concrete Examples	Jigsaw Initial teams	11. Ενότητα E-Engineering Digital Architects. Στήνοντας το Δίκτυο 11. Βίντεο Εισαγωγής 11.1 Διάγραμμα Ακολουθίας 11.2 Ατομική Μελέτη 11.3 Ανάθεση Ρόλων 11.4 Διαχείριση Χρόνου και Διευκρινίσεις		ΜΣ-1 ΜΣ-2 ΚΣ-1 ΜΓΣ-1	→ → → →	hedra Google Docs Trello Padlet Google Docs	RQ1 RQ2 RQ3	40'
ΦΑΣΗ II P E R F O R M A N C E ↓	Dual Coding Retrieval Practice Reflective Learning Diaries	Jigsaw Expert teams Jigsaw Home teams	11.5 Προσομοίωση Οπτικής Επίθεσης Case Study III 11.6 Σχεδιασμός Διαγράμματος Ακολουθίας 11.7 Αξιολόγηση Διαγραμμάτων από Ομοτίμους 11.8 Κουίζ Κατανόησης Θεωρίας 11.9 Αυτοκαταγραφή	Ετεροαξιολόγηση Διαμορφωτική Αξιολόγηση	ΜΣ-1 ΜΣ-2 ΜΣ-6 ΚΣ-1 ΜΓΣ-1	→ ↔ ↔ ↔ →	Lucidchart Lumi Google Forms Lovable AI Evernote	RQ1 RQ2 RQ3	70'
	Concrete Examples Scaffolding Dual Coding Retrieval Practice Reflective Learning Diaries	Think Pair Share	12. Ενότητα A-Arts Η Αισθητική του Δωμάτιου 12. Θεωρητική Επίδειξη 12.1 Ατομική Μελέτη 12.2 Διαχείριση Χρόνου 12.3 Σενάριο Οπτικής Εξαστάσης Case Study IV 12.4 Ανάλυση Σχεδιασμού 12.5 Εργαστήριο Σχεδιασμού 12.6 Αξιολόγηση από Ομοτίμους 12.7 Κουίζ Κατανόησης Θεωρίας 12.8 Αυτοκαταγραφή	Ετεροαξιολόγηση Διαμορφωτική Αξιολόγηση	ΜΣ-1 ΜΣ-2 ΜΓΣ-1 ΜΣ-6 ΚΣ-1 ΜΓΣ-1	→ → ↔ ↔ ↔ →	Google Docs Trello Google Forms Padlet Canva Lumi Evernote	RQ1 RQ2 RQ3	120'
	Concrete Examples Scamper Retrieval Practice Reflective Learning Diaries		13. Ενότητα M-Mathematics Η Ψυχρή Λογική των Αριθμών 13. Θωρηκτική Παρουσίαση 13.1 Ατομική Μελέτη και Εξάσκηση 13.2 Διαχείριση Χρόνου 13.3 Νέοι Δείκτες Μέτρησης Phishing 13.4 Στατιστικά & Γραφήματα 13.5 Αξιολόγηση από Ομοτίμους 13.6 Κουίζ Κατανόησης Θεωρίας 13.7 Αυτοκαταγραφή	Ετεροαξιολόγηση Διαμορφωτική Αξιολόγηση	ΜΣ-1 ΜΣ-2 ΜΓΣ-1 ΜΣ-3 ΜΣ-4 ΜΣ-5 ΜΣ-6 ΚΣ-1 ΜΓΣ-1	→ → ↔ ↔ ↔ → → →	Google Docs Lumi Google Forms Trello Canva IBM SPSS Padlet Evernote	RQ1 RQ2 RQ3	120'
ΦΑΣΗ III S E L F - R E F L E C T I O N	Retrieval Practice Αυτοαξιολόγηση		14. The final phish: Intro video 15. Escape Room 16. Ανασταχασμός 17. Σχεδιασμός επόμενων βημάτων 18. Τελική Αυτοαξιολόγηση Δεξιοτήτων 19. Ερωτηματολόγιο Αξιολόγησης σχεδίου δράσης 20. Παραλαβή Πιστοποιητικού Παρακολούθησης	Τελική Αξιολόγηση Τελική Αυτοαξιολόγηση Post-test Ερωτηματολόγιο αποτελεσματικότητας (likert scale)	ΜΣ-1 ΜΓΣ-1 ΜΓΣ-1 ΜΓΣ-1	→ → → →	hedra genially Google Forms Padlet Canva	RQ1 RQ2 RQ3	120'

Σχήμα 4: Εκπαιδευτικός σχεδιασμός e-course



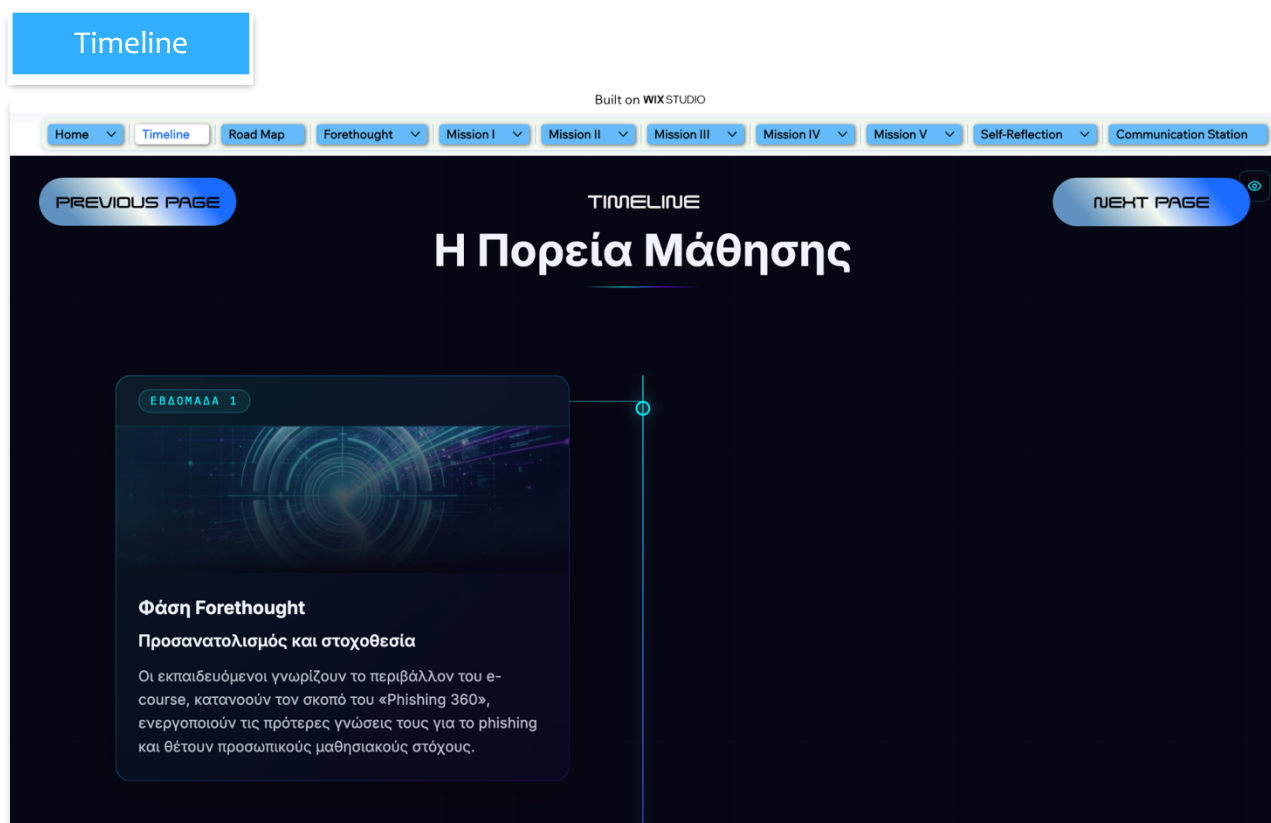
Εικόνα 1: Εισαγωγική Σελίδα (Home Page)

Περιγραφή: Η σελίδα¹ αυτή λειτουργεί ως πύλη εισόδου στο e-course και δεν αποτελεί τμήμα των τριών φάσεων της Αυτορρυθμιζόμενης Μάθησης. Η σελίδα ανοίγει με ένα εισαγωγικό βίντεο, στο οποίο ο ψηφιακός οδηγός «Σοφία» καλωσορίζει τους φοιτητές. Στην εισαγωγική σελίδα (Home Page), χρησιμοποιήθηκαν τα AI εργαλεία Lovable, Google AI Studio και Hedra (Google, 2026a; Hedra, 2026; Lovable, 2026).

Εκφώνηση σεναρίου: «Καλωσορίσατε στο e-course "Phishing 360°: Από το Συναισθημα στα Δεδομένα". Σε αυτό το ψηφιακό ταξίδι, θα γνωρίσετε τον κόσμο της κυβερνοασφάλειας και θα μάθετε πώς λειτουργούν οι επιθέσεις phishing και οι τεχνικές κοινωνικής μηχανικής. Μέσα από δραστηριότητες, σενάρια και προσομοιώσεις, θα αναλύσετε ύποπτα μηνύματα, θα εξετάσετε τεχνικά στοιχεία, θα σχεδιάσετε τη ροή μιας ψηφιακής παγίδας και θα επεξεργαστείτε δεδομένα από προσομοιωμένες εκστρατείες phishing.»

¹ Χρησιμοποιήθηκαν τα εργαλεία Hedra AI (Hedra, 2026) και Google AI Studio (Google, 2026a) στο εισαγωγικό βίντεο. Το Hedra AI αξιοποιήθηκε για τη δημιουργία του avatar της ψηφιακής βοηθού «Σοφία», ενώ το Google AI Studio χρησιμοποιήθηκε για τη μετατροπή κειμένου σε ομιλία (text-to-speech), αποδίδοντας φωνητικά το σενάριο που παρατίθεται ανωτέρω. Οι οδηγίες του e-course δημιουργήθηκαν με το Lovable AI (Lovable, 2026) και το αναλυτικό prompt παρατίθεται στο Κεφάλαιο 4, υποενότητα 4.5.1. Η μουσική υπόκρουση που χρησιμοποιήθηκε στο βίντεο προέρχεται από την πλατφόρμα Pixabay (Pixabay, 2026), υπό την άδεια Pixabay Content License, η οποία επιτρέπει τη δωρεάν χρήση του περιεχομένου χωρίς υποχρέωση αναφοράς του δημιουργού. Η χρήση των εργαλείων είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε από τον συγγραφέα πριν ενσωματωθεί στη σελίδα.

Ακριβώς κάτω από το βίντεο βρίσκεται το κουμπί «View Transcript», το οποίο παρέχει το πλήρες κείμενο του βίντεο, διασφαλίζοντας την προσβασιμότητα του περιεχομένου. Ακολουθούν οι Γενικές Οδηγίες του e-course, όπου παρουσιάζονται μέσα από έναν προκαθορισμένο (rule-based) εκπαιδευτικό chatbot, τη Σοφία, σχεδιασμένο με το εργαλείο Lovable AI. Η αλληλεπίδραση γίνεται αποκλειστικά μέσω κουμπιών προκαθορισμένων ερωτήσεων, καλύπτοντας 14 βασικά θέματα, από τη δομή και τη διάρκεια του μαθήματος μέχρι τα εργαλεία και την υποβολή εργασιών. Μετά από κάθε απάντηση, ο φοιτητής επιστρέφει αυτόματα στο βασικό μενού. Η σελίδα ολοκληρώνεται με το κουμπί εισόδου (Start the Adventure), μέσω του οποίου ο φοιτητής μεταβαίνει στο ίδιο το e-course.



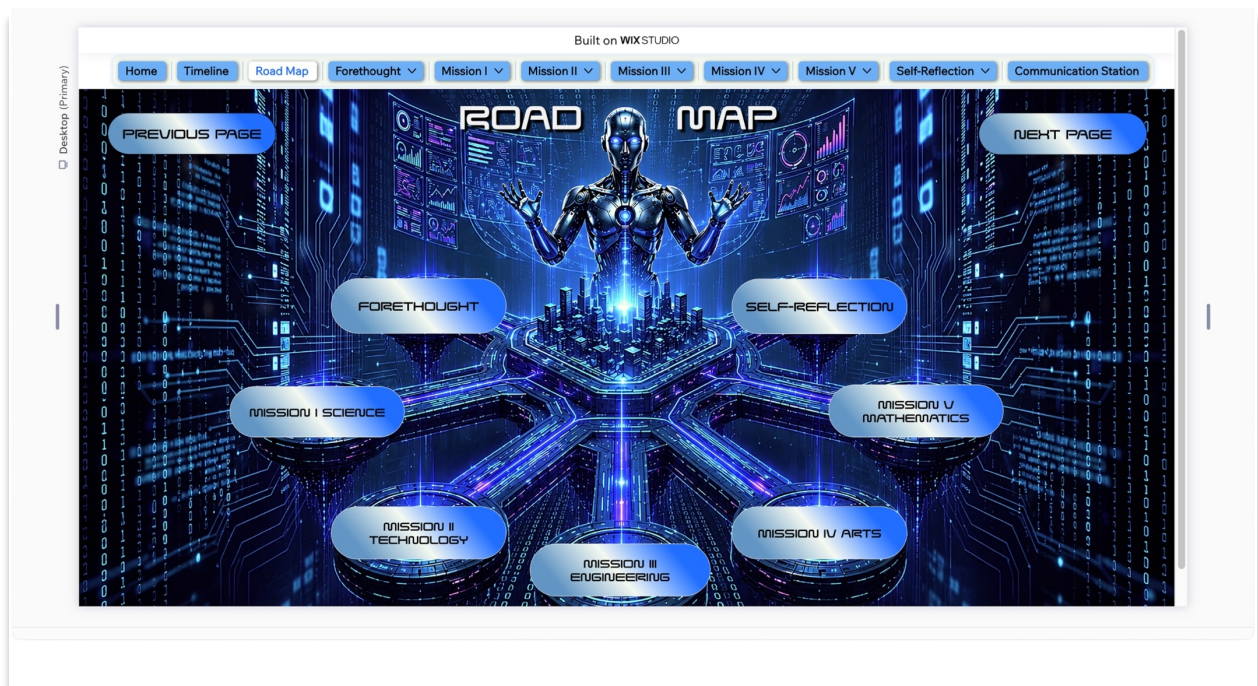
Εικόνα 2: Timeline

Περιγραφή: Η σελίδα αυτή δεν αποτελεί τμήμα των τριών φάσεων της Αυτορρυθμιζόμενης Μάθησης. Το διαδραστικό timeline, αναπτυγμένο στο εργαλείο Base44 AI ², παρουσιάζει τη συνολική πορεία του e-course «Phishing 360^ο: Από το Συναίσθημα στα Δεδομένα», το οποίο οργανώνεται σε επτά εβδομάδες. Στη σελίδα αυτή αξιοποιήθηκε το AI εργαλείο Base44 (Base44, 2026).

Η μαθησιακή διαδρομή ξεκινά με τη φάση Forethought, όπου οι εκπαιδευόμενοι προσανατολίζονται στο πρόγραμμα και θέτουν προσωπικούς στόχους, συνεχίζεται με τις επιμέρους STEAM ενότητες Science, Technology, Engineering, Arts και Mathematics, και ολοκληρώνεται με τη φάση Self-Reflection, όπου πραγματοποιείται αναστοχασμός και αποτίμηση της μαθησιακής πορείας. Μέσα από το timeline αποτυπώνεται συνοπτικά η μετάβαση από την αρχική κατανόηση του phishing και της κοινωνικής μηχανικής, στην τεχνική ανάλυση, τον σχεδιασμό ψηφιακής παγίδας, την οπτική αποδόμηση του δολώματος και την επεξεργασία μετρικών δεδομένων. Παράλληλα, το timeline εξηγεί τους μαθησιακούς στόχους ΜΣ1-ΜΣ6, τον μεταγνωστικό στόχο ΜΓΣ-1 και τον κοινωνικό-συναισθηματικό στόχο ΚΣ-1.

² Χρησιμοποιήθηκε το εργαλείο Base44 AI (Base44, 2026) για τη δημιουργία της διαδραστικής σελίδας Timeline. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε και τροποποιήθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix.

Road Map

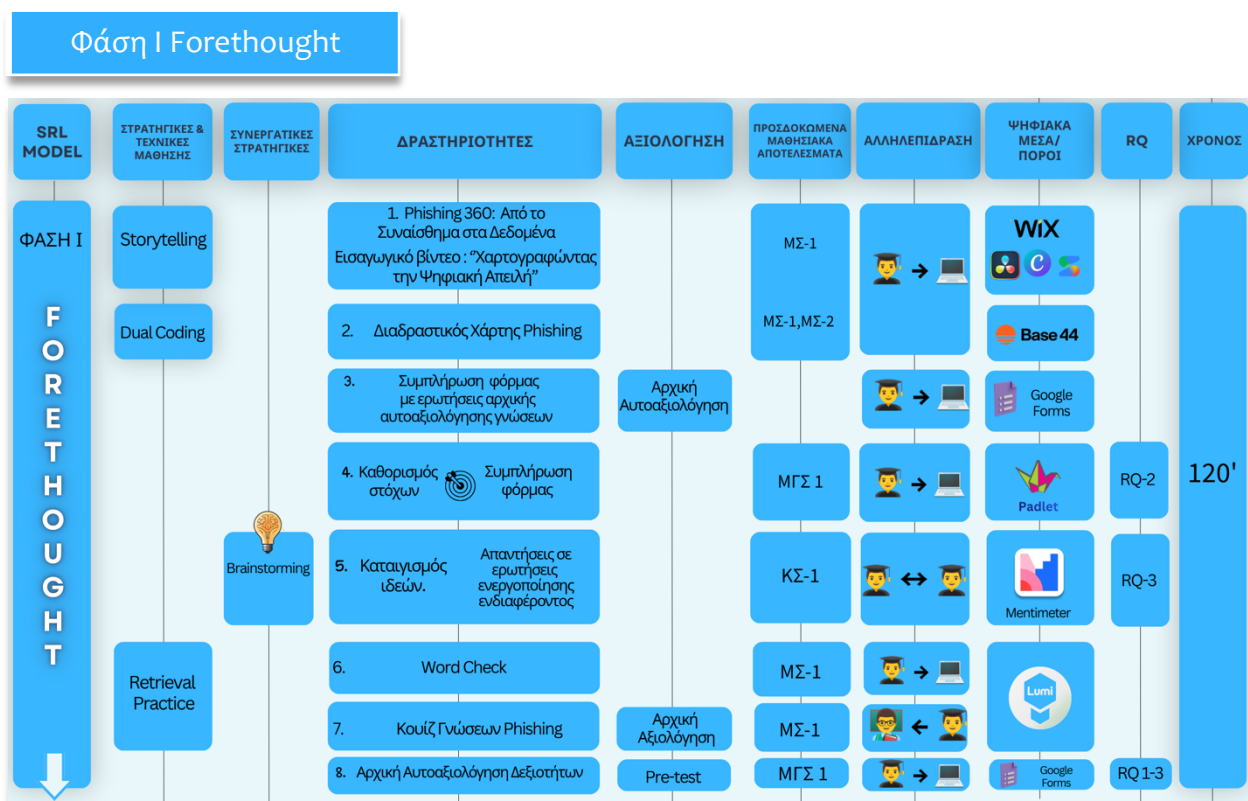


Εικόνα 3: Road Map

Η σελίδα αυτή³ λειτουργεί υποστηρικτικά ως σελίδα πλοήγησης.

Περιγραφή: Το Road Map αποτυπώνει οπτικά ολόκληρη τη διαδρομή του e-course, μέσα από τις τρεις φάσεις της αυτορρυθμιζόμενης μάθησης (Forethought, Performance, Self-Reflection), όπου η φάση Performance αναλύεται περαιτέρω σε πέντε αποστολές (Missions), σύμφωνα με την προσέγγιση STEAM: Science, Technology, Engineering, Arts και Mathematics. Μέσα από μία ενιαία, διαδραστική εικόνα, ο φοιτητής μπορεί να δει με μία ματιά ολόκληρη τη δομή του μαθήματος και να μεταβεί άμεσα σε οποιαδήποτε φάση ή αποστολή επιθυμεί, χωρίς να χρειάζεται να ακολουθήσει γραμμική πλοήγηση μέσω του μενού. Για τη δημιουργία της φωτογραφίας του Road Map αξιοποιήθηκε το AI εργαλείο ChatGPT (OpenAI, 2026).

³ Χρησιμοποιήθηκε το εργαλείο ChatGPT (OpenAI, 2026), για τη δημιουργία της εικόνας του Road Map. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε και τροποποιήθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix. Το αναλυτικό prompt παρατίθεται στο Κεφάλαιο 4, υποενότητα 4.5.4.

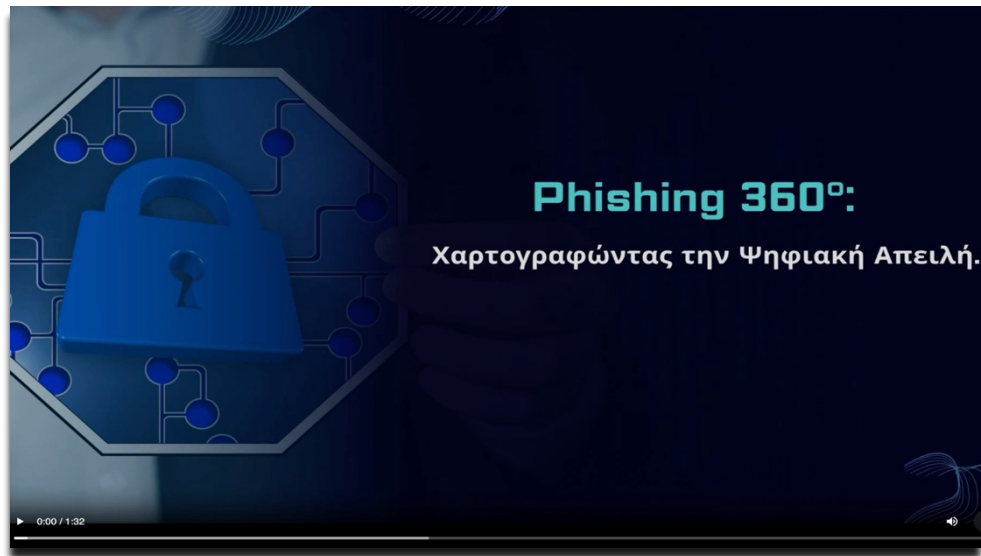


Σχήμα 5: Ροή δραστηριοτήτων Φάσης I (Forethought)

Πίνακας 10 Ανάλυση Φάσης I (Forethought)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Storytelling, Dual Coding, Retrieval Practice.
Συνεργατικές στρατηγικές	Brainstorming.
Στρατηγικές αυτορρύθμισης	Καθορισμός Στόχων, αυτοαξιολόγηση, επανάληψη και απομνημόνευση.
Θεωρητική Σύνδεση	<u>Ανάλυση Έργου (task analysis)</u>: στοχοθεσία, ενεργοποίηση προηγούμενης γνώσης. <u>Πεποιθήσεις αυτοπαρακίνησης</u>: ενεργοποίηση κινήτρων, ενδιαφέρον για το έργο.
Αξιολόγηση	Αρχική Αξιολόγηση (Κουίζ Γνώσεων Phishing), αρχική αυτοαξιολόγηση (Φόρμα Likert Γνώσεων), Pre-test (Skills Self-Check Δεξιότητων).
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα (χωρίς σύγχρονη παρουσία), καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	—

ο Δραστηριότητα 1: Εισαγωγικό βίντεο (Intro Video)



Εικόνα 4: Εισαγωγικό Βίντεο (Φάση Forethought)

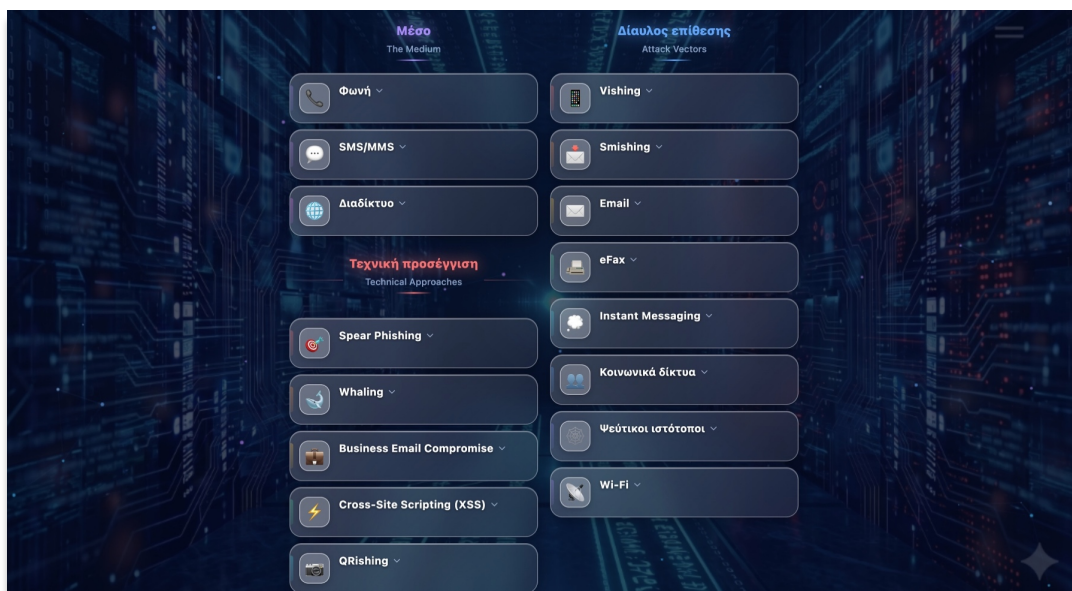
Περιγραφή: Οι φοιτητές παρακολουθούν ένα σύντομο βίντεο⁴, αξιοποιώντας την αφηγηματική στρατηγική Storytelling (Abrahamson, 1998; Smeda et al., 2014). Στο βίντεο παρουσιάζεται η έννοια του phishing ως μορφή επίθεσης κοινωνικής μηχανικής, καθώς και η λογική του «δολώματος» μέσα από το οποίο ο επιτιθέμενος κερδίζει την εμπιστοσύνη του θύματος. Στη συνέχεια, το phishing χαρτογραφείται σε τρεις βασικές διαστάσεις: το μέσο, τον δίαυλο επίθεσης και την τεχνική προσέγγιση, δίνοντας στους φοιτητές μια πρώτη, συνολική εικόνα της πολυπλοκότητας της απειλής, πριν αυτή αναλυθεί περαιτέρω στον διαδραστικό χάρτη phishing που ακολουθεί (Alabdian, 2020). Στο ανωτέρω βίντεο αξιοποιήθηκε το AI εργαλείο Google AI Studio (Google, 2026a).

⁴ Χρησιμοποιήθηκε το Google AI Studio (Google, 2026a) στο βίντεο αυτό για τη μετατροπή κειμένου σε ομιλία (text-to-speech). Συγκεκριμένα, το εργαλείο αξιοποιήθηκε για τη φωνητική απόδοση του σεναρίου που παρατίθεται ανωτέρω. Η μουσική υπόκρουση που χρησιμοποιήθηκε στο βίντεο προέρχεται από την πλατφόρμα Pixabay (Pixabay, 2026), υπό την άδεια Pixabay Content License, η οποία επιτρέπει τη δωρεάν χρήση του περιεχομένου χωρίς υποχρέωση αναφοράς του δημιουργού. Η χρήση των εργαλείων είχε υποστηρικτικό χαρακτήρα και το παραγόμενο ηχητικό υλικό ελέγχθηκε από τον συγγραφέα πριν ενσωματωθεί στην εργασία.

Εκφώνηση σεναρίου:

«Το phishing είναι μια μορφή επίθεσης κοινωνικής μηχανικής, στην οποία ο επιτιθέμενος προσπαθεί να επηρεάσει τον χρήστη, ώστε να αποκαλύψει προσωπικές ή ευαίσθητες πληροφορίες, όπως στοιχεία σύνδεσης, κωδικούς ή οικονομικά δεδομένα. Η λογική του βασίζεται στη δημιουργία ενός «δολώματος», το οποίο κάνει το θύμα να εμπιστευτεί ένα μήνυμα, έναν σύνδεσμο ή ένα ψηφιακό περιβάλλον. Για να κατανοηθεί καλύτερα η απειλή, το phishing μπορεί να χαρτογραφηθεί σε τρεις βασικές διαστάσεις: το μέσο, τον δίαυλο επίθεσης και την τεχνική προσέγγιση. Το μέσο αφορά τον τρόπο με τον οποίο ο επιτιθέμενος επικοινωνεί με το θύμα, όπως μέσω φωνής, SMS/MMS ή διαδικτύου. Ο δίαυλος επίθεσης περιλαμβάνει μορφές όπως το vishing, το smishing, το email, τα κοινωνικά δίκτυα, οι ψεύτικοι ιστότοποι και τα ασύρματα δίκτυα. Η τεχνική προσέγγιση περιλαμβάνει πιο εξειδικευμένες μεθόδους, όπως το spear phishing, το whaling, το business email compromise, το cross-site scripting, το QRishing, το social engineering και το drive-by download. Με αυτή τη χαρτογράφηση, το phishing δεν παρουσιάζεται ως ένα απλό ύποπτο μήνυμα, αλλά ως μια σύνθετη ψηφιακή απειλή που συνδυάζει μέσα επικοινωνίας, τεχνικές μεθόδους και ανθρώπινη συμπεριφορά.»

Δραστηριότητα 2: Διαδραστικός Χάρτης⁵ Phishing (Threat Map)



Εικόνα 5: Threat Map

⁵ Χρησιμοποιήθηκε το εργαλείο Base44 AI (Base44, 2026) στη δραστηριότητα αυτή για τη δημιουργία του διαδραστικού χάρτη. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε και τροποποιήθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix.

Περιγραφή: Στη δραστηριότητα «Threat Map» οι φοιτητές έρχονται σε επαφή με έναν διαδραστικό χάρτη της απειλής του phishing, δημιουργημένο με το εργαλείο Base44 AI (Base44, 2026), βασισμένο στην κατηγοριοποίηση του phishing σε τρεις διαστάσεις: μέσο, δίαυλο επίθεσης και τεχνική προσέγγιση. Ο χάρτης παρουσιάζει τα βασικά μέσα (φωνή, SMS/MMS, διαδίκτυο), τους διαύλους επίθεσης (vishing, smishing, email, eFax, άμεσα μηνύματα, κοινωνικά δίκτυα, ψεύτικοι ιστότοποι, Wi-Fi) και τις τεχνικές προσεγγίσεις (spear phishing, whaling, Business Email Compromise, Cross-Site Scripting, QRishing, social engineering, drive-by download), συνδυάζοντας εικονίδιο και λεζάντα για κάθε κατηγορία. Η ταυτόχρονη παρουσίαση εικόνας και λέξης ενεργοποιεί τη διαδικασία της αναφορικής επεξεργασίας (referential processing) της θεωρίας Dual Coding, κατά την οποία το λεκτικό και το μη λεκτικό σύστημα συνδέονται μεταξύ τους, ενισχύοντας την κωδικοποίηση και την ανάκληση της πληροφορίας (Clark & Paivio, 1987). Η αλληλεπίδραση με τον χάρτη βοηθά τους συμμετέχοντες να αντιληφθούν ότι το phishing δεν περιορίζεται σε ένα απλό ύποπτο email, αλλά αποτελεί σύνθετη ψηφιακή απειλή με πολλαπλές μορφές, οργανώνοντας τις αρχικές τους γνώσεις πριν προχωρήσουν στην υπόλοιπη ύλη του e-course (Alabdan, 2020).

Δραστηριότητα 3: Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων

Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων για το Phishing

Παρακαλώ συμπληρώστε την παρακάτω φόρμα για να αξιολογήσετε τις τρέχουσες γνώσεις σας σχετικά με τις επιθέσεις phishing.

Γνωρίζω τι σημαίνει ο όρος «phishing».

1 2 3 4 5

1 - Διαφωνώ απόλυτα 5 - Συμφωνώ απόλυτα

Μπορώ να αναγνωρίσω ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου.

1 2 3 4 5

1 - Διαφωνώ απόλυτα 5 - Συμφωνώ απόλυτα

Μπορώ να εντοπίσω ύποπτους συνδέσμους σε ένα ψηφιακό μήνυμα.

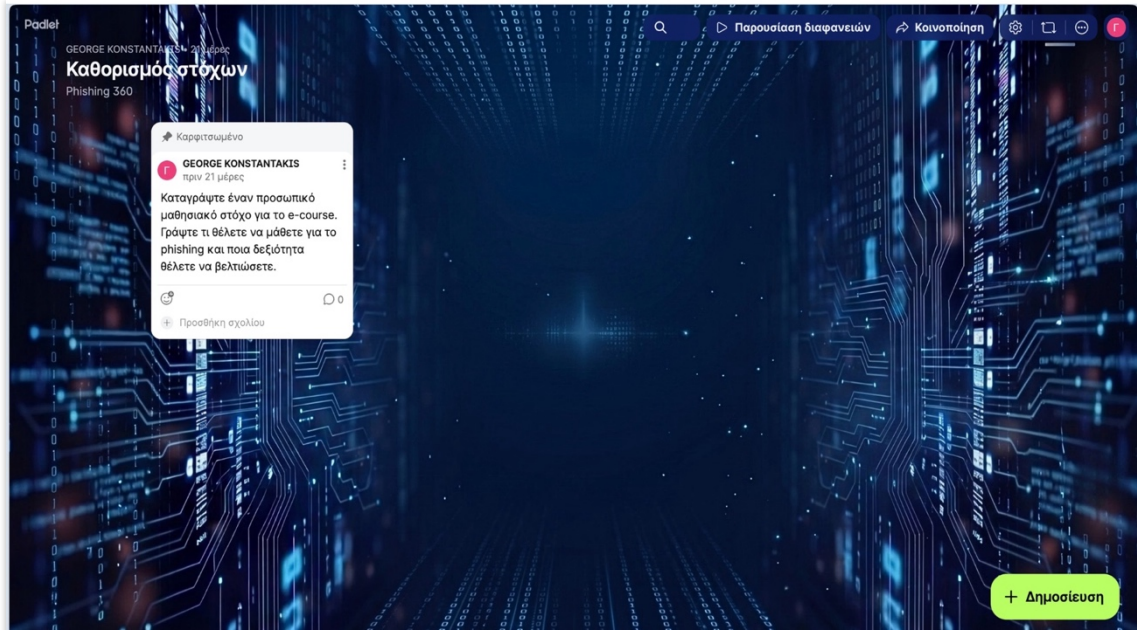
Εικόνα 6: Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων

Περιγραφή: Στη δραστηριότητα «Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων για το Phishing» οι συμμετέχοντες κλήθηκαν να αποτυπώσουν το αρχικό επίπεδο εξοικείωσής τους με βασικές έννοιες του phishing πριν από την έναρξη του e-course. Η φόρμα⁶ δημιουργήθηκε στο Google Forms και οργανώθηκε με δηλώσεις τύπου Likert, ώστε οι εκπαιδευόμενοι να δηλώσουν τον βαθμό συμφωνίας τους με προτάσεις που αφορούσαν την αναγνώριση ύποπτων μηνυμάτων, τον εντοπισμό ύποπτων συνδέσμων, την κατανόηση των προσωπικών πληροφοριών που μπορεί να στοχεύει μια επίθεση phishing, καθώς και τη γνώση βασικών μορφών επίθεσης, όπως το smishing, το vishing και το spear phishing.

Το περιεχόμενο της φόρμας εντάσσει το phishing στις τεχνικές κοινωνικής μηχανικής, εξηγώντας πώς οι επιτιθέμενοι στοχεύουν να αποσπάσουν ευαίσθητα προσωπικά δεδομένα του χρήστη, όπως κωδικούς, στοιχεία σύνδεσης ή οικονομικά δεδομένα. Παράλληλα, η πηγή αναφέρεται σε διαφορετικά μέσα και μορφές phishing, όπως η φωνητική επικοινωνία, τα SMS/MMS, το διαδίκτυο, το vishing, το smishing και το spear phishing. Με αυτόν τον τρόπο, η φόρμα δεν λειτούργησε ως τεστ σωστών και λανθασμένων απαντήσεων, αλλά ως εργαλείο αρχικής αυτοαξιολόγησης, βοηθώντας τους συμμετέχοντες να ενεργοποιήσουν τις πρότερες γνώσεις τους και να αναγνωρίσουν τα σημεία στα οποία χρειάζονται περαιτέρω εξοικείωση (Zimmerman, 2002).

⁶ Η αναλυτική φόρμα αυτοαξιολόγησης γνώσεων διατίθεται στο Παράρτημα.

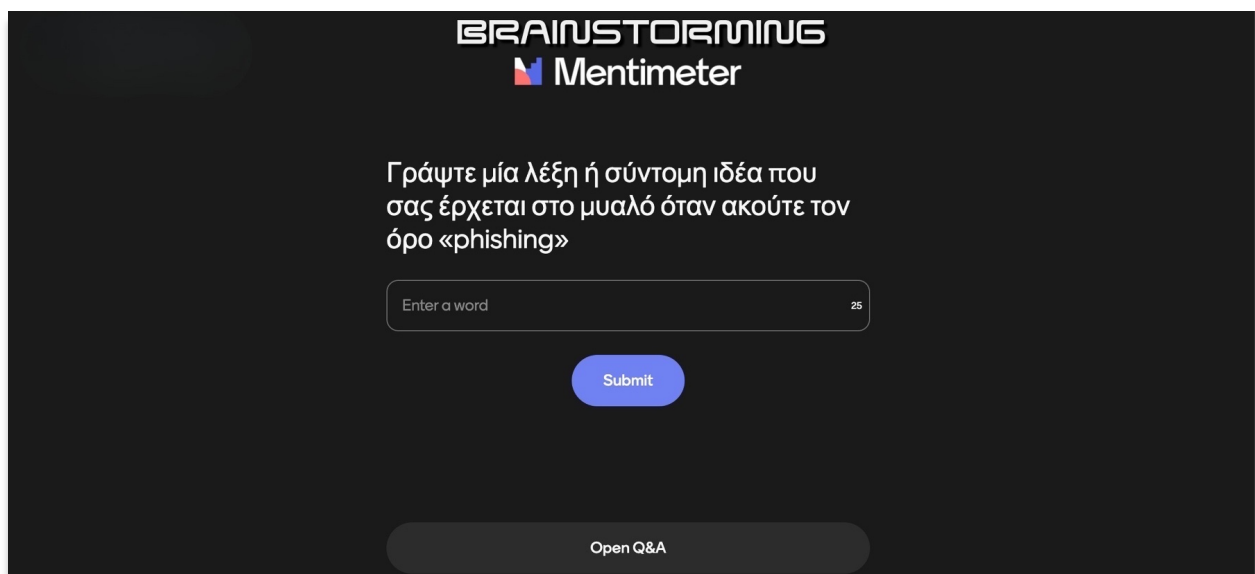
○ Δραστηριότητα 4: Καθορισμός Στόχων



Εικόνα 7: Καθορισμός Στόχων (Φάση Forethought)

Περιγραφή: Οι φοιτητές καταγράφουν στο Padlet έναν προσωπικό μαθησιακό στόχο για το e-course, προσδιορίζοντας τι επιθυμούν να μάθουν για το phishing και ποια δεξιότητα θέλουν να βελτιώσουν. Η δραστηριότητα εντάσσεται στη διαδικασία της ανάλυσης έργου (task analysis), κατά την οποία ο φοιτητής θέτει δικό του στόχο πριν από την έναρξη της μαθησιακής διαδικασίας (Zimmerman, 2002).

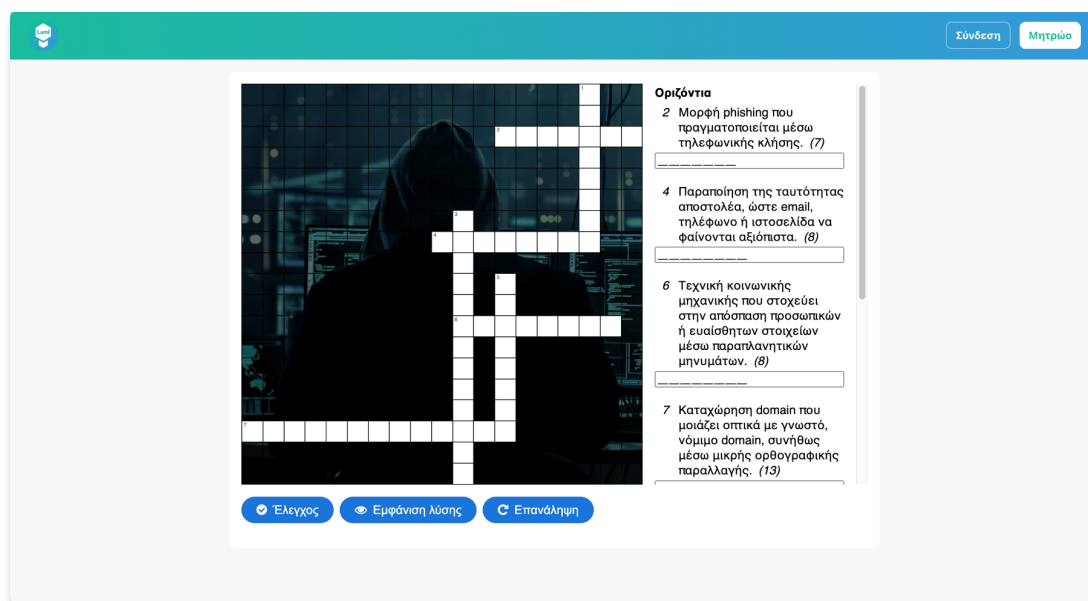
○ Δραστηριότητα 5: Καταιγισμός Ιδεών (Brainstorming)



Εικόνα 8: Καταιγισμός Ιδεών

Περιγραφή: Στη δραστηριότητα «Brainstorming» οι φοιτητές γράφουν στο Mentimeter μία λέξη ή ιδέα που τους έρχεται στο μυαλό όταν ακούν τον όρο «phishing», αξιοποιώντας τη συνεργατική στρατηγική Brainstorming (Çelik & Akay, 2025). Οι απαντήσεις εμφανίζονται όλες μαζί σε νέφος λέξεων, ώστε να βλέπουν τι σκέφτονται και οι συμφοιτητές τους.

ο Δραστηριότητα 6: Word Check (Σταυρόλεξο)



Εικόνα 9: Word Check (Σταυρόλεξο)

Περιγραφή: Οι φοιτητές συμπληρώνουν ένα σταυρόλεξο στο εργαλείο Lumi (Lumi, 2026), βασισμένο σε βασική ορολογία όπως phishing, spear phishing, vishing, smishing, QRishing και spoofing (Alabdan, 2020). Κάθε ένδειξη περιγράφει τον ορισμό του αντίστοιχου όρου, χωρίς να τον κατονομάζει, και ο φοιτητής καλείται να συμπληρώσει τη σωστή λέξη στο αντίστοιχο πλέγμα. Η δραστηριότητα λειτουργεί ως ανασκόπηση της ορολογίας που έχει ήδη συναντήσει σε προηγούμενες ενότητες, αξιοποιώντας την τεχνική Retrieval Practice (Roediger & Karpicke, 2006).

○ Δραστηριότητα 7: Κουίζ Γνώσεων Phishing

Ερώτηση 1: Τι είναι το phishing;

☐ Α) Τεχνική κοινωνικής μηχανικής που προσπαθεί να επηρεάσει τον στόχο ώστε να αποκαλύψει προσωπικές πληροφορίες.

☐ Β) Μέθοδος νόμιμης αποθήκευσης δεδομένων.

☐ Γ) Πρόγραμμα προστασίας υπολογιστή.

☐ Δ) Τεχνική δημιουργίας ασφαλών κωδικών.

✓ Έλεγχος

>

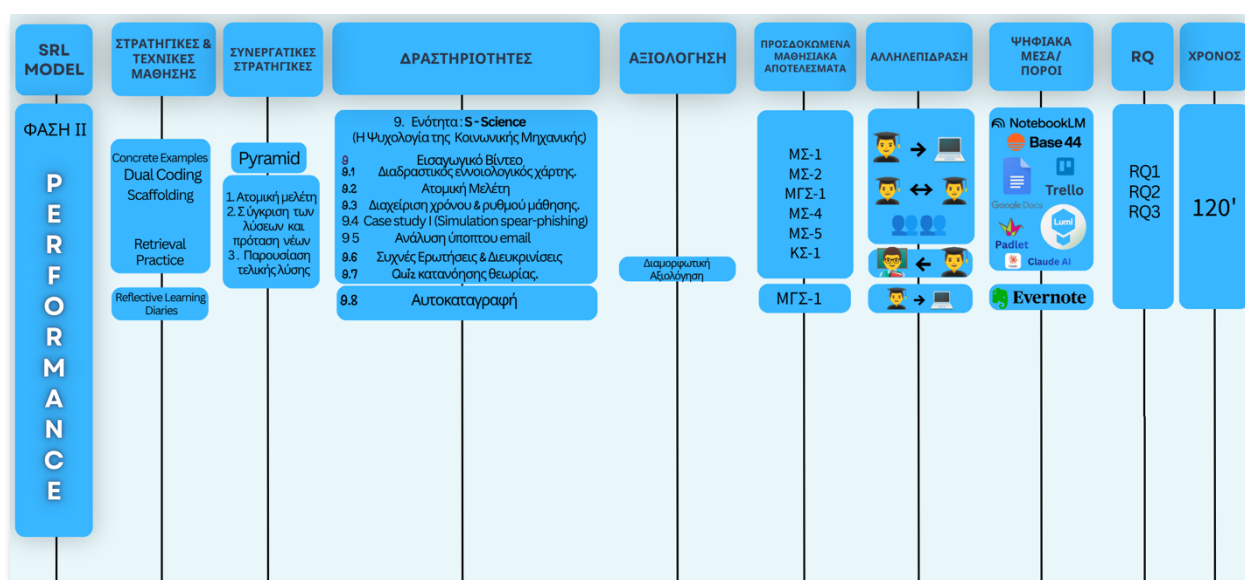
Εικόνα 10: Κουίζ Γνώσεων (Forethought)

Περιγραφή: Οι συμμετέχοντες συμπληρώνουν, στο εργαλείο Lumi (Lumi, 2026), ένα κουίζ οκτώ ερωτήσεων πολλαπλής επιλογής, εστιασμένων σε βασικές έννοιες του phishing, όπως ο ορισμός του, τα προσωπικά δεδομένα που στοχεύει, τα μέσα επικοινωνίας που αξιοποιούνται και επιμέρους μορφές επιθέσεων (vishing, smishing, spear phishing, QRishing). Για κάθε ερώτηση ορίζεται μόνο μία σωστή απάντηση, και παρέχεται άμεση ανατροφοδότηση στις σωστές και λανθασμένες απαντήσεις. Η δραστηριότητα βοηθάει τους συμμετέχοντες να αποτυπώσουν τις πρότερες γνώσεις τους και να έρθουν σε πρώτη επαφή με κατηγορίες που θα αναλυθούν στη συνέχεια του μαθήματος (Alabdan, 2020). Η δραστηριότητα εντάσσεται στην αρχική αξιολόγηση του e-course και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

○ Δραστηριότητα 8: Skills Self-Check (Pre)

Περιγραφή: Οι φοιτητές συμπληρώνουν ένα σύντομο ερωτηματολόγιο στο Google Forms, πριν από την έναρξη του e-course, με 12 δηλώσεις τύπου Likert (κλίμακα 1-5). Το ερωτηματολόγιο οργανώνεται σε τρεις ενότητες, οι οποίες αντιστοιχούν στους τρεις βασικούς δείκτες της παρούσας εργασίας: τη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση και την κατανόηση της οπτικής των άλλων. Μέσα από τις δηλώσεις αυτές, οι φοιτητές αποτυπώνουν το αρχικό τους επίπεδο στην ανάλυση και αξιολόγηση καταστάσεων, στην παρακολούθηση της μαθησιακής τους πορείας και στη συνεργασία με άλλους, πριν αρχίσουν τις δραστηριότητες του e-course. Το ερωτηματολόγιο Skills Self-Check (Pre) διατίθεται στο Παράρτημα.

Φάση II Performance (Ενότητα Science)

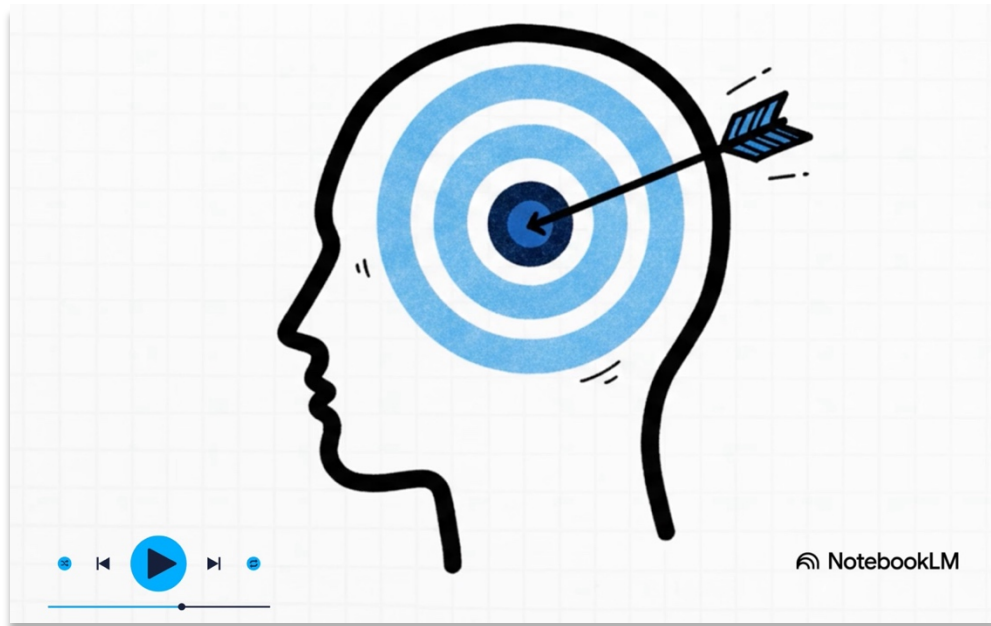


Σχήμα 6: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Science

Πίνακας 11: Ανάλυση Ενότητας Science (Φάση II Performance)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΣ-4, ΜΣ-5, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Dual Coding, Scaffolding, Concrete Examples, Retrieval Practice, Reflective Learning Diaries.
Συνεργατικές στρατηγικές	Πυραμίδα.
Στρατηγικές αυτορρύθμισης	Οργάνωση και μετατροπή πληροφορίας, αναζήτηση πληροφοριών, διαχείριση χρόνου, επανάληψη και απομνημόνευση, αυτοκαταγραφή.
Θεωρητική σύνδεση	Οι δύο κεντρικές διαδικασίες της φάσης Performance: ο αυτοέλεγχος (self-control), που περιλαμβάνει τη διαχείριση χρόνου και την αναζήτηση πληροφοριών και η αυτοπαρατήρηση (self-observation), μέσω αυτοκαταγραφής.
Αξιολόγηση	Διαμορφωτική Αξιολόγηση (Κουίζ Κατανόησης Θεωρίας, βαθμολογούμενο).
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα (χωρίς σύγχρονη παρουσία), καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Science (Επιστήμη): οι φοιτητές μελετούν την ψυχολογία της κοινωνικής μηχανικής, κατανοώντας πώς οι επιθέσεις phishing εκμεταλλεύονται ανθρώπινες γνωστικές λειτουργίες, παράγοντες ευαλωτότητας και αρχές πειθούς.

ο Δραστηριότητα 9: Εισαγωγικό Βίντεο

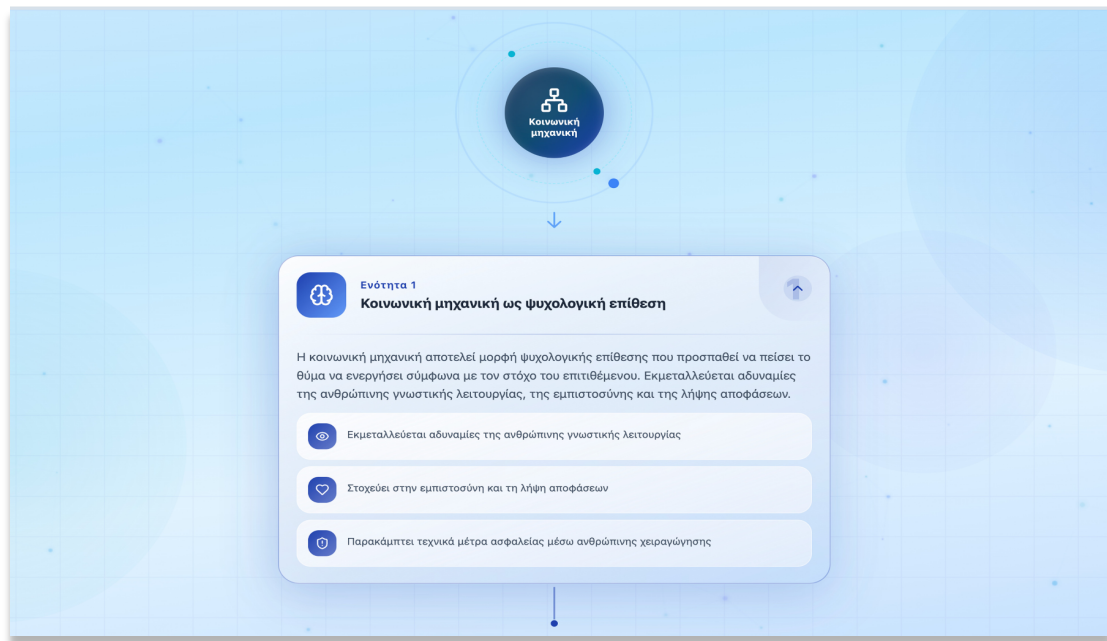


Εικόνα 11: Εισαγωγικό βίντεο: «Η ψυχολογία της Κοινωνικής Μηχανικής»

Περιγραφή: Αξιοποιήθηκε το εργαλείο NotebookLM⁷ (Google, 2026e) για τη δημιουργία εκπαιδευτικού βίντεο με θέμα «Η Ψυχολογία της Κοινωνικής Μηχανικής». Το βίντεο παρουσιάζει την κοινωνική μηχανική ως μορφή ψυχολογικής επίθεσης που εκμεταλλεύεται την ανθρώπινη σκέψη, την εμπιστοσύνη και τη λήψη αποφάσεων, αναλύει βασικές γνωστικές λειτουργίες που επηρεάζονται (αντίληψη, μνήμη, λήψη αποφάσεων, δράση) και παράγοντες ευαλωτότητας (γνωστικός φόρτος, στρες, μειωμένη προσοχή, εμπειρία, κουλτούρα). Παρουσιάζει επίσης τον ρόλο της πειθούς στα phishing emails με έμφαση σε βασικές αρχές πειθούς όπως η αυθεντία, το έντονο συναίσθημα, η ακεραιότητα και η ανταπόδοση. Μέσα από αυτή τη θεωρητική επίδειξη, οι εκπαιδευόμενοι κατανοούν ότι η αναγνώριση phishing απαιτεί όχι μόνο τεχνικές γνώσεις, αλλά και ικανότητα εντοπισμού ψυχολογικών τεχνικών χειραγώγησης (Ferreira & Teles, 2019; Montañez et al., 2020), αξιοποιώντας τη στρατηγική Concrete Examples (Rawson et al., 2015).

⁷ Χρησιμοποιήθηκε το εργαλείο NotebookLM (Google, 2026e) για τη δημιουργία του ανωτέρω βίντεο. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix. Το αναλυτικό prompt παρατίθεται στο Κεφάλαιο 4, υποενότητα 4.5.2.

ο Δραστηριότητα 9.1: Διαδραστικός Εννοιολογικός Χάρτης⁸



Εικόνα 12: Διαδραστικός εννοιολογικός χάρτης

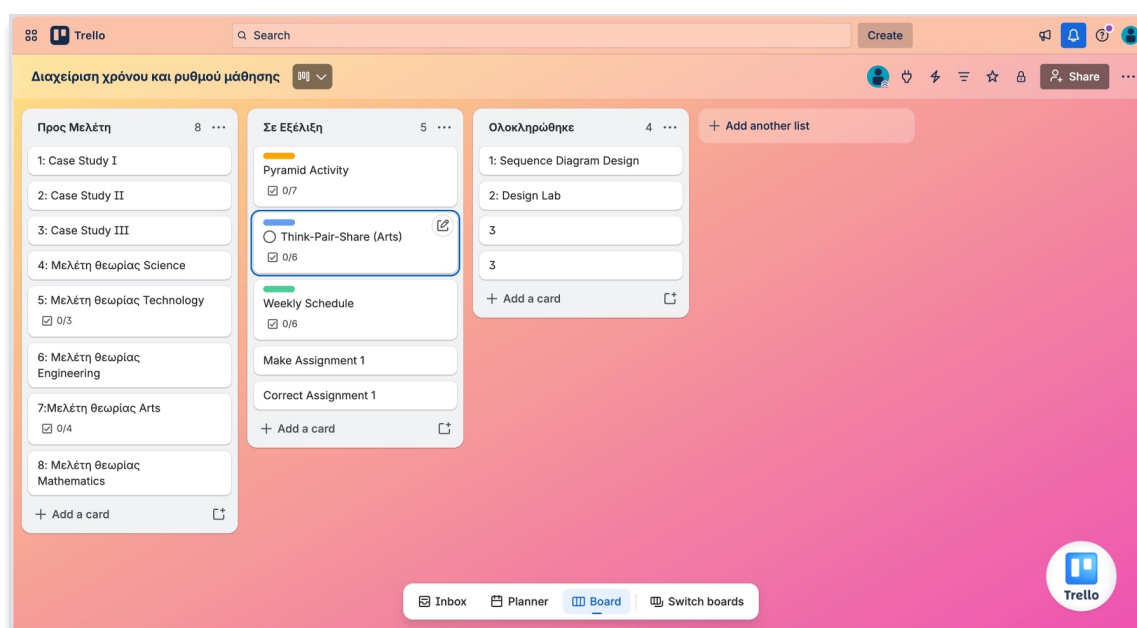
Περιγραφή: Οι συμμετέχοντες αλληλεπιδρούν με έναν διαδραστικό εννοιολογικό χάρτη, δημιουργημένο με το εργαλείο Base44 AI (Base44, 2026), ο οποίος οργανώνει τις βασικές έννοιες γύρω από τον κεντρικό άξονα της κοινωνικής μηχανικής και δείχνει πώς ο επιτιθέμενος μπορεί να επηρεάσει την ανθρώπινη κρίση. Συγκεκριμένα, παρουσιάζει την κοινωνική μηχανική ως ψυχολογική επίθεση και αναδεικνύει τις γνωστικές διεργασίες που εμπλέκονται στη λήψη αποφάσεων. Στη συνέχεια, καταγράφει τους βραχυπρόθεσμους και μακροπρόθεσμους παράγοντες ευαλωτότητας και συνδέει τα παραπλανητικά μηνύματα phishing με τεχνικές πειθούς που μπορούν να κάνουν ένα αίτημα να φαίνεται αξιόπιστο. Με τη βοήθεια του χάρτη, οι εκπαιδευόμενοι κατανοούν πως η κοινωνική μηχανική εκμεταλλεύεται την ανθρώπινη συμπεριφορά και την εμπιστοσύνη (Ferreira & Teles, 2019; Montañez et al., 2020), μέσω του συνδυασμού εικόνας και κειμένου, σύμφωνα με την αρχή του Dual Coding (Clark & Paivio, 1987).

⁸ Χρησιμοποιήθηκε το εργαλείο Base44 AI (Base44, 2026) για τη δημιουργία του ανωτέρω διαδραστικού εννοιολογικού χάρτη. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε και τροποποιήθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix. Το αναλυτικό prompt παρατίθεται στο Κεφάλαιο 4, υποενότητα 4.5.3.

ο Δραστηριότητα 9.2: Ατομική Μελέτη

Περιγραφή: Οι φοιτητές καλούνται να μελετήσουν ένα σύντομο ψηφιακό έγγραφο σε Google Docs (Google, 2026c) για την ψυχολογία της κοινωνικής μηχανικής. Το υλικό παρουσιάζει την κοινωνική μηχανική ως ψυχολογική επίθεση που αξιοποιεί ανθρώπινες γνωστικές λειτουργίες όπως (αντίληψη, εργαζόμενη μνήμη, λήψη αποφάσεων, δράση) και παράγοντες ευαλωτότητας (γνωστικός φόρτος, στρες, μειωμένη επαγρύπνηση, γνώση, εμπειρία, κουλτούρα), καθώς και τον ρόλο της πειθούς στα phishing emails, αξιοποιώντας τη στρατηγική Concrete Examples (Rawson et al., 2015) με έμφαση σε αρχές όπως η αυθεντία, το έντονο συναίσθημα, η ακεραιότητα και η ανταπόδοση. Ακολουθούν τρεις ερωτήσεις αξιολόγησης επικινδυνότητας τις οποίες ο φοιτητής απαντά σε σύντομο κείμενο και αναρτά στο Google Classroom μέσω του υπερσυνδέσμου που παρέχεται. Η δραστηριότητα προετοιμάζει τους εκπαιδευόμενους με οργανωμένο θεωρητικό υπόβαθρο πριν την πρακτική ανάλυση phishing μηνυμάτων (Ferreira & Teles, 2019; Montañez et al., 2020), αξιοποιώντας τη στρατηγική Scaffolding (Wood et al., 1976) μέσω δομημένου χάρτη μελέτης, επισήμανσης κρίσιμων σημείων και ερωτήσεων αξιολόγησης και αυτοελέγχου.

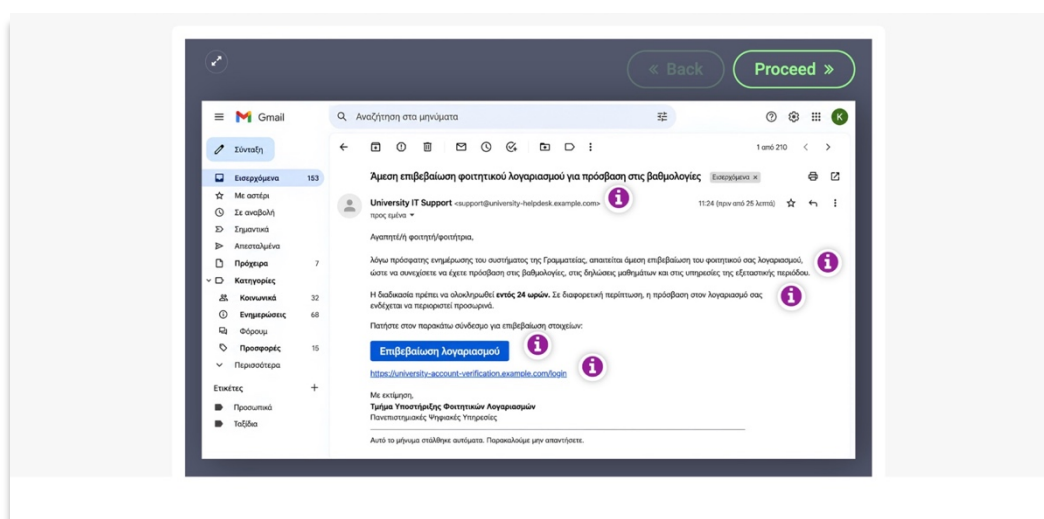
ο Δραστηριότητα 9.3: Διαχείριση χρόνου και ρυθμού μάθησης



Εικόνα 13: Διαχείριση Χρόνου & Ρυθμού Μάθησης

Περιγραφή: Αρχικά οι φοιτητές κατεβάζουν σε pdf ένα ενδεικτικό παράδειγμα οργάνωσης χρόνου που δίδεται από τον ΑΙ οδηγό Σοφία, το οποίο λειτουργεί ως πρότυπο τόσο για την τρέχουσα όσο και για κάθε επόμενη ενότητα του μαθήματος, ώστε να έχουν ένα σημείο αναφοράς πριν φτιάξουν τον δικό τους πίνακα κάθε φορά. Έπειτα μεταβαίνουν στο εργαλείο Trello για να οργανώσουν τον χρόνο και τον ρυθμό μελέτης τους στην ενότητα της κοινωνικής μηχανικής. Δημιουργούν έναν προσωπικό πίνακα με στήλες όπως «Προς Μελέτη», «Σε Εξέλιξη» και «Ολοκληρώθηκε», και κατανέμουν τις επιμέρους εργασίες της ενότητας σε καρτέλες με συγκεκριμένες προθεσμίες. Η δραστηριότητα εξασκεί στην πράξη τη διαχείριση χρόνου ως στρατηγική της SRL και οι εκπαιδευόμενοι μαθαίνουν να θέτουν ρεαλιστικά χρονικά όρια για κάθε βήμα της μάθησής τους (Zimmerman, 2002).

○ Δραστηριότητα 9.4: Case Study I (Simulation Spear-phishing)

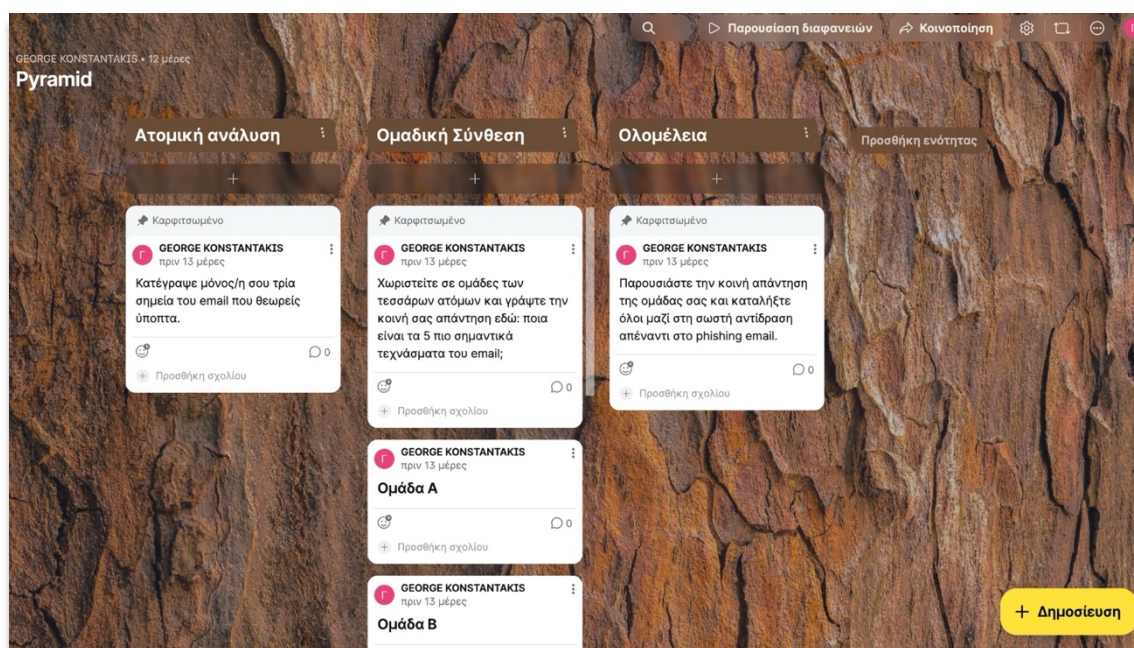


Εικόνα 14: Simulation Spear-phishing Case Study I

Περιγραφή: Η προσομοίωση υλοποιείται στο περιβάλλον Lumi, με τη χρήση διαδραστικού σεναρίου H5P (branching scenario), τεχνική μάθησης που ενισχύει την εμπλοκή και τη θετική εμπειρία των φοιτητών σε ψηφιακά περιβάλλοντα μάθησης (Jacob & Centofanti, 2024). Οι φοιτητές εισέρχονται σε μια προσομοίωση ύποπτου email, το οποίο εμφανίζεται ως μήνυμα που αφορά την περίοδο της εξεταστικής και ζητά άμεση επιβεβαίωση λογαριασμού. Στόχος είναι οι εκπαιδευόμενοι να αναγνωρίσουν βασικά χαρακτηριστικά spear-phishing και να αξιολογήσουν την ορθότερη αντίδραση.

Στο πρώτο μέρος της δραστηριότητας αξιοποιούνται hotspots πάνω στο προσομοιωμένο email. Τα hotspots καθοδηγούν τους φοιτητές να παρατηρήσουν κρίσιμα σημεία, όπως ο αποστολέας, ο ύποπτος σύνδεσμος, η πίεση χρόνου, το αίτημα για προσωπικά στοιχεία και η χρήση ψυχολογικών τεχνασμάτων, όπως ο φόβος απώλειας πρόσβασης και η επίκληση αυθεντίας. Στη συνέχεια, οι φοιτητές καλούνται να απαντήσουν σε μία αναστοχαστική ερώτηση μέσα στο Lumi. Η ερώτηση περιλαμβάνει τρεις πιθανές επιλογές, από τις οποίες μόνο μία αντιστοιχεί στην ασφαλέστερη αντίδραση. Για κάθε επιλογή παρέχεται άμεση ανατροφοδότηση, ώστε οι φοιτητές να κατανοήσουν γιατί μια ενέργεια είναι επικίνδυνη, μερικώς σωστή ή ασφαλής. Ο συνδυασμός εικόνας και επεξηγηματικού κειμένου σε κάθε hotspot αξιοποιεί την αρχή του Dual Coding (Clark & Paivio, 1987).

ο Δραστηριότητα 9.5: Ανάλυση ύποπτου email



Εικόνα 15: Δραστηριότητα Ανάλυσης ύποπτου email (Πυραμίδα)

Περιγραφή: Μετά την ολοκλήρωση του διακλαδωτού σεναρίου spear-phishing, οι φοιτητές λαμβάνουν πρόσβαση σε ένα ψηφιακό έγγραφο οδηγιών (Google Docs) για τη δραστηριότητα της ανάλυσης ύποπτου email μέσω της στρατηγικής της Πυραμίδας (Manathunga & Hernández-Leo, 2018), στο οποίο ο AI βοηθός Sofia παρουσιάζει και εξηγεί τα τρία διαδοχικά βήματα της στρατηγικής:

1. Ατομική ανάλυση: Ο φοιτητής καταγράφει μόνος του τρία σημεία του email που θεωρεί ύποπτα.
2. Ανάλυση σε τετράδες: Οι φοιτητές χωρίζονται σε ομάδες των τεσσάρων, συγκρίνουν τις ατομικές τους απαντήσεις και επιλέγουν από κοινού τα πέντε πιο σημαντικά τεχνάσματα κοινωνικής μηχανικής που εντοπίζουν στο μήνυμα.
3. Ολομέλεια: Κάθε ομάδα παρουσιάζει την κοινή της απάντηση, και η τάξη καταλήγει συλλογικά στη σωστή αντίδραση απέναντι στο phishing email.

Αφού διαβάσουν τις οδηγίες, οι φοιτητές πατούν το επόμενο κουμπί στην πλατφόρμα Wix «Open Padlet Board», και μεταφέρονται στην πλατφόρμα Padlet, όπου καταγράφουν τις απαντήσεις τους στις αντίστοιχες στήλες (Ατομική Ανάλυση, Ομαδική Σύνθεση, Ολομέλεια), αξιοποιώντας τις συνεργατικές δεξιότητες επίλυσης προβλήματος που περιγράφονται στο πλαίσιο των (Hesse et al., 2015).

ο Δραστηριότητα 9.6: Συχνές Ερωτήσεις & Διευκρινίσεις

Περιγραφή: Οι φοιτητές χρησιμοποιούν το εργαλείο τεχνητής νοημοσύνης Claude AI για να διατυπώσουν και να επιλύσουν τυχόν απορίες που προέκυψαν κατά τη μελέτη της ενότητας της κοινωνικής μηχανικής. Αφού έχουν ήδη εντοπίσει τα σημεία που τους δυσκόλεψαν, απευθύνονται στο εργαλείο διατυπώνοντας την ερώτησή τους με δικά τους λόγια και λαμβάνουν άμεση ανατροφοδότηση, προσαρμοσμένη στο δικό τους επίπεδο κατανόησης. Με τον τρόπο αυτό, το γνωστικό κενό καλύπτεται τη στιγμή που εντοπίζεται, αξιοποιώντας τη στρατηγική αυτορρύθμισης της Αναζήτησης Πληροφοριών (Zimmerman, 2002). Παράλληλα, η δραστηριότητα βοηθάει σημαντικά στην ενίσχυση του ψηφιακού γραμματισμού των φοιτητών, καθώς εξοικειώνονται με τη χρήση εργαλείων τεχνητής νοημοσύνης ως υποστηρικτικό μέσο στη μαθησιακή διαδικασία.

ο Δραστηριότητα 9.7: Κουίζ κατανόησης θεωρίας.

Τι είναι η κοινωνική μηχανική στον χώρο της κυβερνοασφάλειας;

- ☐ Α. Μια καθαρά τεχνική επίθεση που βασίζεται μόνο σε κακόβουλο λογισμικό.
- ☐ Β. Μια ψυχολογική επίθεση που προσπαθεί να πείσει το άτομο να ενεργήσει όπως θέλει ο επιτιθέμενος.
- ☐ Γ. Ένα εργαλείο ασφαλείας που μπλοκάρει αυτόματα τα phishing emails.

Ελεγχος >

© ○ ○ ○ ○

lymi

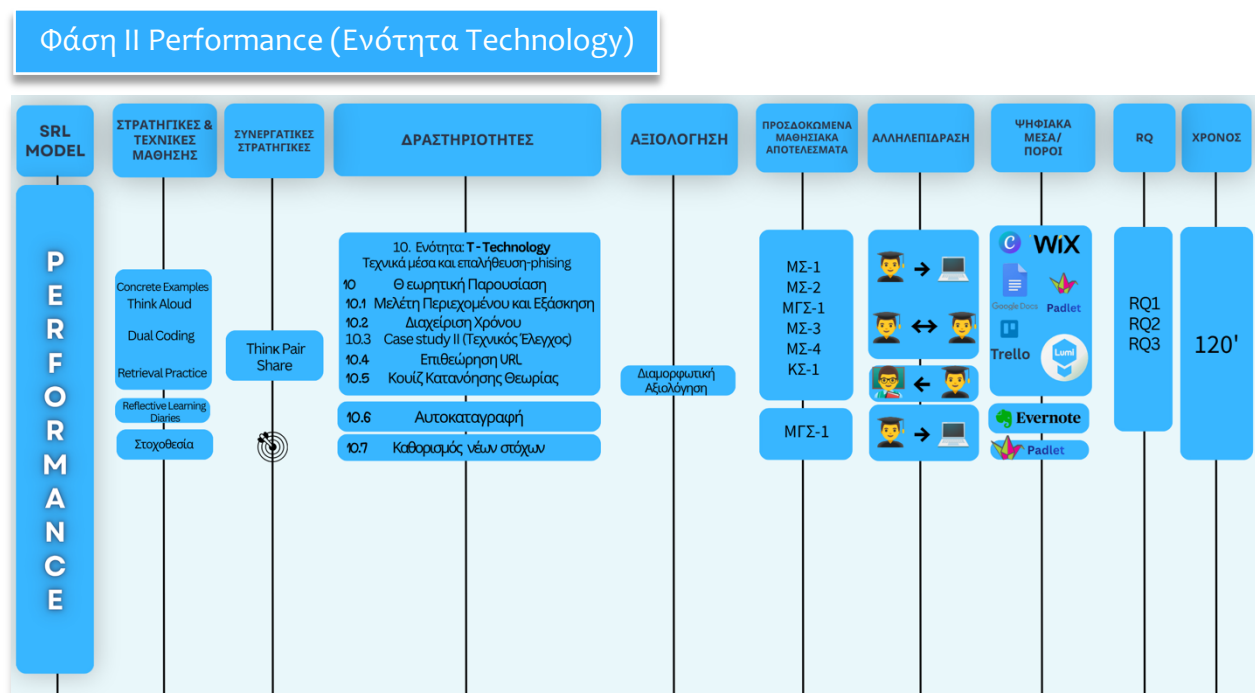
Εικόνα 16: Κουίζ Κατανόησης Θεωρίας (Science)

Περιγραφή: Μετά την παρουσίαση της θεωρίας για την κοινωνική μηχανική, οι φοιτητές ολοκληρώνουν ένα σύντομο Κουίζ Κατανόησης Θεωρίας, πέντε ερωτήσεων (τέσσερις πολλαπλής επιλογής, μία Σωστό/Λάθος), εστιασμένων στον ορισμό της κοινωνικής μηχανικής, τον στόχο των phishing emails, την αυθεντία ως αρχή πειθούς, την επίδραση του γνωστικού φόρτου και τη σημασία της γνώσης γύρω από κυβερνοαπειλές. Για κάθε ερώτηση παρέχεται ανατροφοδότηση που εξηγεί γιατί μια επιλογή είναι σωστή ή λανθασμένη, βοηθώντας τους φοιτητές να κατανοήσουν πώς οι επιθέσεις κοινωνικής μηχανικής αξιοποιούν την ανθρώπινη ψυχολογία και τον γνωστικό φόρτο. Η δραστηριότητα αυτή εντάσσεται στην ενδιάμεση αξιολόγηση και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

Πηγές Κουίζ: (Ferreira & Teles, 2019; Montañez et al., 2020).

○ Δραστηριότητα 9.8: Αυτοκαταγραφή

Περιγραφή: Ολοκληρώνοντας την ενότητα Science, ο κάθε φοιτητής ανοίγει το εργαλείο Evernote και κρατά έναν σύντομο απολογισμό: ποια σημεία της θεωρίας για την κοινωνική μηχανική νιώθει ότι κατέχει καλά, ποια χρειάζονται μία ακόμη επανάληψη και πού δυσκολεύτηκε περισσότερο μέχρι εκείνο το σημείο. Χρησιμοποιείται η τεχνική Reflective Learning Diary (Chulan et al., 2025), μέσω της οποίας οι φοιτητές σημειώνουν ποια στάδια της θεωρίας κατανόησαν καλά και πού χρειάζεται αναθεώρηση, ώστε να προσαρμόσουν τα επόμενα βήματά τους, στο πλαίσιο της αυτοκαταγραφής (Zimmerman, 2002).

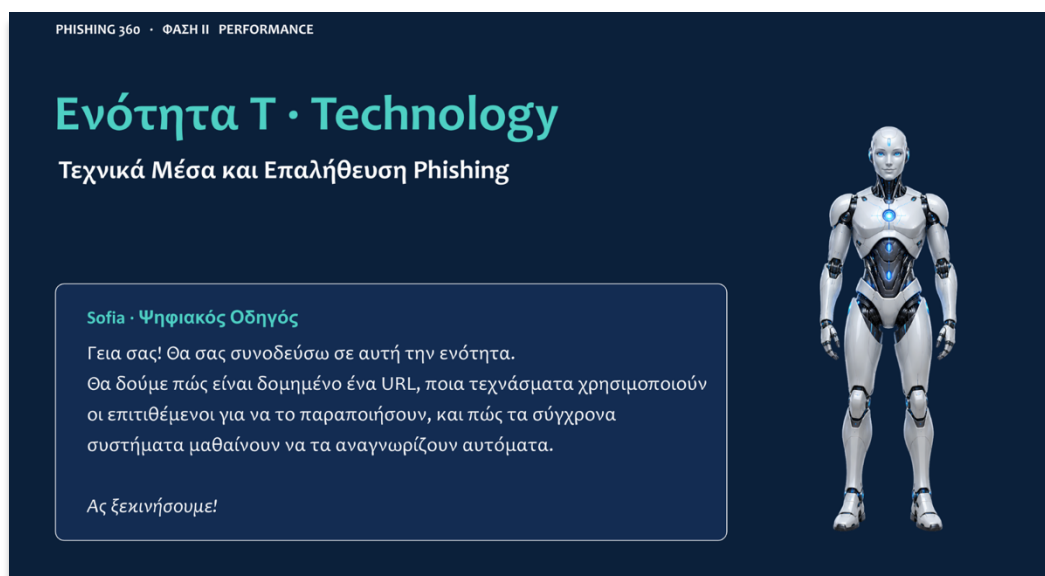


Σχήμα 7: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Technology

Πίνακας 12: Ανάλυση Ενότητας Technology (Φάση II Performance)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΣ-3, ΜΣ-4, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Think-Aloud, Retrieval Practice, Concrete Examples, Dual Coding, Reflective Learning Diaries.
Συνεργατικές στρατηγικές	Think-Pair-Share.
Στρατηγικές αυτορρύθμισης	Καθορισμός στόχων, οργάνωση και μετατροπή πληροφορίας, επανάληψη και απομνημόνευση, αυτοκαταγραφή, αναζήτηση βοήθειας.
Θεωρητική σύνδεση	Οι δύο κεντρικές διαδικασίες της φάσης Performance. Ο αυτοέλεγχος (self-control), που περιλαμβάνει τη διαχείριση χρόνου, και η αυτοπαρατήρηση (self-observation), μέσω αυτοκαταγραφής.
Αξιολόγηση	Διαμορφωτική Αξιολόγηση (Κουίζ Κατανόησης Θεωρίας, βαθμολογούμενο).
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα, χωρίς σύγχρονη παρουσία, καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Technology (Τεχνολογία). Οι φοιτητές μελετούν τη δομή ενός URL, τεχνικές παραπλάνησης και μεθόδους τεχνικής ανίχνευσης phishing, εφαρμόζοντας τη γνώση σε πραγματικά εργαλεία ελέγχου.

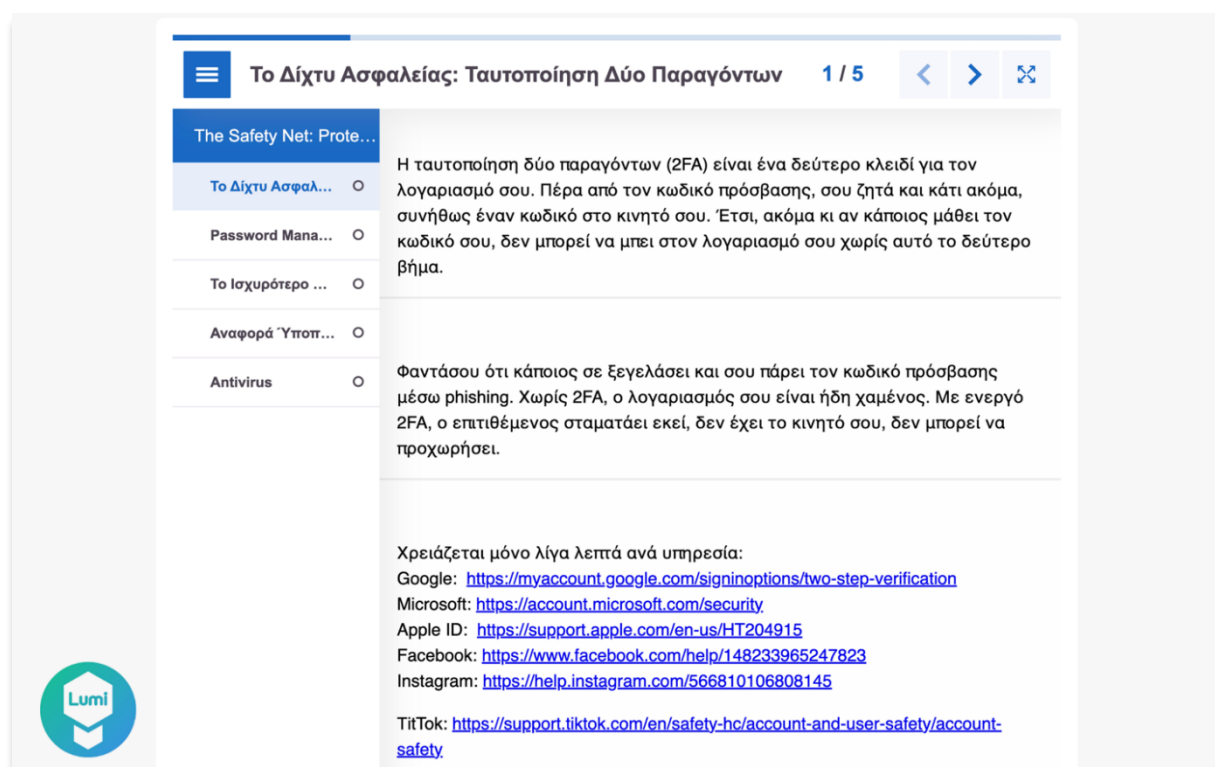
ο Δραστηριότητα 10: Θεωρητική Παρουσίαση



Εικόνα 17: Θεωρητική Παρουσίαση Ενότητας Technology

Περιγραφή: Η ενότητα ξεκινά με μια θεωρητική παρουσίαση, στο εργαλείο Google Slides, όπου η ψηφιακή βοηθός Σοφία καλωσορίζει τους φοιτητές στην ενότητα Technology και τους ενημερώνει για όσα πρόκειται να μάθουν. Η παρουσίαση αναλύει τη δομή ενός URL (πρωτόκολλο, subdomain, domain, path), τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να παραπλανήσουν τον χρήστη αξιοποιώντας συγκεκριμένα παραδείγματα (Concrete Examples) (Rawson et al., 2015), όπως τυχαίοι χαρακτήρες, cybersquatting, typosquatting, καθώς και τον τρόπο με τον οποίο τα σύγχρονα συστήματα ανιχνεύουν τεχνικά ένα phishing URL, συγκρίνοντας παραδοσιακές μεθόδους με μεθόδους μηχανικής μάθησης. Η ενότητα κλείνει με στατιστικά στοιχεία που τεκμηριώνουν την αναγκαιότητα της τεχνικής εκπαίδευσης απέναντι στον κίνδυνο του phishing (Kenneth et al., 2023; Marshall et al., 2024; Sahingoz et al., 2019).

Επιπλέον, κάτω από την κύρια παρουσίαση, υπάρχει δεύτερο κουμπί με τίτλο «The Safety Net: Protective Measures», υλοποιημένο ως Interactive Book⁹ στο εργαλείο Lumi. Η ενότητα αυτή λειτουργεί συμπληρωματικά, παρουσιάζοντας πρακτικά μέτρα προστασίας που μπορεί να λάβει κάθε φοιτητής, όπως η ενεργοποίηση ταυτοποίησης δύο παραγόντων (2FA), η χρήση password manager, η χρήση φυσικού κλειδιού ασφαλείας (security key), η αναφορά ύποπτων email και η χρήση antivirus λογισμικού. Κάθε μέτρο περιλαμβάνει σύνδεσμο προς την αντίστοιχη επίσημη σελίδα ρυθμίσεων. Στη δραστηριότητα αυτή αξιοποιείται η στρατηγική αναζήτησης βοήθειας (help-seeking) της Αυτορρυθμιζόμενης Μάθησης, καθώς η άμεση πρόσβαση σε συγκεκριμένους πόρους δράσης υποστηρίζει τον φοιτητή τη στιγμή που χρειάζεται καθοδήγηση (Barnard et al., 2009).



Εικόνα 18: Interactive Book (Lumi)

⁹ Η φωτογραφία εξωφύλλου του Interactive Book προέρχεται από έτοιμο πρότυπο (template) του Canva.

○ Δραστηριότητα 10.1: Μελέτη Περιεχομένου & Εξάσκηση

Μελέτη Περιεχομένου και Πρακτική Εφαρμογή

Ενημερώνεται αυτόματα κάθε 5 λεπτά



Sofia — Ψηφιακός Οδηγός

Γεια σας ξανά! Πριν περάσουμε στην πράξη, ας θυμηθούμε τα βασικά από τη θεωρία.

Σύντομη Επανάληψη

- Ένα URL αποτελείται από το πρωτόκολλο, το subdomain, το domain name (SLD και TLD) και το path. Το domain name είναι το πιο κρίσιμο σημείο ελέγχου της αυθεντικότητας μιας σελίδας.
- Οι επιθέμενοι παραπλανούν τον χρήστη με τυχαίους χαρακτήρες στο domain, συνδυασμό λέξεων γνωστών επωνυμιών, cybersquatting και typosquatting.
- Οι καλύτερες μέθοδοι ανίχνευσης με λίστες (blacklist/whitelist) πετυχαίνουν γύρω στο 20%. Η μηχανική μάθηση, αναλύοντας το ίδιο το κείμενο του URL, έφτασε σε ακρίβεια 97.98%.
- Σε πραγματική έρευνα, το 76% των φοιτητών άνοιξε ένα πειραματικό phishing email και το 22% έκανε τελικά κλικ στον ύποπτο σύνδεσμο.
- Η εκπαίδευση κάνει τη διαφορά: σε ανασκόπηση 42 μελετών, το ποσοστό μη αναγνωρισμένων phishing email έπεσε από 43% σε 25% μετά από εκπαίδευση, δηλαδή μέση βελτίωση 20%.

Εικόνα 19: Μελέτη Περιεχομένου & Εξάσκηση (Technology)

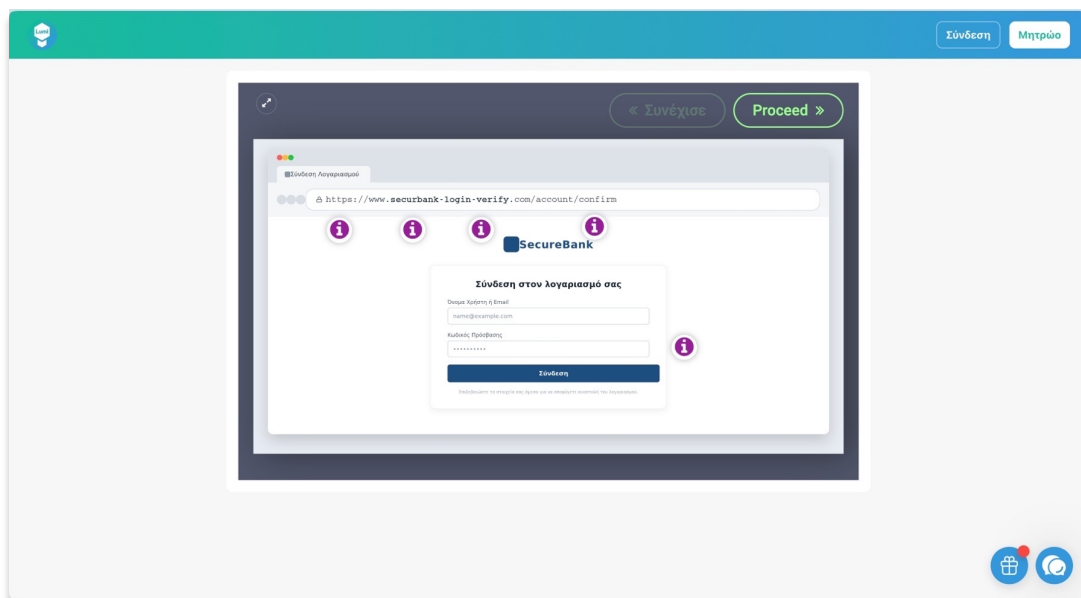
Περιγραφή: Σε αυτή τη δραστηριότητα, οι φοιτητές έχουν πρόσβαση σε ένα υπερκείμενο στο εργαλείο Google Docs με ενεργούς συνδέσμους προς πραγματικά sites και εργαλεία ελέγχου. Το έγγραφο ξεκινά με σύντομη επανάληψη της θεωρίας (δομή URL, τεχνικές παραπλάνησης, μέθοδοι τεχνικής ανίχνευσης) (Kenneth et al., 2023; Marshall et al., 2024; Sahingoz et al., 2019) και παραθέτει δύο πίνακες με πραγματικά sites όπως temu.com, wikipedia.org, amazon.com και εργαλεία τεχνικού ελέγχου όπως τα VirusTotal, URLVoid, CheckPhish. Οι φοιτητές ανοίγουν κάθε site και το ελέγχουν σε καθένα από τα τρία εργαλεία, ακολουθώντας τη μέθοδο Think-Aloud, προσαρμοσμένη σε ψηφιακό πλαίσιο ελέγχου αξιοπιστίας ιστοσελίδων (Coiro, 2011).

Πριν από κάθε ενέργεια, οι εκπαιδευόμενοι καταγράφουν την πρόβλεψή τους, και αμέσως μετά το αποτέλεσμα κάθε εργαλείου, καταγράφουν τη σκέψη που τους προκαλεί, καθιστώντας ορατή ολόκληρη τη διαδρομή του συλλογισμού τους αντί μόνο το τελικό αποτέλεσμα. Έτσι, η θεωρητική γνώση για την τεχνική ανίχνευση phishing εφαρμόζεται άμεσα σε πραγματικά, λειτουργικά εργαλεία.

○ Δραστηριότητα 10.2: Διαχείριση χρόνου (Time Management)

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές χρησιμοποιούν το εργαλείο Trello για να οργανώσουν τον χρόνο τους κατά τη μελέτη των τεχνικών μέσων ανίχνευσης phishing. Δημιουργούν πίνακα με καρτέλες για κάθε βήμα της ενότητας, όπως τη μελέτη της δομής ενός URL, την πρακτική εξάσκηση με τα εργαλεία ελέγχου και την τεχνική επιθεώρηση, ορίζοντας προθεσμίες για καθεμία. Η οπτική οργάνωση του Trello βοηθά τους φοιτητές να διαχειριστούν αποτελεσματικά τον ρυθμό μελέτης τους σε μια ενότητα με αρκετά τεχνικό περιεχόμενο, ενισχύοντας παράλληλα την αυτορρύθμιση και την υπευθυνότητα απέναντι στον προσωπικό τους χρόνο. Με τον τρόπο αυτό, οι φοιτητές εφαρμόζουν στην πράξη τη στρατηγική SRL της διαχείρισης χρόνου, αποκτώντας μια οπτική εικόνα της προόδου τους και μαθαίνοντας να θέτουν ρεαλιστικά χρονικά όρια για κάθε βήμα της μάθησής τους (Zimmerman, 2002).

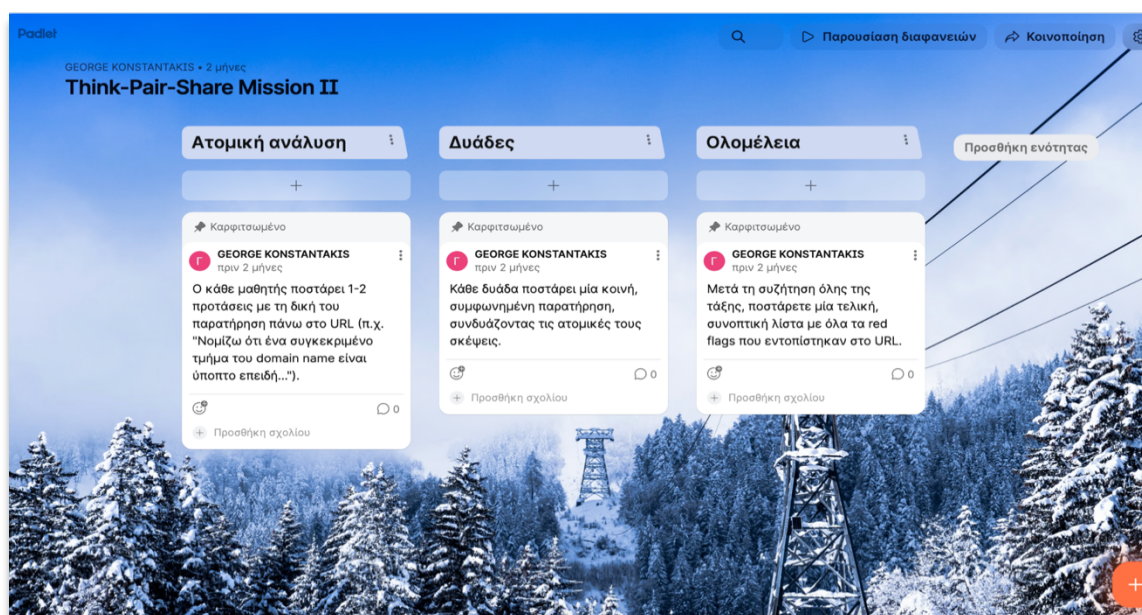
○ Δραστηριότητα 10.3: Τεχνική Επιθεώρηση Case Study II



Εικόνα 20: Τεχνική Επιθεώρηση Case Study II

Περιγραφή: Εδώ, οι φοιτητές δουλεύουν στο Lumi πάνω σε Branching σενάριο τεχνικής επιθεώρησης URL εξετάζοντας μια πλαστή σελίδα σύνδεσης πριν εισάγουν οποιοδήποτε στοιχείο. Η χρήση διαδραστικού σεναρίου H5P (branching scenario) είναι τεχνική μάθησης που ενισχύει την εμπλοκή και τη θετική εμπειρία των φοιτητών σε ψηφιακά περιβάλλοντα μάθησης (Jacob & Centofanti, 2024). Στην πρώτη εικόνα, οι φοιτητές πατάνε τα hotspots πάνω στο URL μιας ψεύτικης τραπεζικής σελίδας και βλέπουν εξηγήσεις για typosquatting, συνδυασμό λέξεων κλειδιών, απουσία ελέγχου δύο παραγόντων ταυτοποίησης (απαιτείται πάντα βάσει PSD2), καθώς και για αθώα στοιχεία όπως HTTPS ή path, με άμεση επεξήγησή σε κάθε hotspot. Ακολουθεί ερώτηση πολλαπλής επιλογής για το πιο κρίσιμο σημείο ελέγχου αυθεντικότητας ενός URL, με ανατροφοδότηση σε σωστή και λανθασμένες απαντήσεις. Στη δεύτερη εικόνα, οι φοιτητές εφαρμόζουν την ίδια λογική σε μια ψεύτικη σελίδα PayPal με διαφορετικό τέχνασμα, παραπλανητικό subdomain, όπου το «paypal.com» μοιάζει domain αλλά είναι απλώς υποτμήμα άλλου, πραγματικού domain. Πατώντας τα ίδια hotspots βλέπουν ποιο κομμάτι είναι το πραγματικό domain, εμπεδώνοντας όσα διδάχθηκαν για τη δομή URL (Sahingoz et al., 2019). Ο συνδυασμός εικόνας και επεξηγηματικού κειμένου σε κάθε hotspot αξιοποιεί την αρχή του Dual Coding (Clark & Paivio, 1987).

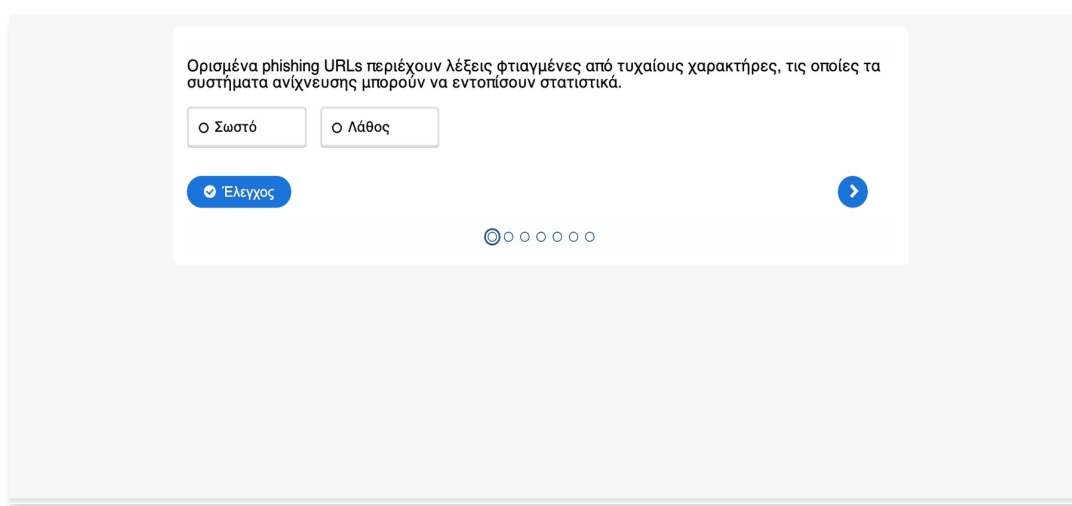
ο Δραστηριότητα 10.4: Επιθεώρηση URL



Εικόνα 21: Επιθεώρηση URL με τη στρατηγική Think-Pair-Share

Περιγραφή: Στη δραστηριότητα αυτή, ο ψηφιακός οδηγός Σοφία δίνει στους φοιτητές τις οδηγίες σε Google Doc, ενημερώνοντάς τους ότι θα εφαρμόσουν την ίδια λογική τεχνικής ανάλυσης URL σε ένα καινούργιο, πραγματικό URL, πρώτα ατομικά και μετά σε συνεργασία με τον διπλανό τους. Οι φοιτητές εξετάζουν το URL τμήμα προς τμήμα και εντοπίζουν ποια σημεία θεωρούν ύποπτα και γιατί, και στη συνέχεια μεταβαίνουν στο Padlet της δραστηριότητας, όπου καταγράφουν τις παρατηρήσεις τους σε τρία στάδια: ατομικά, σε δυάδες με τον διπλανό τους, και τέλος στην ολομέλεια της τάξης, σύμφωνα με τη λογική της στρατηγικής Think-Pair-Share (Sembert et al., 2021).

ο Δραστηριότητα 10.5: Κουίζ Κατανόησης Θεωρίας



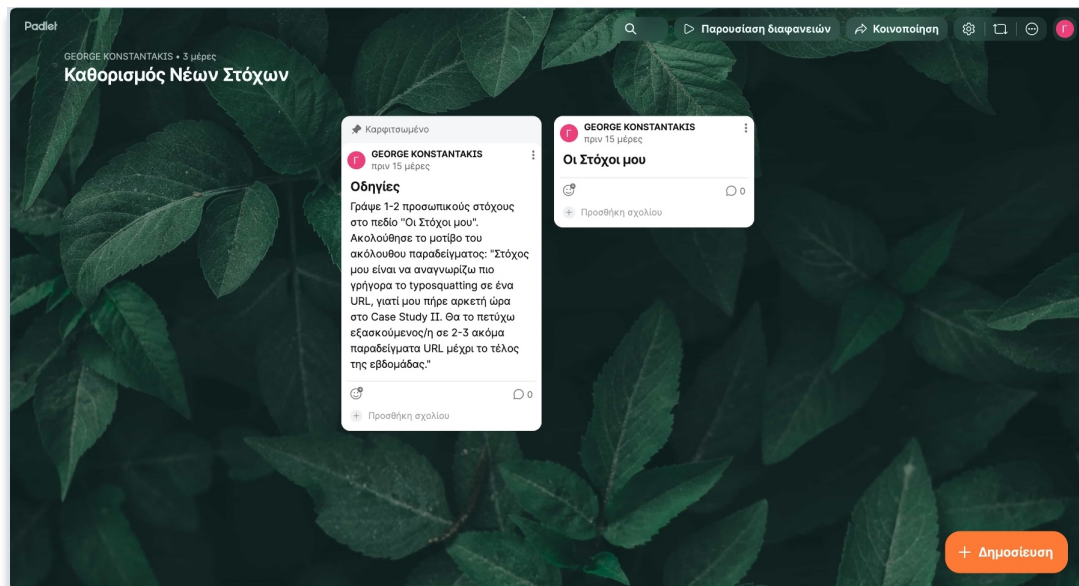
Εικόνα 22: Κουίζ Κατανόησης Θεωρίας (Technology)

Περιγραφή: Οι φοιτητές συμπληρώνουν ένα κουίζ σωστό/λάθος επτά ερωτήσεων στο εργαλείο Lumi, ελέγχοντας την κατανόηση βασικών τεχνικών στοιχείων της ενότητας Technology (Sahingoz et al., 2019), όπως τη σημασία του domain name ως κρίσιμο σημείο ελέγχου αυθεντικότητας, το γεγονός ότι το path καθορίζεται ελεύθερα, τεχνικές παραπλάνησης όπως typosquatting και combined word usage, την ευκολία αγοράς/αντιγραφής ενός SLD, καθώς και δύο τεχνικά χαρακτηριστικά ανίχνευσης: στατιστικό εντοπισμό τυχαίων χαρακτήρων και έλεγχο TLD. Κάθε ερώτηση συνοδεύεται από ανατροφοδότηση, τόσο για τη σωστή απάντηση όσο και για τις λανθασμένες. Η δραστηριότητα αυτή εντάσσεται στην ενδιάμεση αξιολόγηση και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

ο Δραστηριότητα 10.6: Αυτοκαταγραφή

Περιγραφή: Στο κλείσιμο της ενότητας Technology, ο κάθε φοιτητής συνοψίζει στο εργαλείο Evernote τι κατάλαβε από τα τεχνικά χαρακτηριστικά ανίχνευσης phishing και σε ποια σημεία θεωρεί ότι χρειάζεται περισσότερη εξάσκηση. Σημειώνει επίσης τις δυσκολίες που συνάντησε μέχρι εκείνο το σημείο, ώστε να έχει σαφή εικόνα των κενών του πριν προχωρήσει στην επόμενη ενότητα. Η καταγραφή αυτών των δυσκολιών μέσω της τεχνικής Reflective Learning Diary (Chulan et al., 2025) βοηθάει τους εκπαιδευόμενους να σχεδιάσουν καλύτερα τα επόμενα βήματά τους, στο πλαίσιο της αυτοκαταγραφής (Zimmerman, 2002).

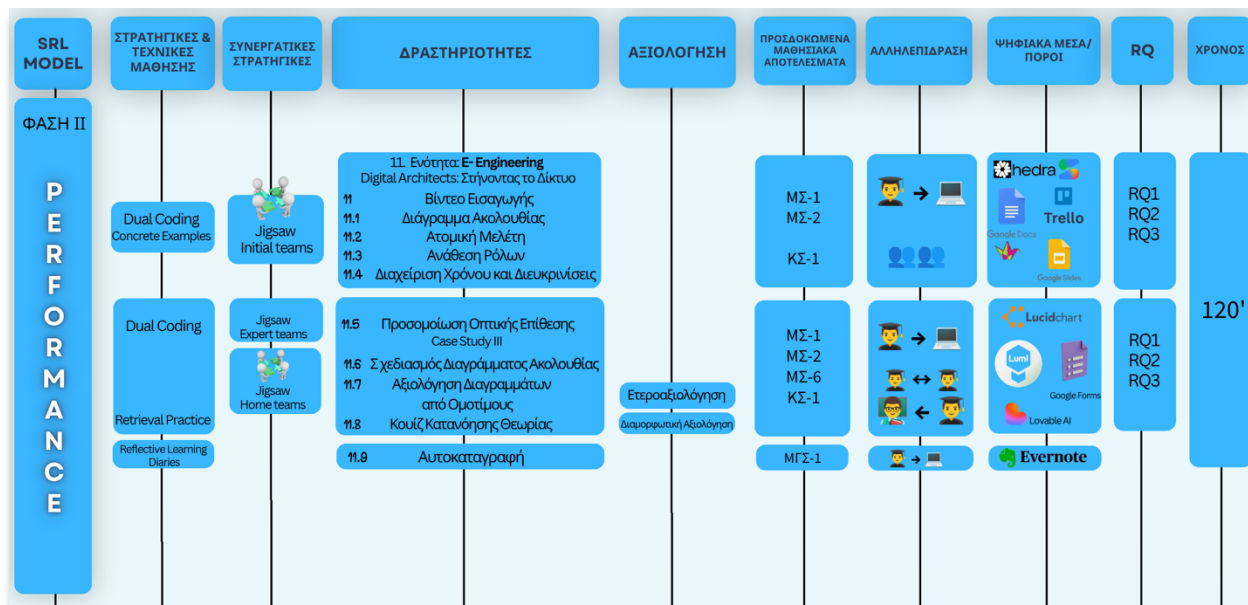
ο Δραστηριότητα 10.7: Καθορισμός νέων στόχων



Εικόνα 23: Καθορισμός νέων στόχων

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές γράφουν στο Padlet 1 έως 2 προσωπικούς στόχους στο πεδίο «Οι Στόχοι μου», ακολουθώντας συγκεκριμένο μοτίβο. Αναφέρουν τι θέλουν να βελτιώσουν, γιατί, βασιζόμενοι σε δυσκολία που συνάντησαν σε προηγούμενη δραστηριότητα, και πώς σκοπεύουν να το πετύχουν μέχρι συγκεκριμένο χρονικό ορίζοντα, όπως στο παράδειγμα που δίνεται από τον καθηγητή: «Στόχος μου είναι να αναγνωρίζω πιο γρήγορα το typosquatting σε ένα URL, γιατί μου πήρε αρκετή ώρα στο Case Study II. Θα το πετύχω εξασκούμενος ή εξασκούμενη σε 2 έως 3 ακόμα παραδείγματα URL μέχρι το τέλος της εβδομάδας.» Η δραστηριότητα εντάσσεται στη διαδικασία της ανάλυσης έργου (task analysis), κατά την οποία ο φοιτητής θέτει νέους στόχους (Zimmerman, 2002).

Φάση II Performance (Ενότητα Engineering)



Σχήμα 8: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Engineering

Πίνακας 13: Ανάλυση Ενότητας Engineering (Φάση II Performance)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΣ-6, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Dual Coding, Concrete Examples, Retrieval Practice, Reflective Learning Diaries.
Συνεργατικές στρατηγικές	Jigsaw, Ετεροαξιολόγηση.
Στρατηγικές αυτορρύθμισης	Αναζήτηση πληροφοριών, επανάληψη και απομνημόνευση, οργάνωση και μετατροπή πληροφορίας (διαγράμματα), αυτοκαταγραφή.
Θεωρητική σύνδεση	Ενεργοποίηση κινήτρων (self-motivation beliefs), ενδιαφέρον για το έργο, στο εισαγωγικό βίντεο. Αυτοέλεγχος (self-control), αναζήτηση πληροφοριών και διαχείριση χρόνου. Αυτοπαράτηρηση (self-observation), μέσω αυτοκαταγραφής.
Αξιολόγηση	Διαμορφωτική αξιολόγηση (Κουίζ Κατανόησης Θεωρίας) βαθμολογούμενο.
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα, χωρίς σύγχρονη παρουσία, καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Engineering (Μηχανική). Οι φοιτητές αναλαμβάνουν τον ρόλο μηχανικού που σχεδιάζει την τεχνική υποδομή μιας phishing επίθεσης, μοντελοποιώντας τη ροή της σε διάγραμμα ακολουθίας μέσα από συνεργασία ομάδων ειδικών.

ο Δραστηριότητα 11: Εισαγωγικό βίντεο¹⁰



Εικόνα 24: Εισαγωγικό Βίντεο (Engineering)

Περιγραφή: Η ψηφιακή βοηθός Σοφία, σε ρεαλιστική μορφή avatar, που ενισχύει το ενδιαφέρον και την παρακίνηση των εκπαιδευόμενων (Baylor, 2011), καλωσορίζει τους φοιτητές στην αποστολή Engineering, εξηγώντας τους ότι θα αναλάβουν τον ρόλο του μηχανικού που σχεδιάζει μια επίθεση phishing. Το βίντεο δίνει μια συνοπτική προεπισκόπηση της ροής της ενότητας: θεωρητικό διάγραμμα ροής, ατομική μελέτη τεχνικής υποδομής, οργάνωση χρόνου σε ομάδες ειδικών, προσομοίωση πραγματικής επίθεσης με εντοπισμό ύποπτων σημείων, και τελικά το σχεδιασμό ενός κοινού τεχνικού διαγράμματος ροής στις αρχικές ομάδες (Home Teams). Στο ανωτέρω βίντεο, χρησιμοποιήθηκαν τα AI εργαλεία Google AI Studio και Hedra (Google, 2026a; Hedra, 2026).

¹⁰ Χρησιμοποιήθηκαν τα εργαλεία Hedra AI (Hedra, 2026) και Google AI Studio (Google, 2026a) στο εισαγωγικό βίντεο. Το Hedra AI αξιοποιήθηκε για τη δημιουργία του avatar της ψηφιακής βοηθού «Σοφία», ενώ το Google AI Studio χρησιμοποιήθηκε για τη μετατροπή κειμένου σε ομιλία (text-to-speech), αποδίδοντας φωνητικά το σενάριο που παρατίθεται ανωτέρω. Η μουσική υπόκρουση που χρησιμοποιήθηκε στο βίντεο προέρχεται από την πλατφόρμα Pixabay (Pixabay, 2026), υπό την άδεια Pixabay Content License, η οποία επιτρέπει τη δωρεάν χρήση του περιεχομένου χωρίς υποχρέωση αναφοράς του δημιουργού. Η χρήση των εργαλείων είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε από τον συγγραφέα πριν ενσωματωθεί στο βίντεο.

Εκφώνηση σεναρίου:

«Καλησπέρα σε όλους. Καλωσορίσατε στην αποστολή Engineering, όπου θα μπείτε στον ρόλο του μηχανικού που σχεδιάζει μια επίθεση phishing. Θα ξεκινήσουμε με ένα θεωρητικό διάγραμμα ροής που θα σας δείξει βήμα-βήμα πώς εξελίσσεται μια τέτοια επίθεση, και θα συνεχίσουμε με ατομική μελέτη του θεωρητικού υλικού, ώστε να κατανοήσετε την τεχνική υποδομή της. Στη συνέχεια θα χωριστείτε σε ομάδες ειδικών, οργανώνοντας τον χρόνο σας ώστε να προλάβετε να ολοκληρώσετε την προετοιμασία σας εγκαίρως. Θα δείτε μια προσομοίωση πραγματικής επίθεσης και θα εντοπίσετε τα ύποπτα σημεία της. Έπειτα θα επιστρέψετε στην αρχική σας ομάδα, όπου όλοι μαζί θα σχεδιάσετε το δικό σας τεχνικό διάγραμμα ροής, είσαστε έτοιμοι;».

Πηγές σεναρίου εισαγωγικού βίντεο: (Luse & Burkman, 2021; Morić et al., 2025)

ο Δραστηριότητα 11.1: Διάγραμμα Ακολουθίας¹¹



Εικόνα 25: Διάγραμμα Ακολουθίας

¹¹ Χρησιμοποιήθηκε το εργαλείο Lovable AI (Lovable, 2026), για τη δημιουργία του ανωτέρω θεωρητικού διαγράμματος ακολουθίας. Η χρήση του είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε και τροποποιήθηκε από τον συγγραφέα πριν την ενσωμάτωσή του στο Wix.

Περιγραφή: Στη δραστηριότητα αυτή παρουσιάζεται ένα θεωρητικό διάγραμμα ροής (attack flow diagram), σχεδιασμένο ως διαδραστική εφαρμογή στο εργαλείο Lovable AI (Lovable, 2026), το οποίο απεικονίζει σε 8 διαδοχικά βήματα την πλήρη εξέλιξη μιας επίθεσης phishing: από την τεχνική υποδομή (domain, server, mail routing), τη ρύθμιση του phishing email και τη δημιουργία της ψεύτικης σελίδας, μέχρι τα τρία στάδια ευπάθειας του θύματος (άνοιγμα, κλικ, υποβολή στοιχείων) και την καταγραφή των τελικών αποτελεσμάτων (Morić et al., 2025). Στόχος είναι οι εκπαιδευόμενοι να αποκτήσουν μια πρώτη οπτική κατανόηση της αλληλουχίας της επίθεσης, πριν προχωρήσουν στην ατομική μελέτη και τον σχεδιασμό του δικού τους τεχνικού διαγράμματος. Η ταυτόχρονη παρουσίαση εικόνας και λέξης ενεργοποιεί τη διαδικασία της αναφορικής επεξεργασίας (referential processing) της θεωρίας Dual Coding, κατά την οποία το λεκτικό και το μη λεκτικό σύστημα συνδέονται μεταξύ τους, ενισχύοντας την κωδικοποίηση και την ανάκληση της πληροφορίας (Clark & Paivio, 1987).

ο Δραστηριότητα 11.2: Ατομική Μελέτη

PHISHING 360° · ΦΑΣΗ II PERFORMANCE

Ενότητα Engineering

Digital Architects: Στήνοντας το Δίκτυο

Θεωρητική παρουσίαση της τεχνικής υποδομής, των παραμέτρων ρύθμισης και της μεθοδολογίας μιας επίθεσης phishing, στο πλαίσιο του σχεδιασμού συστημάτων ασφάλειας.

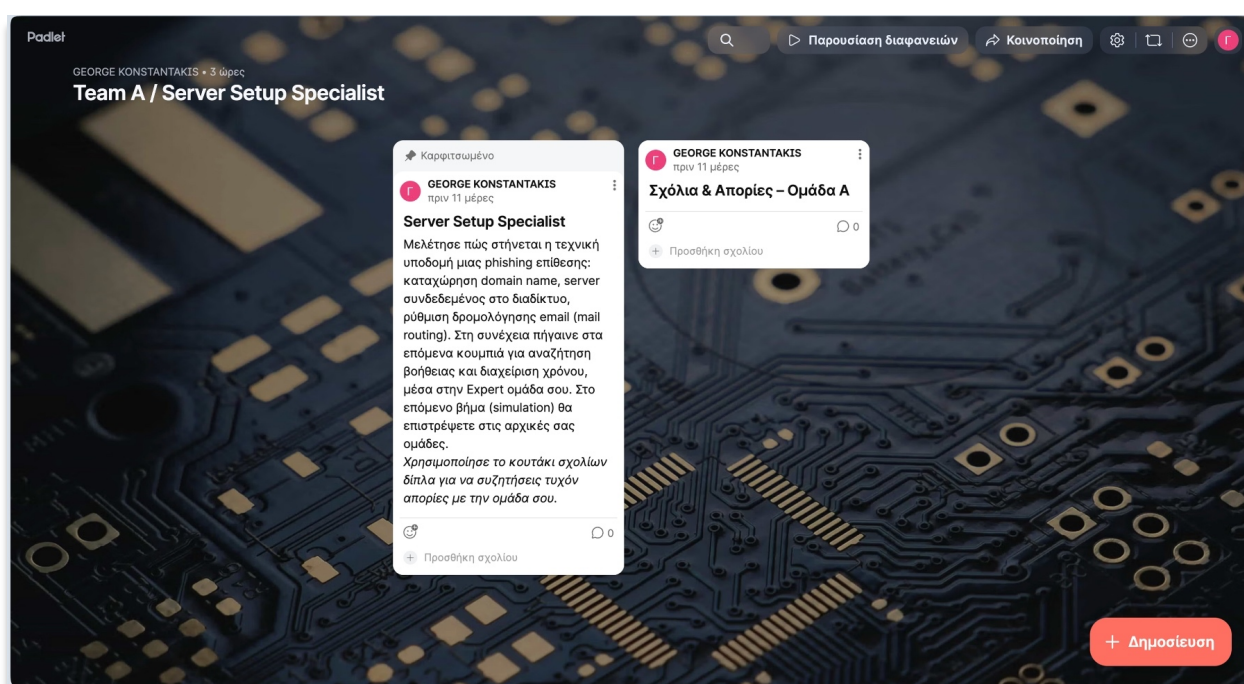
● Sofia-Ψηφιακός Οδηγός

Εικόνα 26: Ατομική Μελέτη (Engineering)

Περιγραφή: Οι εκπαιδευόμενοι παρακολουθούν μια παρουσίαση 5 διαφανειών στο εργαλείο Google Slides που καλύπτει το θεωρητικό υπόβαθρο της ενότητας Engineering μέσω συγκεκριμένων παραδειγμάτων (Concrete Examples) (Rawson et al., 2015): την τεχνική υποδομή μιας επίθεσης phishing (domain, server, mail routing, hosting, εργαλείο διαχείρισης εκστρατείας), τις παραμέτρους ρύθμισης ενός phishing email (αποστολέας, θέμα, παραπλανητικός σύνδεσμος, ψεύτικη σελίδα σύνδεσης), τα τρία στάδια ευπάθειας του θύματος με πραγματικά δεδομένα από εφαρμοσμένη προσομοίωση, καθώς και τη μεθοδολογία του επιτιθέμενου (πλαίσιο MITRE ATT&CK) (Georgiadou et al., 2021) σε συνδυασμό με την οργάνωση σε ομάδες ειδικών (Jigsaw) (Cochon Drouet et al., 2023). Στόχος είναι η εμπέδωση της θεωρίας πριν οι εκπαιδευόμενοι προχωρήσουν στην πρακτική εφαρμογή.

Πηγές θεωρίας: (Arduin & Costé, 2026; Luse & Burkman, 2021; Moric et al., 2025)

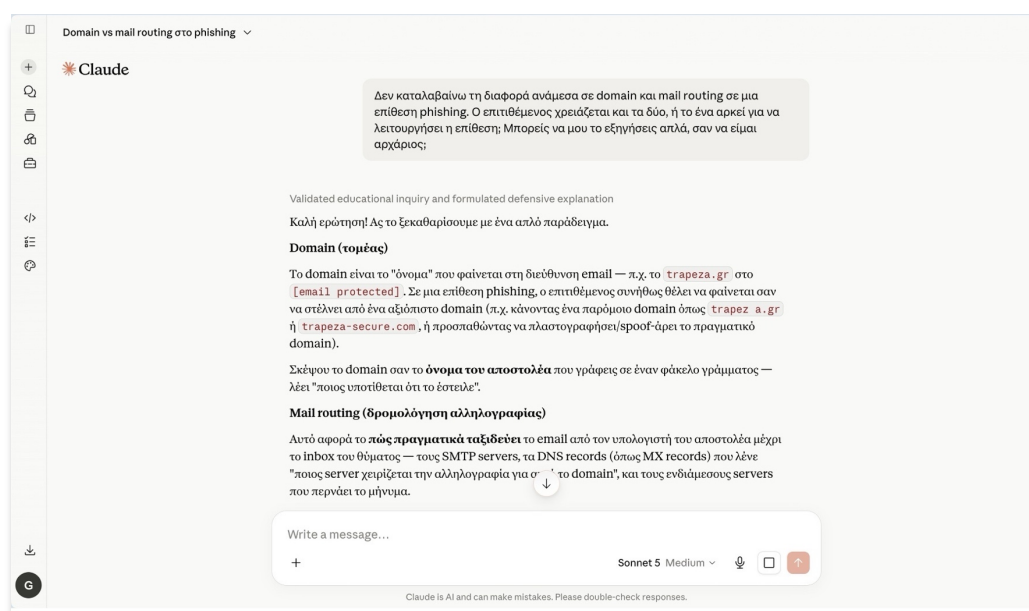
○ Δραστηριότητα 11.3: Ανάθεση Ρόλων



Εικόνα 27: Ανάθεση σε Ομάδες Ειδικών (Jigsaw)

Περιγραφή: Στη δραστηριότητα αυτή, ο ψηφιακός οδηγός Σοφία δίνει στους φοιτητές τις οδηγίες σε Google Doc, ενημερώνοντάς τους ότι θα χωριστούν σε ομάδες ειδικών με τρεις ρόλους: Server Setup Specialist, Flow Architect και Security Analyst, εφαρμόζοντας τη στρατηγική Jigsaw (Kekeba et al., 2024). Κάθε φοιτητής μεταβαίνει στο ξεχωριστό Padlet της ομάδας του: το Team A μελετά την τεχνική υποδομή ως Server Setup Specialist, το Team B μελετά τη ρύθμιση του phishing email ως Flow Architect, και το Team C μελετά τα στάδια ευπάθειας και τα μετρικά αποτελέσματα ως Security Analyst, με βάση το θεωρητικό υλικό της ενότητας (Arduin & Costé, 2026; Moric et al., 2025). Επίσης ενημερώνονται οι φοιτητές και για τα επόμενα βήματα που θα ακολουθήσουν μέσα στην Expert ομάδα τους, πριν την επιστροφή στην αρχική τους ομάδα.

○ Δραστηριότητα 11.4: Διαχείριση Χρόνου και Διευκρινίσεις



Εικόνα 28: Αναζήτηση διευκρινήσεων στο Claude AI

Περιγραφή: Στη δραστηριότητα αυτή, οι εκπαιδευόμενοι, ως Expert Teams, έχουν πρόσβαση σε δύο κουμπιά. Αν έχουν απορίες πάνω στο υλικό μελέτης του ρόλου τους, πατούν το πρώτο κουμπί και μεταφέρονται στο Claude AI, όπου αναζητούν διευκρινίσεις σχετικά με όσα μελέτησαν, εφαρμόζοντας τη στρατηγική της αναζήτησης πληροφοριών (Zimmerman, 2002). Πατώντας το επόμενο κουμπί, μεταφέρονται στο εργαλείο Trello, όπου οργανώνουν τον χρόνο τους μέσα στον ρόλο ειδικότητας που έχουν αναλάβει, εφαρμόζοντας παράλληλα τη στρατηγική της διαχείρισης χρόνου (Zimmerman, 2002), ώστε να ολοκληρώσουν έγκαιρα τη μελέτη τους και να προλάβουν να επιστρέψουν στην αρχική τους ομάδα με τις απαραίτητες γνώσεις.

Δραστηριότητα 11.5: Προσομοίωση Οπτικής Επίθεσης



Εικόνα 29: Δραστηριότητα Οπτικής Επίθεσης (Case Study III)

Περιγραφή: Οι εκπαιδευόμενοι παρακολουθούν μια οπτική προσομοίωση μιας επίθεσης phishing, μέσω διακλαδωτού σεναρίου (branching scenario), σε 8 διαδοχικά στάδια: από την καταχώρηση domain και server, τη ρύθμιση του phishing email και τη δημιουργία της ψεύτικης σελίδας, μέχρι τα τρία στάδια ευπάθειας του θύματος (άνοιγμα email, κλικ στον σύνδεσμο, υποβολή στοιχείων) και την καταγραφή των τελικών αποτελεσμάτων. Σε κάθε στάδιο, μέσω σημείων αλληλεπίδρασης (hotspots), οι εκπαιδευόμενοι λαμβάνουν επεξηγήσεις πάνω στα τεχνικά στοιχεία που καθιστούν την επίθεση πειστική. Η δραστηριότητα ολοκληρώνεται με ερώτηση αναστοχασμού πάνω στα πραγματικά δεδομένα που παρουσιάστηκαν, πριν οι εκπαιδευόμενοι επιστρέψουν στην αρχική τους ομάδα για τον σχεδιασμό τεχνικού διαγράμματος ροής. Η ταυτόχρονη παρουσίαση εικόνας και επεξηγηματικού κειμένου σε κάθε hotspot ενισχύει την κωδικοποίηση της πληροφορίας, σύμφωνα με την αρχή του Dual Coding (Clark & Paivio, 1987).

Πηγές: (Luse & Burkman, 2021; Morić et al., 2025).

○ Δραστηριότητα 11.6: Σχεδιασμός Διαγράμματος Ακολουθίας

Περιγραφή: Οι εκπαιδευόμενοι, ως αρχική ομάδα, βλέπουν οδηγίες στο εργαλείο Google Docs σχετικά με τη μοντελοποίηση της επίθεσης phishing που είδαν στην προσομοίωση, ως τεχνικό διάγραμμα αλληλουχίας με τρεις οντότητες: επιτιθέμενος, σύστημα ή εργαλείο, και θύμα. Στη συνέχεια μεταβαίνουν στο σχεδιαστικό εργαλείο Lucidchart, όπου σχεδιάζουν μαζί το διάγραμμα, με κάθε μέλος να συνεισφέρει το τεχνικό περιεχόμενο του ρόλου του. Τέλος, μέσω του κουμπιού «Submit Assignment», συνδέονται στην αντίστοιχη ενότητα εργασιών στο Google Classroom, «Παράδοση Sequence Diagram, Ενότητα Engineering», όπου οι εκπαιδευόμενοι ανεβάζουν την εργασία τους, η οποία αξιολογείται με ρουμπρίκα με τα κριτήρια τεχνική ορθότητα και σαφήνεια παρουσίασης.

○ Δραστηριότητα 11.7: Ετεροαξιολόγηση διαγραμμάτων¹²

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές αξιολογούν το διάγραμμα ακολουθίας μιας άλλης ομάδας, συμπληρώνοντας μία φόρμα στο Google forms με επτά δηλώσεις τύπου Likert (κλίμακα 1-5), οι οποίες εξετάζουν την ορθότητα και τη σαφήνεια της τεχνικής υποδομής, των παραμέτρων του phishing email, της ψεύτικης σελίδας, των τριών σταδίων ευπάθειας, της καταγραφής αποτελεσμάτων, της σαφήνειας των βελών, και της συνολικής τεχνικής ακρίβειας του διαγράμματος σε σχέση με την προσομοίωση. Η φόρμα κλείνει με ανοιχτό πεδίο σχολίων και προτάσεων βελτίωσης.

¹² Η αναλυτική φόρμα της ετεροαξιολόγησης διαγραμμάτων παρατίθεται στο Παράρτημα.

○ Δραστηριότητα 11.8: Κουίζ κατανόησης θεωρίας

Ποιο από τα παρακάτω ΔΕΝ αποτελεί μέρος της τεχνικής υποδομής μιας phishing επίθεσης;

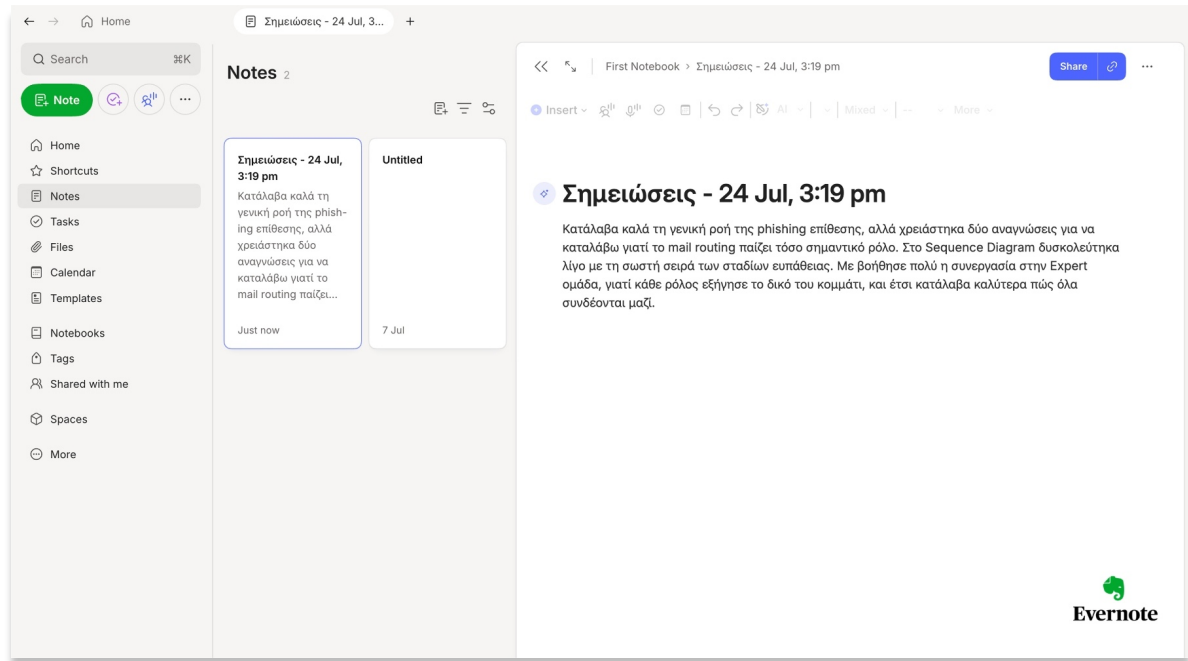
- ☐ A) Καταχώρηση domain name
- ☐ B) Server συνδεδεμένος στο διαδίκτυο
- ☐ C) Antivirus πρόγραμμα
- ☐ D) Mail routing

1 0 0 0 0 0

Εικόνα 30: Κουίζ Κατανόησης Θεωρίας (Engineering)

Περιγραφή: Οι εκπαιδευόμενοι απαντούν σε κουίζ 6 ερωτήσεων (4 πολλαπλής επιλογής, 2 Σωστό/Λάθος) μέσω του εργαλείου Lumi, με στόχο τον έλεγχο κατανόησης βασικών εννοιών της Ενότητας Engineering: την τεχνική υποδομή μιας phishing επίθεσης, τις παραμέτρους ρύθμισης του phishing email, τα τρία στάδια ευπάθειας του θύματος και τον ρόλο της ψεύτικης σελίδας σύνδεσης (Morić et al., 2025). Κάθε ερώτηση συνοδεύεται από άμεση ανατροφοδότηση, τόσο σε σωστή όσο και σε λανθασμένη απάντηση. Η δραστηριότητα αυτή εντάσσεται στην ενδιάμεση αξιολόγηση και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

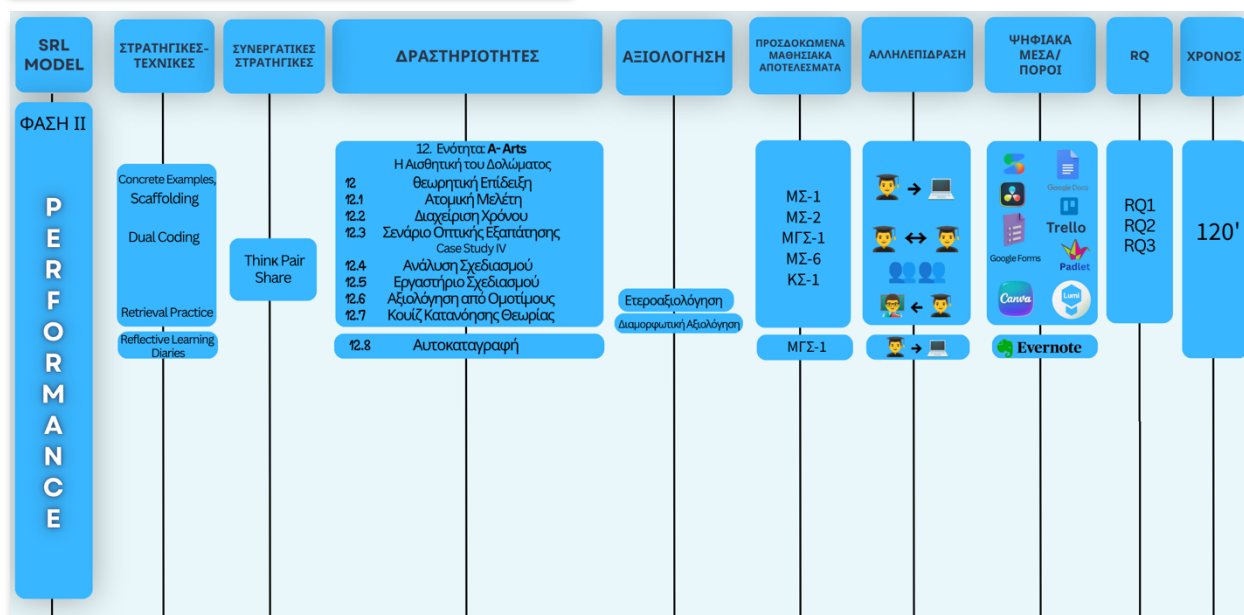
○ Δραστηριότητα 11.9: Αυτοκαταγραφή



Εικόνα 31: Καταγραφή Μαθησιακής Πορείας με το εργαλείο Evernote

Περιγραφή: Ο κάθε φοιτητής ανοίγει το εργαλείο Evernote και σημειώνει ποια στάδια της τεχνικής υποδομής μιας επίθεσης phishing νιώθει ότι έχει κατανοήσει πλήρως, πού δυσκολεύτηκε και τι χρειαζόταν να ξαναδεί. Η καταγραφή αυτών των δυσκολιών μέσω της τεχνικής Reflective Learning Diary (Chulan et al., 2025) βοηθάει τους εκπαιδευόμενους να σχεδιάσουν καλύτερα τα επόμενα βήματά τους, στο πλαίσιο της αυτοκαταγραφής (Zimmerman, 2002).

Φάση II Performance (Ενότητα Arts)

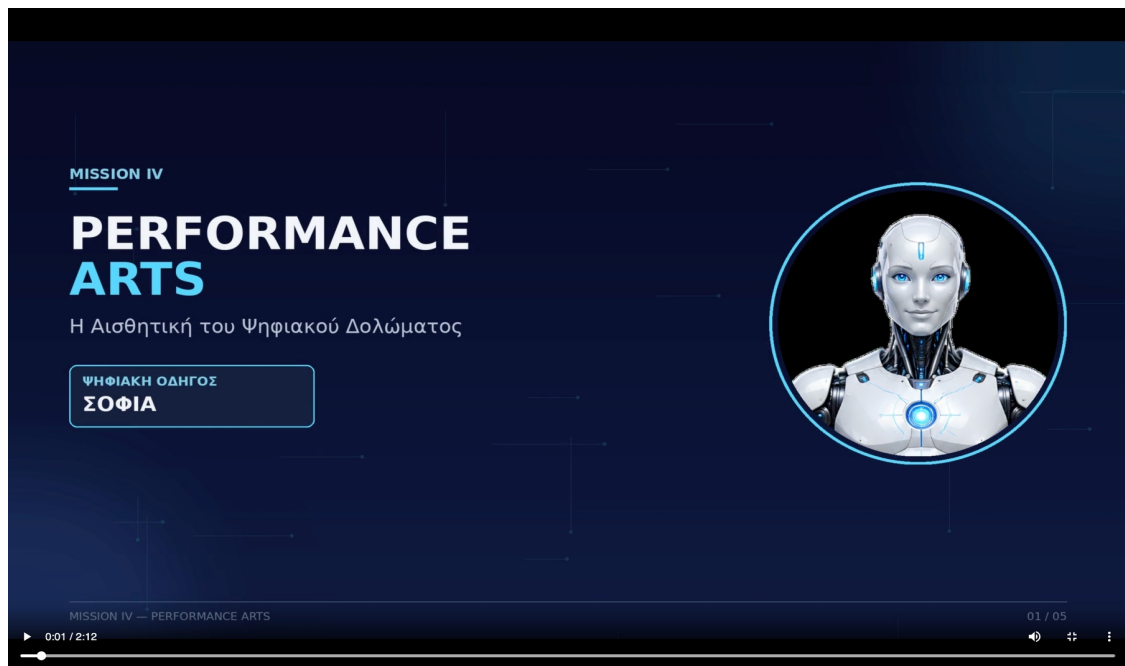


Σχήμα 9: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Arts

Πίνακας 14 : Ανάλυση Ενότητας Arts (Φάση II Performance)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΣ-6, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Concrete Examples, Scaffolding, Dual Coding, Retrieval Practice, Reflective Learning Diaries.
Συνεργατικές στρατηγικές	Think-Pair-Share.
Στρατηγικές Αυτορρύθμισης	Οργάνωση και μετατροπή πληροφορίας, επανάληψη και απομνημόνευση, διαχείριση χρόνου, καταγραφή αρχείων και αυτοκαταγραφή.
Θεωρητική σύνδεση	Αυτοέλεγχος (self-control), διαχείριση χρόνου. Αυτοπαρατήρηση (self-observation), μέσω αυτοκαταγραφής, κεντρικές διαδικασίες της φάσης Performance.
Αξιολόγηση	Κουίζ κατανόησης Θεωρίας (διαμορφωτική αξιολόγηση) βαθμολογούμενο.
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα, χωρίς σύγχρονη παρουσία, καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Arts (Τέχνες): Οι φοιτητές μελετούν τεχνικές οπτικής εξαπάτησης και γραφιστικά κόλπα phishing, σχεδιάζοντας το δικό τους mockup λογότυπου και μακέτας στο Canva.

○ Δραστηριότητα 12: Θεωρητική Επίδειξη (Βίντεο Θεωρίας)



Εικόνα 32: Θεωρητική Επίδειξη (Arts)

Περιγραφή: Σε αυτή τη δραστηριότητα, η ψηφιακή οδηγός Σοφία παρουσιάζει στους φοιτητές τη θεωρία της οπτικής εξαπάτησης σε επιθέσεις phishing, εξηγώντας πώς οι επιτιθέμενοι αντιγράφουν λογότυπα γνήσιων ιστοσελίδων για να πείσουν οπτικά το θύμα και πώς το χρώμα και η κατανομή του μέσα σε ένα λογότυπο λειτουργούν ως μοναδικό αναγνωριστικό αποτύπωμα (Panda et al., 2022). Έπειτα η ψηφιακή βοηθός εξηγεί ποιοι είναι οι τρεις βαθμοί οπτικής ομοιότητας μιας ψεύτικης ιστοσελίδας με τη γνήσια (J.-L. Chen et al., 2020), και ποια σχεδιαστικά τεχνάσματα (Dark Patterns) χρησιμοποιούνται ώστε η ίδια η διεπαφή να παραπλανά τον χρήστη (Geronimo et al., 2020; Gray et al., 2018). Με την ολοκλήρωση του βίντεο¹³ οι φοιτητές αποκτούν το απαραίτητο θεωρητικό υπόβαθρο που θα χρειαστούν στην επόμενη δραστηριότητα (Ατομική Μελέτη), όπου θα μελετήσουν τα βήματα σχεδιασμού ενός δολώματος πριν προχωρήσουν στην πρακτική εφαρμογή τους στο εργαλείο Canva (Canva, 2026). Σε αυτή τη δραστηριότητα αξιοποιείται η στρατηγική Concrete Examples (Rawson et al., 2015).

¹³ Η μουσική υπόκρουση που χρησιμοποιήθηκε στο βίντεο προέρχεται από την πλατφόρμα Pixabay (Pixabay, 2026), υπό την άδεια Pixabay Content License, η οποία επιτρέπει τη δωρεάν χρήση του περιεχομένου χωρίς υποχρέωση αναφοράς του δημιουργού.

Εκφώνηση σεναρίου:

« Σε επιθέσεις phishing, οι επιτιθέμενοι αντιγράφουν λογότυπο, θέμα και χρώμα γνήσιων ιστοσελίδων, ώστε το θύμα να πιστέψει πως βρίσκεται στην αυθεντική σελίδα. Ακόμη κι αν αλλάξει η γραμματοσειρά ενός λογότυπου, ο συνδυασμός των χρωμάτων και η κατανομή τους παραμένουν παρόμοια, αυτό παραπλανά τον χρήστη. Η ανίχνευση βασίζεται σε εντοπισμό του λογότυπου, εξαγωγή χρωματικών χαρακτηριστικών και σύγκριση με βάση γνήσιων λογότυπων. Κάθε λογότυπο περιγράφεται μέσω της τιμής απόχρωσης (hue) των εικονοστοιχείων του και της θέσης του κέντρου βάρους κάθε απόχρωσης μέσα στην εικόνα. Η κατανομή του χρώματος γύρω από αυτό το κέντρο παραμένει σταθερή ανεξάρτητα από το μέγεθος, επιτρέποντας αναγνώριση του λογότυπου χωρίς μετατροπή διαστάσεων. Οι ψεύτικες ιστοσελίδες κατατάσσονται σε τρεις κατηγορίες ομοιότητας με τη γνήσια σελίδα: πολύ όμοιες, τοπικά όμοιες, και μη απομιμούμενες. Στις «πολύ όμοιες» συγκρίνεται ολόκληρο το στιγμιότυπο της σελίδας, ενώ στις «τοπικά όμοιες» εξετάζεται κυρίως το λογότυπο, μέσω τεχνικής αναγνωρίσιμης ανεξαρτήτως μεγέθους ή φωτισμού. Ορισμένες σελίδες phishing χρησιμοποιούν ολόκληρο στιγμιότυπο γνήσιας σελίδας ως φόντο, προσθέτοντας μόνο πεδία εισαγωγής στοιχείων, ώστε να αποφύγουν την ανίχνευση. Ως «Dark Patterns» ορίζονται διεπαφές σχεδιασμένες σκόπιμα ώστε να εξαπατούν τον χρήστη, αξιοποιώντας γνώσεις ψυχολογίας εις βάρος του. Πέντε βασικές κατηγορίες: ενόχληση (Nagging), παρεμπόδιση (Obstruction), απόκρυψη (Sneaking), παρέμβαση στη διεπαφή (Interface Interference) και εξαναγκασμός (Forced Action). Έρευνα σε 240 δημοφιλείς εφαρμογές κινητών βρήκε ότι το 95% περιείχε τουλάχιστον ένα τέτοιο τέχνασμα, με μέσο όρο 7,4 ανά εφαρμογή.»

○ Δραστηριότητα 12.1: Ατομική Μελέτη

Ατομική Μελέτη-Mission IV

Ενημερώνεται αυτόματα κάθε 5 λεπτά

MISSION IV · PERFORMANCE ARTS

Βήματα Σχεδιασμού ενός Ψηφιακού Δολώματος



ΨΗΦΙΑΚΗ ΟΔΗΓΟΣ · ΣΟΦΙΑ
Πριν σχεδιάσετε το δικό σας mockup οπτικού δολώματος στο Canva, ακολουθήστε τα 5 βήματα παρακάτω. Κάθε βήμα βασίζεται σε όσα μάθαμε στο θεωρητικό μέρος για το πώς σχεδιάζεται και πώς αναγνωρίζεται ένα πειστικό ψηφιακό δόλωμα.

ΒΗΜΑ 1 · Εμπνευση & Θεματική Επιλογή
Η ομάδα ξεκινά επιλέγοντας τη θεματική ή απειλή που θα αναπαραστήσει το δόλωμα, μέσα από συζήτηση γύρω από ένα πραγματικό ζήτημα κυβερνοασφάλειας, αντίστοιχα με τη διαδικασία όπου καλλιτέχνες, ακαδημαϊκοί και ειδικοί ασφάλειας συναντήθηκαν, μοιράστηκαν προβληματισμούς και σχημάτισαν ομάδες γύρω από κοινά θέματα.

ΒΗΜΑ 2 · Οπτική Αντιγραφή Χρώματος & Λογότυπου
Στο mockup επιλέγεται συνδυασμός χρωμάτων και η κατανομή τους μέσα στο σχέδιο, ώστε να θυμίζει ένα αναγνωρίσιμο λογότυπο. Ακόμη κι αν αλλάξει η γραμματόσειρά, ο συνδυασμός των χρωμάτων και η κατανομή τους μέσα στην εικόνα παραμένουν το βασικό στοιχείο που κάνει το σχέδιο αναγνωρίσιμο, και άρα πειστικό.

ΒΗΜΑ 3 · Επιλογή Βαθμού Ομοιότητας
Αποφασίζεται αν το δόλωμα θα είναι «πολύ όμοιο» με το πρωτότυπο, δηλαδή θα αντιγράφει ολόκληρη τη μακέτα ή σελίδα, ή «τοπικά όμοιο», όπου αντιγράφεται μόνο το λογότυπο μέσα σε νέο σχεδιασμό. Η επιλογή αυτή καθορίζει πόσο κοντά στο πρωτότυπο θα κινηθεί η ομάδα.

ΒΗΜΑ 4 · Ενσωμάτωση Τεχνικών Πειθούς
Προστίθεται στο σχέδιο ένα στοιχείο «Αισθητικής Παραποίησης» (π.χ. χρώμα ή γλώσσα που προκαλεί συναισθήματα ή αίσθημα επείγοντος) ή «Ψευδούς Ιεράρχησης» (μία επιλογή να φαίνεται οπτικά πιο σημαντική ή πιο αξιόπιστη από τις υπόλοιπες), ώστε το mockup να αναδεικνύει πώς λειτουργεί στην πράξη ένα πραγματικό σχεδιαστικό τέχνησμα.

ΒΗΜΑ 5 · Παρουσίαση & Αναστοχασμός

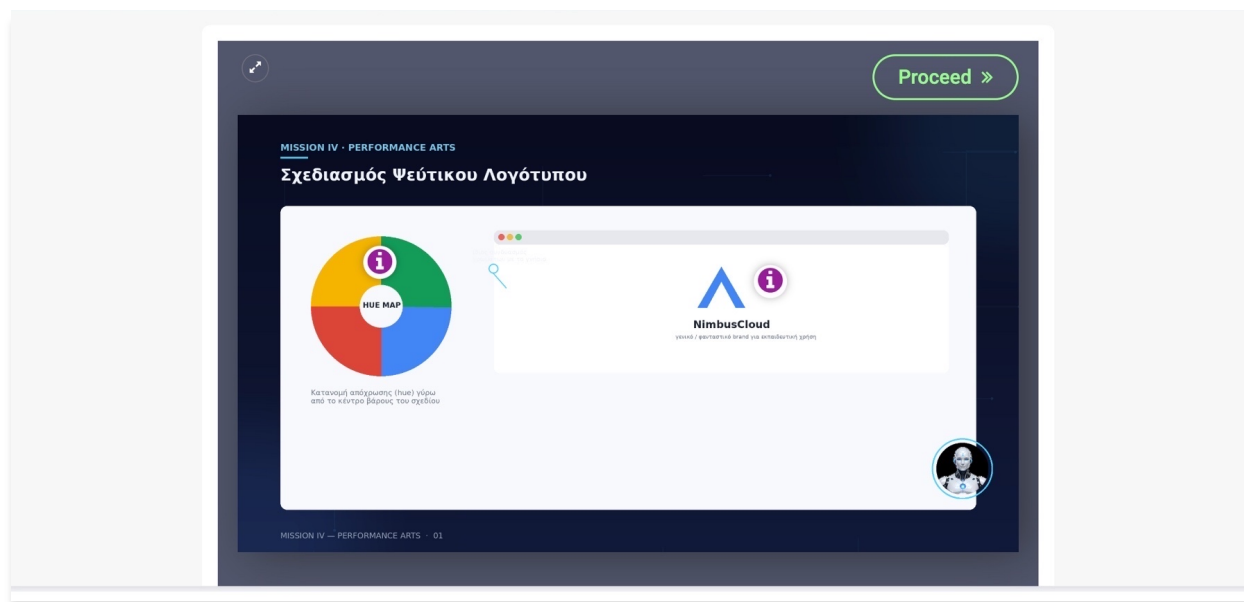
Εικόνα 33: Ατομική Μελέτη (Arts)

Περιγραφή: Η δραστηριότητα ξεκινά με σύντομη παρουσίαση, στην οποία η ψηφιακή οδηγός Σοφία καθοδηγεί τους φοιτητές μέσα από τα 5 βήματα σχεδιασμού ενός ψηφιακού δολώματος: επιλογή θεματικής και απειλής μέσα από συζήτηση γύρω από ένα πραγματικό ζήτημα κυβερνοασφάλειας, αντίστοιχα με τη διαδικασία δημιουργικής συνεργασίας καλλιτεχνών, ακαδημαϊκών και ειδικών ασφάλειας (Hall et al., 2022), οπτική αντιγραφή χρώματος και λογότυπου με βάση τον συνδυασμό και την κατανομή των χρωμάτων που κάνουν ένα σχέδιο αναγνωρίσιμο (Panda et al., 2022), επιλογή του βαθμού ομοιότητας του mockup με το πρωτότυπο, πολύ όμοιο ή τοπικά όμοιο (J.-L. Chen et al., 2020), ενσωμάτωση μιας τεχνικής πειθούς όπως η αισθητική παραποίηση ή η ψευδής ιεράρχηση (Geronimo et al., 2020; Gray et al., 2018). Με βάση αυτά τα βήματα, οι φοιτητές προχωρούν ατομικά στον πρακτικό σχεδιασμό του δικού τους mockup οπτικού δολώματος στο Canva που θα γίνει σε επόμενη δραστηριότητα. Στη δραστηριότητα αυτή αξιοποιείται η στρατηγική Scaffolding (Wood et al., 1976), οργανώνοντας μια σύνθετη δημιουργική εργασία σε 5 καθοδηγούμενα, διαδοχικά βήματα.

○ Δραστηριότητα 12.2: Διαχείριση Χρόνου

Περιγραφή: Οι φοιτητές χρησιμοποιούν το ψηφιακό εργαλείο Trello για να οργανώσουν τον χρόνο τους κατά τον σχεδιασμό του ψηφιακού δολώματος. Δημιουργούν πίνακα με καρτέλες για κάθε βήμα της ενότητας, όπως τη μελέτη της θεωρίας χρώματος και λογότυπου, την επιλογή του βαθμού οπτικής ομοιότητας του mockup με το πρωτότυπο, τον σχεδιασμό του λογοτύπου και της μακέτας στο Canva, και την προετοιμασία της τελικής παρουσίασης, ορίζοντας προθεσμίες για καθεμία. Η οπτική οργάνωση του Trello βοηθά τους φοιτητές να διαχειριστούν αποτελεσματικά τον ρυθμό εργασίας τους σε μια ενότητα με έντονο δημιουργικό και σχεδιαστικό χαρακτήρα, ενισχύοντας παράλληλα την αυτορρύθμιση και την υπευθυνότητα απέναντι στον προσωπικό τους χρόνο. Με τον τρόπο αυτό, οι φοιτητές εφαρμόζουν στην πράξη τη στρατηγική SRL της διαχείρισης χρόνου, αποκτώντας μια οπτική εικόνα της προόδου τους και μαθαίνοντας να θέτουν ρεαλιστικά χρονικά όρια για κάθε βήμα της μάθησής τους (Zimmerman, 2002).

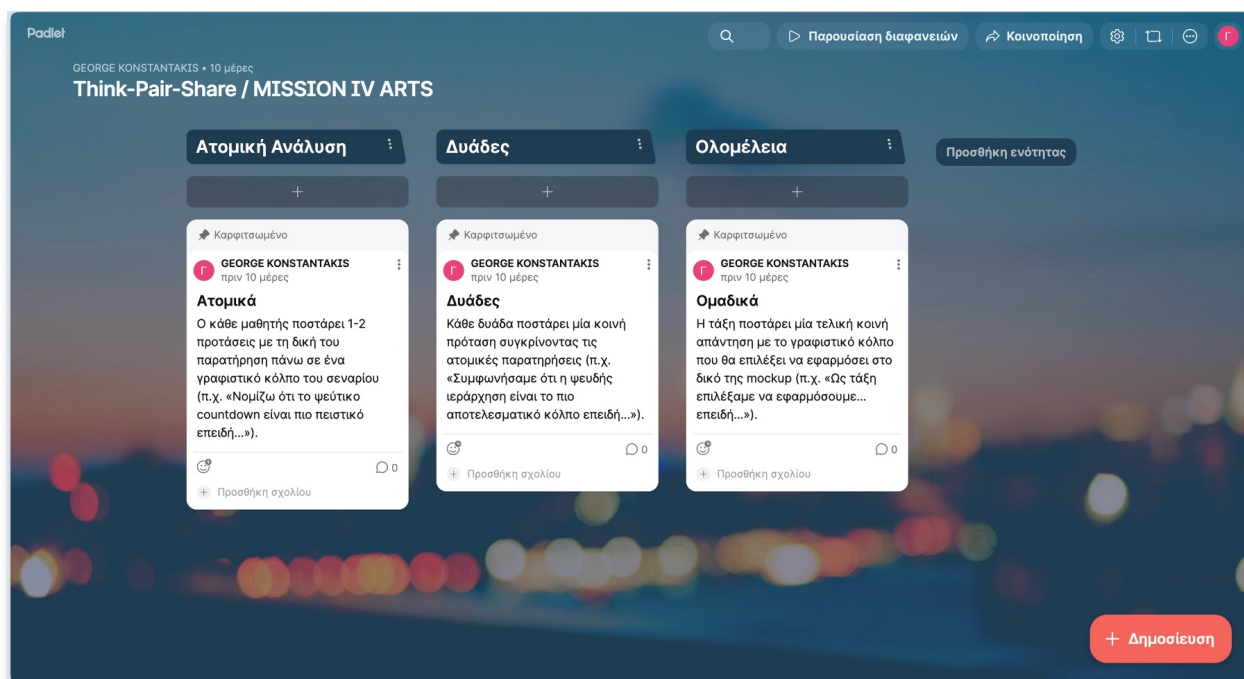
○ Δραστηριότητα 12.3: Σενάριο Οπτικής Εξαπάτησης (Case Study IV)



Εικόνα 34: Σενάριο Οπτικής Εξαπάτησης

Περιγραφή: Η δραστηριότητα υλοποιείται στο Lumi ως διαδραστικό σενάριο με hotspots, όπου η ψηφιακή οδηγός Σοφία καλωσορίζει τους φοιτητές και τους καθοδηγεί να εντοπίσουν τέσσερα γραφιστικά κόλπα που χρησιμοποιούνται σε επιθέσεις phishing. Οι φοιτητές πατούν πάνω σε hot spots τεσσάρων εικόνων για να ανακαλύψουν πώς ένα ψεύτικο λογότυπο αντιγράφει τον συνδυασμό χρωμάτων και την κατανομή απόχρωσης του γνήσιου (Panda et al., 2022), πώς η πίεση χρόνου, όπως αυτή που δημιουργεί ένα ψεύτικο αντίστροφο μέτρημα, μειώνει την ικανότητα αναγνώρισης phishing emails (Auton & Sturman, 2025), πώς ολόκληρη μια σελίδα μπορεί να είναι απλώς ακίνητη εικόνα με μόνο δύο πραγματικά λειτουργικά πεδία (J.-L. Chen et al., 2020). Έπειτα οι φοιτητές αναγνωρίζουν πώς η ψευδής ιεράρχηση κατευθύνει οπτικά τον χρήστη προς μία επιλογή μέσω μεγέθους και χρώματος (Gray et al., 2018). Στο τέλος του διαδραστικού αυτού σεναρίου, οι φοιτητές βλέπουν συνοπτική οθόνη με τα τέσσερα κόλπα που αναγνώρισαν, ενισχύοντας την ικανότητά τους να εντοπίζουν οπτική εξαπάτηση σε πραγματικές ψηφιακές απειλές. Ο συνδυασμός εικόνας και επεξηγηματικού κειμένου σε κάθε hotspot αξιοποιεί την αρχή του Dual Coding (Clark & Paivio, 1987).

○ Δραστηριότητα 12.4: Ανάλυση Σχεδιασμού



Εικόνα 35: Δραστηριότητα Ανάλυσης Σχεδιασμού (Think-Pair-Share)

Περιγραφή: Αρχικά, η ψηφιακή οδηγός Σοφία δίνει στους φοιτητές οδηγίες μέσα από έγγραφο στο εργαλείο Google Docs, περιγράφοντας τα τέσσερα στάδια της δραστηριότητας: ατομική εργασία, дуάδες, ολομέλεια, και σχεδιασμό στο Canva.

Στη συνέχεια, οι φοιτητές δουλεύουν στο Padlet σε τρεις στήλες σύμφωνα με τη λογική της στρατηγικής Think-Pair-Share (Sembert et al., 2021). Ατομικά, ο κάθε φοιτητής ποντάρει 1-2 προτάσεις με τη δική του παρατήρηση πάνω σε ένα γραφιστικό κόλπο του σεναρίου. Σε дуάδες, κάθε ζευγάρι συγκρίνει τις ατομικές παρατηρήσεις και ποστάρει μία κοινή πρόταση. Ομαδικά, η τάξη καταλήγει σε μία τελική κοινή απάντηση με το γραφιστικό κόλπο που θα επιλέξει να εφαρμόσει στο δικό της mockup, πριν περάσει στην πρακτική εφαρμογή στο εργαλείο Canva.

○ **Δραστηριότητα 12.5: Εργαστήριο σχεδιασμού (Design Lab)**

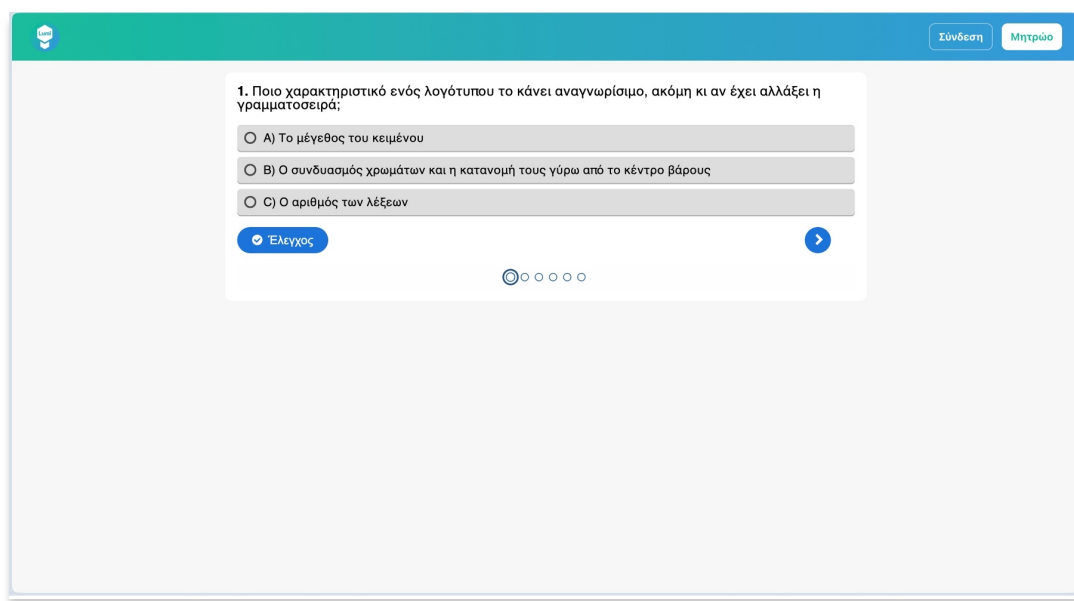
Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές σχεδιάζουν στο εργαλείο Canva το δικό τους mockup λογότυπου και μακέτας, εφαρμόζοντας συνειδητά ένα ή περισσότερα από τα γραφιστικά κόλπα που αναγνώρισαν στο σενάριο και συμφώνησαν στο Padlet. Με την ολοκλήρωση του σχεδιασμού, ανεβάζουν το τελικό γραφιστικό τους στο Google Classroom, ως αρχείο εικόνας ή σύνδεσμο Canva, ώστε να είναι έτοιμο για την επόμενη φάση της ετεροαξιολόγησης. Το τελικό γραφιστικό αξιολογείται με ρουμπρίκα με τα κριτήρια τεχνική ορθότητα και σαφήνεια παρουσίασης.

○ **Δραστηριότητα 12.6: Ετεροαξιολόγηση Γραφιστικών (Peer Assessment¹⁴)**

Περιγραφή: Στη δραστηριότητα αυτή, οι εκπαιδευόμενοι αξιολογούν ο ένας το γραφιστικό του άλλου μέσω του εργαλείου Google Form, αναγνωρίζοντας ποιο κόλπο χρησιμοποιήθηκε στο mockup του συμφοιτητή τους, βαθμολογώντας πόσο πειστικό είναι, και δίνοντας ανατροφοδότηση για το τι πέτυχε και τι θα μπορούσε να βελτιωθεί.

¹⁴ Η αναλυτική φόρμα της ετεροαξιολόγησης γραφιστικών παρατίθεται στο Παράρτημα.

○ Δραστηριότητα 12.7: Κουίζ κατανόησης Θεωρίας



1. Ποιο χαρακτηριστικό ενός λογότυπου το κάνει αναγνωρίσιμο, ακόμη κι αν έχει αλλάξει η γραμματοσειρά;

- ☐ A) Το μέγεθος του κειμένου
- ☐ B) Ο συνδυασμός χρωμάτων και η κατανομή τους γύρω από το κέντρο βάρους
- ☐ C) Ο αριθμός των λέξεων

☒ Έλεγχος ➔

© ○ ○ ○ ○ ○

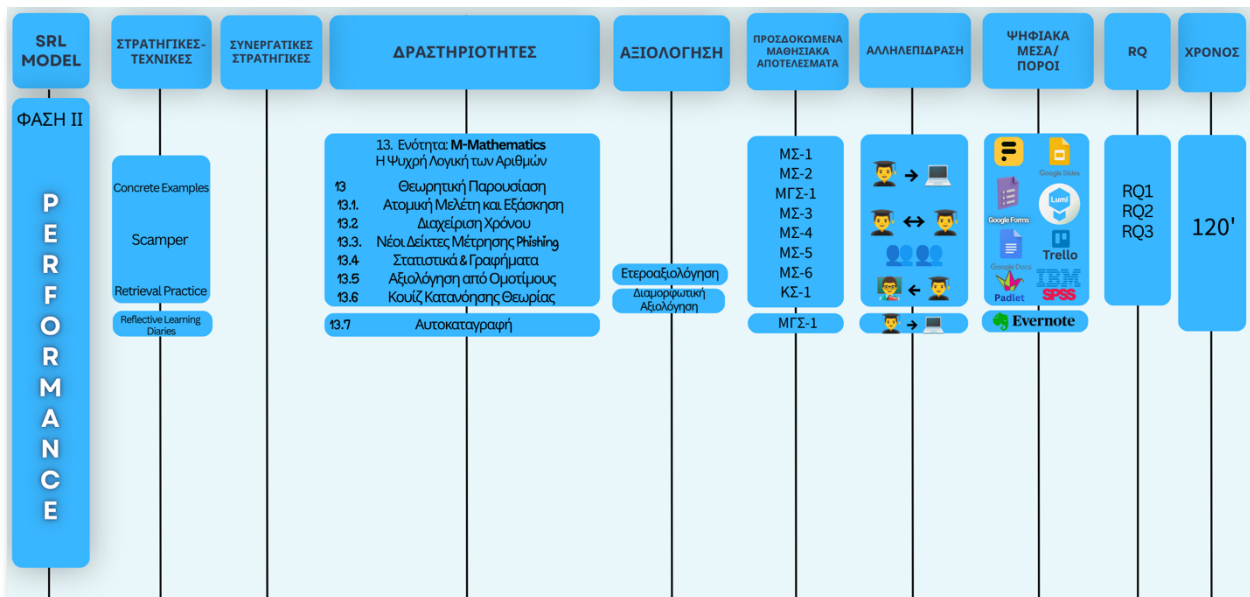
Εικόνα 36: Κουίζ Κατανόησης Θεωρίας (Arts)

Περιγραφή: Στη δραστηριότητα αυτή, οι εκπαιδευόμενοι απαντούν μέσω του εργαλείου Lumi σε έξι ερωτήσεις: τρεις πολλαπλής επιλογής και τρεις τύπου Σωστό/Λάθος, πάνω σε λογότυπο και χρώμα, κατηγορίες οπτικής ομοιότητας, ψευδή ιεράρχηση, συχνότητα σχεδιαστικών τεχνασμάτων και πίεση χρόνου. Κάθε ερώτηση συνοδεύεται από άμεση ανατροφοδότηση, τόσο για τη σωστή όσο και για τη λανθασμένη απάντηση, αξιοποιώντας τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006). Πηγές Κουίζ: (Auton & Sturman, 2025; J.-L. Chen et al., 2020; Geronimo et al., 2020; Gray et al., 2018; Panda et al., 2022).

○ Δραστηριότητα 12.8: Αυτοκαταγραφή

Περιγραφή: Ο κάθε φοιτητής μεταβαίνει στο εργαλείο Evernote και σημειώνει ποια σημεία της οπτικής εξαπάτησης νιώθει ότι έχει κατανοήσει καλά και ποια χρειάζονται περισσότερη εξάσκηση. Καταγράφει επίσης τυχόν δυσκολίες στο mockup που σχεδίασε στο Canva, ώστε να έχει πλήρη εικόνα πριν προχωρήσει στην επόμενη ενότητα. Η καταγραφή αυτών των δυσκολιών μέσω της τεχνικής Reflective Learning Diary (Chulan et al., 2025) βοηθάει τους εκπαιδευόμενους να σχεδιάσουν καλύτερα τα επόμενα βήματά τους, στο πλαίσιο της αυτοκαταγραφής (Zimmerman, 2002).

Φάση II Performance (Ενότητα Mathematics)



Σχήμα 10: Ροή δραστηριοτήτων Φάσης II (Performance), Ενότητα Mathematics

Πίνακας 15: Ανάλυση Ενότητας Mathematics (Φάση II Performance)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΣ-2, ΜΣ-3, ΜΣ-4, ΜΣ-5, ΜΣ-6, ΜΓΣ-1, ΚΣ-1.
Στρατηγικές & τεχνικές Μάθησης	Concrete Examples, SCAMPER, Retrieval Practice, Reflective Learning Diaries.
Συνεργατικές στρατηγικές	-
Στρατηγικές αυτορρύθμισης	Οργάνωση και μετατροπή πληροφορίας, επανάληψη και απομνημόνευση, διαχείριση χρόνου, καταγραφή αρχείων και αυτοκαταγραφή.
Θεωρητική σύνδεση	Αυτοέλεγχος (self-control), διαχείριση χρόνου, αυτοπαρατήρηση (self-observation), μέσω αυτοκαταγραφής, κεντρικές διαδικασίες της φάσης Performance.
Αξιολόγηση	Κουίζ Κατανόησης Θεωρίας (διαμορφωτική αξιολόγηση) βαθμολογούμενο, Ετεροαξιολόγηση γραφημάτων.
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα, χωρίς σύγχρονη παρουσία, καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Mathematics (Μαθηματικά). Οι φοιτητές υπολογίζουν και ερμηνεύουν στατιστικούς δείκτες μιας επίθεσης phishing, όπως το Ποσοστό Κλικ και το Ποσοστό Επιτυχίας, και σχεδιάζουν γραφήματα για την παρουσίασή τους.

○ Δραστηριότητα 13: Θεωρητική Παρουσίαση μέσω Διαφανειών

Πώς Υπολογίζουμε το Ποσοστό Επιτυχίας

Πόσοι «έπεσαν στην παγίδα», όχι απλώς πόσοι έκαναν κλικ

Ποσοστό Επιτυχίας (%) = (Θύματα που Έδωσαν Στοιχεία ÷ Αριθμός Κλικ) × 100

ΕΝΔΕΙΚΤΙΚΟ ΠΑΡΑΔΕΙΓΜΑ

Από τα 40 άτομα που έκαναν κλικ (προηγούμενο παράδειγμα), τα 15 έδωσαν πραγματικά τον κωδικό τους.

Υπολογισμός: $(15 \div 40) \times 100$

37,5%

Ποσοστό Επιτυχίας

Προσοχή στη διαφορά: το Ποσοστό Κλικ δείχνει το ενδιαφέρον ενώ το Ποσοστό Επιτυχίας δείχνει το πραγματικό θύμα.

Εικόνα 37: Θεωρητική Παρουσίαση (Mathematics)

Περιγραφή: Η ενότητα ξεκινά με μια παρουσίαση στο Google Slides, όπου η ψηφιακή βοηθός Sofia καλωσορίζει τους φοιτητές στην ενότητα Mathematics και τους ενημερώνει για όσα πρόκειται να μάθουν. Η παρουσίαση ξεκινά από τους βασικούς στατιστικούς όρους (δείγμα, ποσοστό, ποσοστό κλικ, ποσοστό επιτυχίας) και δείχνει, μέσα από απλά αριθμητικά παραδείγματα, πώς υπολογίζεται καθένας από αυτούς τους δείκτες και ποια είναι η διαφορά ανάμεσα σε έναν χρήστη που απλώς πάτησε έναν ύποπτο σύνδεσμο και σε έναν χρήστη που τελικά έδωσε τα προσωπικά του στοιχεία. Στη συνέχεια παρουσιάζονται τρεις βασικοί τύποι γραφήματος: ραβδόγραμμα, γράφημα τάσης και κυκλικό διάγραμμα, με ενδεικτικά παραδείγματα που δείχνουν πότε χρησιμοποιείται το καθένα (Gavett et al., 2017; Iuga et al., 2016; Jampen et al., 2020). Η ενότητα κλείνει με έναν πρακτικό οδηγό πέντε βημάτων για τη σωστή ανάγνωση ενός γραφήματος (τίτλος, άξονες, υπόμνημα, τάση, συμπέρασμα), ώστε οι φοιτητές να μάθουν όχι μόνο να υπολογίζουν, αλλά και να ερμηνεύουν σωστά και με συνέπεια ένα γράφημα. Σε αυτή τη δραστηριότητα αξιοποιείται η στρατηγική Concrete Examples (Rawson et al., 2015).

ο Δραστηριότητα 13.1: Ατομική Μελέτη & Εξάσκηση

Περιγραφή: Η ενότητα ξεκινά με ένα έγγραφο (Google Doc), όπου ο κάθε εκπαιδευόμενος εφαρμόζει μόνος του όσα άκουσε στη θεωρητική παρουσίαση. Το έγγραφο ξεκινά με μια πολύ σύντομη υπενθύμιση των βασικών εννοιών (ποσοστό κλικ, ποσοστό επιτυχίας, τύποι γραφήματος) και προχωρά σε μια άσκηση υπολογισμού με φανταστικά δεδομένα: ο φοιτητής υπολογίζει το ποσοστό κλικ και το ποσοστό επιτυχίας για τέσσερα τμήματα ενός πανεπιστημίου, εφαρμόζοντας τους τύπους της θεωρίας. Η δραστηριότητα κλείνει με τέσσερις εικόνες γραφημάτων (ραβδόγραμμα, γράφημα τάσης, κυκλικό διάγραμμα, πίνακας αριθμών) και μια σύντομη ερώτηση αναστοχασμού: «Ποιο γράφημα θα ταίριαζε καλύτερα για την παρουσίαση των αποτελεσμάτων;». Στη συνέχεια, το ίδιο έγγραφο εισάγει μια σύντομη θεωρητική επισκόπηση της κρυπτογραφίας, τον τύπο $n = p \times q$ και ένα ενδεικτικό παράδειγμα με μικρούς πρώτους αριθμούς ($p = 3, q = 11$). Ο φοιτητής καλείται στη συνέχεια να κάνει το αντίστροφο, να βρει τους δύο πρώτους αριθμούς που παράγουν το $n = 221$, δοκιμάζοντας διαδοχικά πρώτους αριθμούς μέχρι να εντοπίσει τον σωστό. Έπειτα παρέχεται μια ερώτηση αναστοχασμού που συνδέει τον αριθμό των δοκιμών σε αυτό το μικρό παράδειγμα με το γιατί ένα πραγματικό κλειδί RSA παραμένει πρακτικά αδύνατο να σπάσει μόνο με δοκιμές. Ακολουθούν τρεις ερωτήσεις αξιολόγησης σχετικά με την ερμηνεία των ποσοστών ως δεικτών κινδύνου, τις οποίες ο φοιτητής απαντά σε σύντομο κείμενο και αναρτά στο Google Classroom μέσω του υπερσυνδέσμου που παρέχεται. Στο τέλος της δραστηριότητας αυτής, οι φοιτητές καλούνται να συμπληρώσουν ένα Checklist¹⁵ που δημιουργήθηκε στο εργαλείο Fillout, σχεδιασμένο ώστε να ενισχύει την ικανότητα των φοιτητών να παρακολουθούν οι ίδιοι την πρόοδό τους σε online μάθημα (Cavanaugh et al., 2012), προκειμένου να επιβεβαιώσουν ότι ολοκλήρωσαν όλα τα απαιτούμενα βήματα.

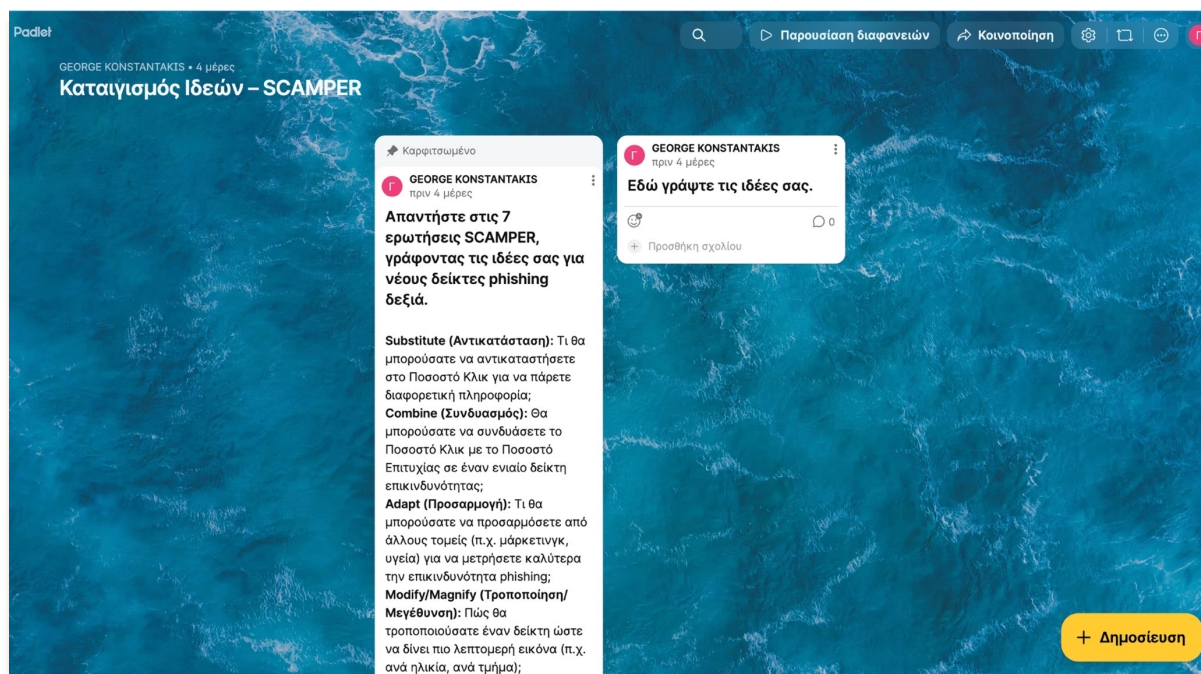
Πηγές Θεωρίας: (Gavett et al., 2017; Iuga et al., 2016; Jampen et al., 2020; Meelu & Malik, 2010).

¹⁵ Η αναλυτική παρουσίαση του Checklist παρατίθεται στο Παράρτημα.

○ Δραστηριότητα 13.2: Διαχείριση Χρόνου

Περιγραφή: Στη δραστηριότητα αυτή, οι εκπαιδευόμενοι χρησιμοποιούν το ψηφιακό εργαλείο Trello για να οργανώσουν τον χρόνο τους κατά την επεξεργασία των μετρικών και τη δημιουργία γραφημάτων. Δημιουργούν πίνακα με καρτέλες για κάθε βήμα της ενότητας, όπως τη μελέτη των βασικών όρων (ποσοστό κλικ, ποσοστό επιτυχίας), την εκτέλεση των αριθμητικών υπολογισμών στην ατομική άσκηση, την επιλογή κατάλληλου τύπου γραφήματος για τα δεδομένα, και την προετοιμασία της τελικής παρουσίασης στατιστικής ανάλυσης, ορίζοντας προθεσμίες για καθεμία. Η οπτική οργάνωση του Trello βοηθά τους φοιτητές να διαχειριστούν αποτελεσματικά τον ρυθμό εργασίας τους σε μια ενότητα με έντονο αναλυτικό και υπολογιστικό χαρακτήρα. Με τον τρόπο αυτό, οι φοιτητές εφαρμόζουν στην πράξη τη στρατηγική SRL της διαχείρισης χρόνου, αποκτώντας μια οπτική εικόνα της προόδου τους και μαθαίνοντας να θέτουν ρεαλιστικά χρονικά όρια για κάθε βήμα της μάθησής τους (Zimmerman, 2002).

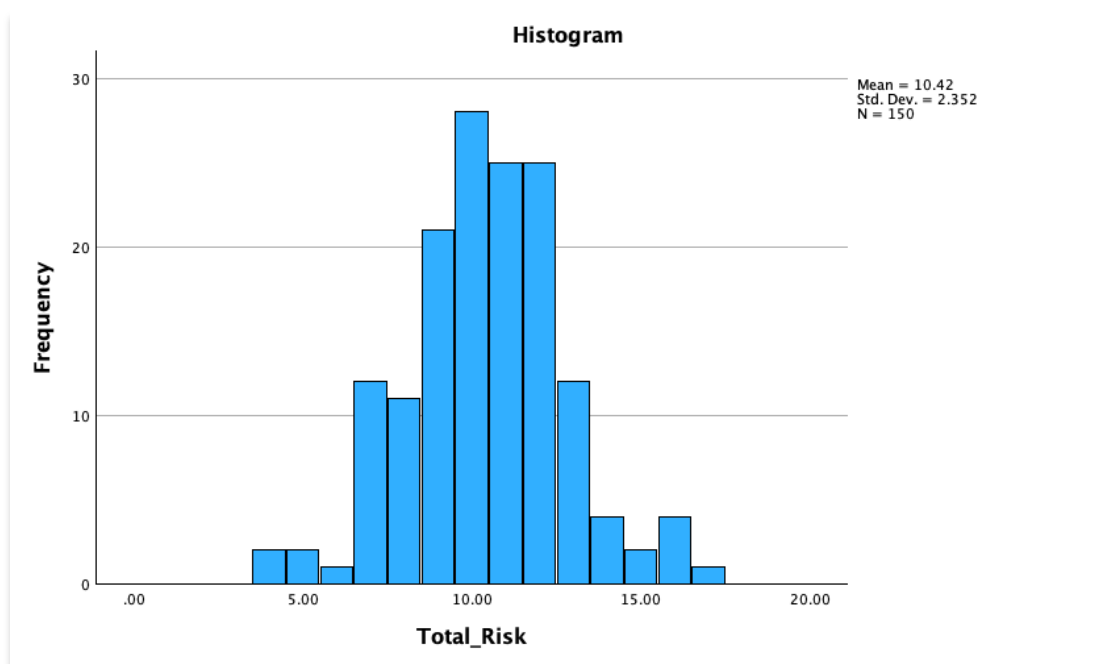
○ Δραστηριότητα 13.3: Ιδεοθύελλα Νέων Δεικτών



Εικόνα 38: Ιδεοθύελλα νέων δεικτών (Τεχνική SCAMPER)

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές εργάζονται ομαδικά στο Padlet, σκεπτόμενοι νέους πιθανούς δείκτες μέτρησης μιας επίθεσης phishing, πέρα από το Ποσοστό Κλικ και το Ποσοστό Επιτυχίας που ήδη γνώρισαν. Η δραστηριότητα αξιοποιεί την τεχνική SCAMPER (Serrat, 2017), μια δομημένη μέθοδο ιδεοθύελλας που καθοδηγεί τη σκέψη μέσα από επτά ερωτήσεις, εξετάζοντας πώς κάτι ήδη υπάρχον θα μπορούσε να αντικατασταθεί, να συνδυαστεί, να προσαρμοστεί, να τροποποιηθεί, να αξιοποιηθεί διαφορετικά, να αφαιρεθεί ή να αντιστραφεί. Οι επτά ερωτήσεις τοποθετούνται στην αριστερή στήλη του Padlet, ενώ οι φοιτητές καταγράφουν τις ιδέες τους στη δεξιά στήλη, μοιράζονται τις σκέψεις τους με τους συμμαθητές τους και σχολιάζουν τις προτάσεις τους. Μέσα από αυτή τη διαδικασία, οι φοιτητές εξασκούνται στην παραγωγή πρωτότυπων ιδεών, ενώ παράλληλα κατανοούν τη διαφορετική οπτική των συνεργατών τους πάνω στο ίδιο πρόβλημα.

○ Δραστηριότητα 13.4: Στατιστικά & Γραφήματα



Εικόνα 39: Ιστόγραμμα Total_Risk (SPSS)

Περιγραφή: Αρχικά, οι φοιτητές διαβάζουν τις οδηγίες μέσα από το αρχείο Google Docs, ανοίγουν το αρχείο δεδομένων (.sav) στο πρόγραμμα SPSS (IBM, 2026), και ελέγχουν την εσωτερική αξιοπιστία των τριών κλιμάκων του ερωτηματολογίου (γνώση, επικίνδυνο κλικ, παροχή στοιχείων) μέσω του δείκτη Cronbach's (Gialamas, 2024), καθώς και τη συσχέτιση ανάμεσά τους. Στη συνέχεια, ολοκληρώνουν τη δραστηριότητα παράγοντας ένα ιστόγραμμα, ένα γράφημα πίτας και ένα συγκριτικό γράφημα. Τέλος, ανεβάζουν την εργασία τους στο Google Classroom. Μέσα από τη δραστηριότητα αυτή, οι φοιτητές εξοικειώνονται με βασικές τεχνικές στατιστικής ανάλυσης και αναπτύσσουν την ικανότητα να εξάγουν τεκμηριωμένα συμπεράσματα για τη σχέση ανάμεσα στη γνώση περί phishing και την επικίνδυνη διαδικτυακή συμπεριφορά.

ο Δραστηριότητα 13.5: Ετεροαξιολόγηση ¹⁶

Περιγραφή: Οι φοιτητές αξιολογούν τα γραφήματα ενός συνεκπαιδευμένου τους μέσω του εργαλείου Google Forms. Αρχικά καταγράφουν το όνομα του συνεκπαιδευόμενου που αξιολογούν. Στη συνέχεια, για καθένα από τα τρία γραφήματα (ιστόγραμμα ηλικίας, γράφημα πίτας φύλου, συγκριτικό γράφημα), απαντούν σε 3 ερωτήσεις κλίμακας Likert (1-5), οι οποίες αντιστοιχούν στην τεχνική ορθότητα, τη σαφήνεια παρουσίασης και την καταλληλότητα του τύπου γραφήματος για το είδος των δεδομένων.

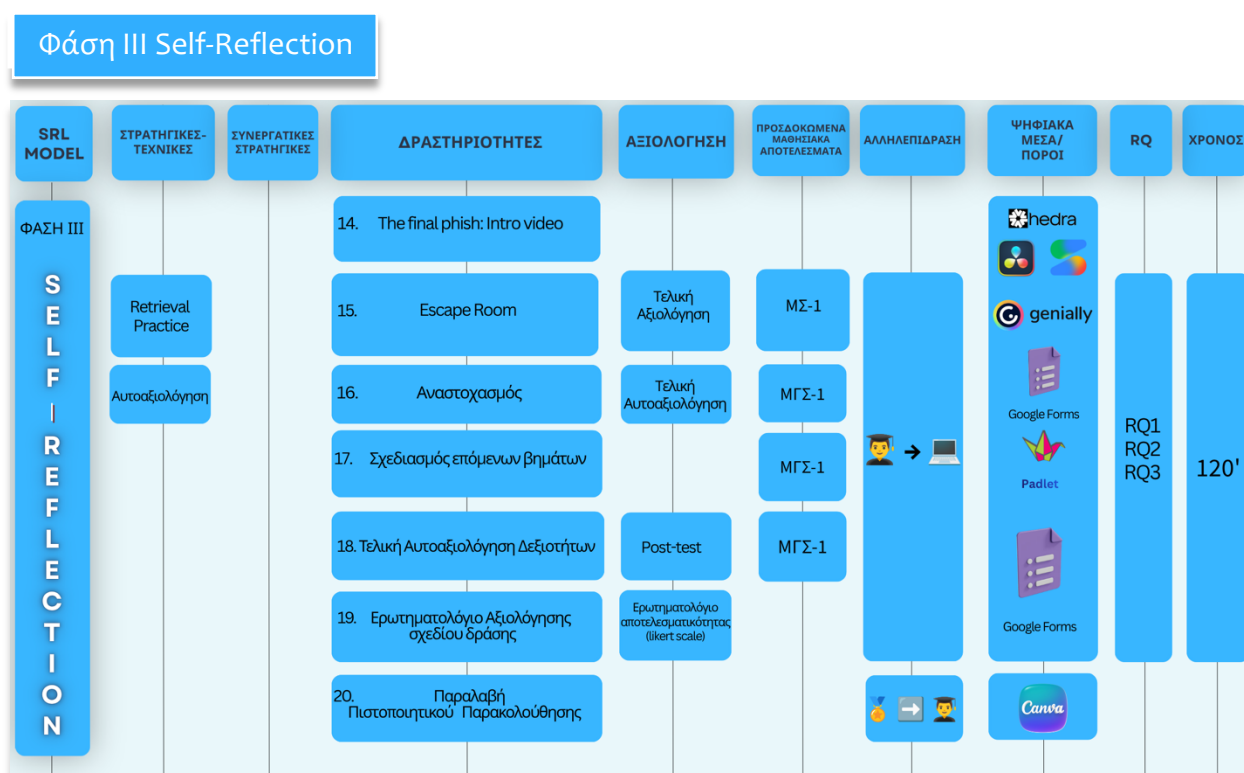
ο Δραστηριότητα 13.6: Κουίζ Κατανόησης Θεωρίας

Περιγραφή: Οι φοιτητές απαντούν ατομικά σε ένα κουίζ στο εργαλείο Lumi που αποτελείται από έξι ερωτήσεις πολλαπλής επιλογής και τρεις ερωτήσεις σωστό/λάθος, βασισμένο στη θεωρία που διδάχτηκαν (ποσοστό κλικ, ποσοστό επιτυχίας, τύποι γραφήματος, ανάγνωση γραφήματος, Cronbach's alpha, συσχέτιση μεταβλητών). Σε κάθε απάντηση, σωστή ή λάθος, υπάρχει άμεση ανατροφοδότηση. Η δραστηριότητα αυτή εντάσσεται στην ενδιάμεση αξιολόγηση και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

¹⁶ Η αναλυτική φόρμα ετεροαξιολόγησης γραφημάτων διατίθεται στο Παράρτημα.

○ Δραστηριότητα 13.7: Αυτοκαταγραφή

Περιγραφή: Ο κάθε φοιτητής μεταβαίνει στο εργαλείο Evernote και σημειώνει ποιους στατιστικούς δείκτες του SPSS νιώθει ότι έχει κατανοήσει καλά και ποιους χρειάζεται να ξαναδεί. Τέλος, καταγράφει τυχόν δυσκολίες που συνάντησε κατά τη χρήση του προγράμματος, ώστε να έχει πλήρη εικόνα πριν κλείσει την ενότητα Mathematics. Η καταγραφή αυτών των δυσκολιών μέσω της τεχνικής Reflective Learning Diary (Chulan et al., 2025) βοηθάει τους εκπαιδευόμενους να σχεδιάσουν καλύτερα τα επόμενα βήματά τους, στο πλαίσιο της αυτοκαταγραφής (Zimmerman, 2002).

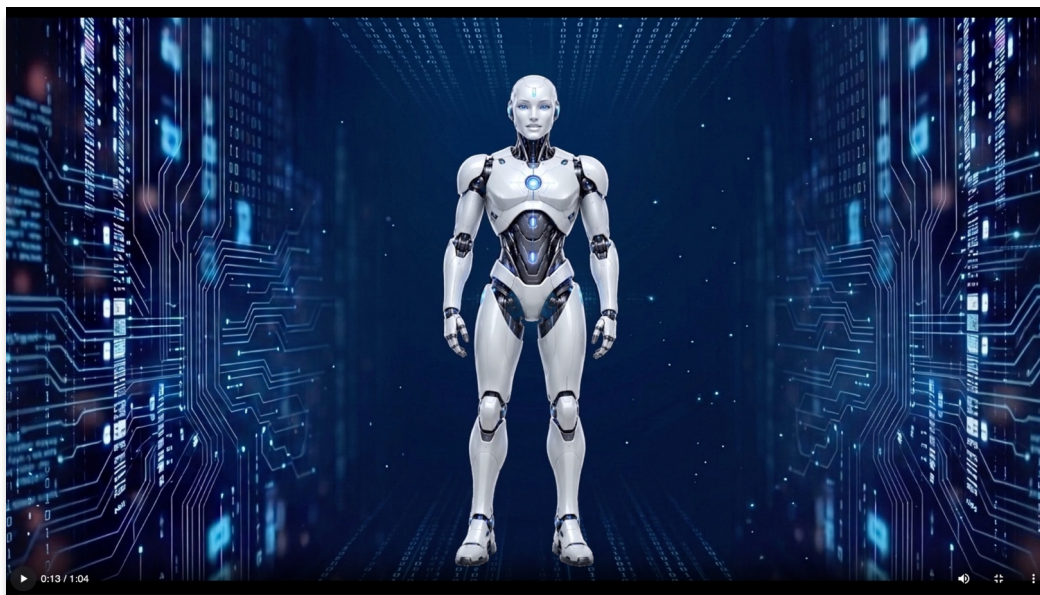


Σχήμα 11: Ροή δραστηριοτήτων Φάσης III (Self-Reflection)

Πίνακας 16: Ανάλυση Φάσης III (Self-Reflection)

Εκπαιδευτικοί στόχοι	ΜΣ-1, ΜΓΣ-1
Στρατηγικές & τεχνικές Μάθησης	Retrieval Practice.
Συνεργατικές στρατηγικές	Καμία.
Στρατηγικές αυτορρύθμισης	Τοποθέτηση Στόχων και Σχεδιασμός.
Θεωρητική σύνδεση	Στο Ερωτηματολόγιο Αναστοχασμού, οι φοιτητές εφαρμόζουν τα δύο θεωρητικά συστατικά της φάσης Self-Reflection: πρώτα την αυτοκρίση, αξιολογώντας την τελική τους επίδοση και αναζητώντας τους λόγους στους οποίους αποδίδουν το αποτέλεσμα τους, και έπειτα την αυτοαντίδραση, εκφράζοντας την ικανοποίησή τους από την πορεία που ακολούθησαν και σκεπτόμενοι πώς θα προσάρμοζαν τις στρατηγικές τους στο μέλλον.
Αξιολόγηση	Τελική αξιολόγηση-Genially Escape Room (βαθμολογούμενη). Skills Self Check Post (Μη βαθμολογούμενη).
Μέθοδος μάθησης	Ασύγχρονη.
Ρόλος εκπαιδευτικού/AI	Εποπτικός ρόλος διδάσκοντα, χωρίς σύγχρονη παρουσία, καθοδήγηση μέσω AI (Σοφία).
Σύνδεση με STEAM	Δεν αφορά συγκεκριμένη ενότητα STEAM. Η φάση Self-Reflection συνοψίζει και τις πέντε ενότητες: Science, Technology, Engineering, Arts, Mathematics, μέσω Escape Room στο εργαλείο Genially.

○ Δραστηριότητα 14: Εισαγωγικό Βίντεο Self-Reflection



Εικόνα 40: Εισαγωγικό Βίντεο (Self-Reflection)

Περιγραφή: Οι φοιτητές παρακολουθούν ένα σύντομο βίντεο¹⁷, όπου ο AI οδηγός Σοφία τους καλωσορίζει στη φάση Self-Reflection, ανακεφαλαιώνει όσα έμαθαν στις πέντε ενότητες STEAM, και παρουσιάζει τα επόμενα βήματα escape room, αναστοχασμός, τελικός έλεγχος δεξιοτήτων, αξιολόγηση του e-course και παραλαβή πιστοποιητικού.

Εκφώνηση Σεναρίου:

«Ταξίδεψες μέσα από πέντε διαφορετικούς κόσμους. Στην Επιστήμη, κατάλαβες πώς η ανθρώπινη ψυχολογία γίνεται όπλο στα χέρια ενός επιτιθέμενου. Στην Τεχνολογία, έμαθες να διαβάζεις ένα URL σαν ντετέκτιβ. Στη Μηχανική, μπήκες στο μυαλό του επιτιθέμενου και είδες πώς χτίζεται μια επίθεση βήμα βήμα. Στις Τέχνες, ανακάλυψες πώς ένα απλό λογότυπο μπορεί να κρύβει παραπλάνηση. Και στα Μαθηματικά, έμαθες να διαβάζεις τους αριθμούς πίσω από κάθε εκστρατεία phishing. Πέντε αποστολές, μία γνώση. Σε αυτή την ενότητα, θα δοκιμάσεις πρώτα ό,τι έμαθες σε ένα διαδραστικό escape room στο Genially. Μετά θα αναστοχαστείς πάνω στη διαδρομή σου, θα ξαναδείς τις δεξιότητές σου μέσα από έναν τελικό έλεγχο, και θα αξιολογήσεις το ίδιο το e-course. Στο τέλος, θα παραλάβεις το πιστοποιητικό σου. Είστε έτοιμοι για το ταξίδι που έρχεται;»

¹⁷ Χρησιμοποιήθηκαν τα εργαλεία Hedra AI (Hedra, 2026) για τη δημιουργία του avatar της ψηφιακής βοηθού «Σοφία», και Google AI Studio (Google, 2026a) για τη μετατροπή κειμένου σε ομιλία (text-to-speech) του σεναρίου που παρατίθεται ανωτέρω, στο εισαγωγικό βίντεο. Η μουσική υπόκρουση προέρχεται από το Pixabay (Pixabay, 2026), υπό την άδεια Pixabay Content License, η οποία επιτρέπει δωρεάν χρήση χωρίς υποχρέωση αναφοράς του δημιουργού. Η χρήση τους είχε υποστηρικτικό χαρακτήρα, και το παραγόμενο περιεχόμενο ελέγχθηκε από τον συγγραφέα πριν ενσωματωθεί στο βίντεο.

○ Δραστηριότητα 15: Escape Room (Genially)



Εικόνα 41: Escape Room (Genially)

Περιγραφή: Οι φοιτητές συμμετέχουν σε ένα διαδραστικό escape room στο Genially (Genially, 2026), ακολουθώντας τη Sofia σε μια σειρά αποστολών σχετικών με την αναγνώριση και την αντιμετώπιση επιθέσεων phishing. Αρχικά, μέσα από δραστηριότητα drag-and-drop, ανασυνθέτουν τον ορισμό του phishing ως τεχνικής κοινωνικής μηχανικής. Έπειτα, εξετάζουν τη χρήση της αυθεντίας ως αρχής πειθούς και αναγνωρίζουν ποια στοιχεία ανήκουν στην τεχνική υποδομή μιας επίθεσης. Στη συνέχεια, απαντούν σε ερωτήσεις σχετικά με τη δημιουργία και τον βασικό στόχο ενός phishing email. Σε επόμενη αποστολή συγκρίνουν αυθεντικά και παραποιημένα λογότυπα, ώστε να εντοπίσουν οπτικές ενδείξεις εξαπάτησης. Έπειτα οργανώνουν στη σωστή σειρά τα βήματα παρουσίασης και σύγκρισης των ποσοστών κλικ εργαζομένων από διαφορετικά τμήματα μιας εταιρείας, επιλέγοντας το κατάλληλο γράφημα. Στο τέλος καλούνται να αποφασίσουν αν η Sofia θα επιλέξει την ασφαλή αντίδραση ή θα αγνοήσει τον κίνδυνο, οδηγώντας την ιστορία σε διαφορετική κατάληξη ανάλογα με την επιλογή τους (Alabdan, 2020; Auton & Sturman, 2025; J.-L. Chen et al., 2020; Ferreira & Teles, 2019; Gavett et al., 2017; Geronimo et al., 2020; Gray et al., 2018; Jampen et al., 2020; Luse & Burkman, 2021; Montañez et al., 2020; Morić et al., 2025; Panda et al., 2022; Sahingoz et al., 2019). Η δραστηριότητα αυτή εντάσσεται στην τελική αξιολόγηση και αξιοποιεί τη στρατηγική Retrieval Practice (Roediger & Karpicke, 2006).

○ Δραστηριότητα 16: Ερωτηματολόγιο Αναστοχασμού

Ερωτηματολόγιο Αναστοχασμού
Αναστοχάσου πάνω στην πορεία και τις επιλογές σου

sipstudiogk@gmail.com [Εναλλαγή λογαριασμού](#)

Δεν κοινοποιήθηκε

Αξιολογώ την τελική μου επίδοση με βάση τα δικά μου κριτήρια επιτυχίας.

1 2 3 4 5

Διαφωνώ απόλυτα ☐ ☐ ☐ ☐ ☐ Συμφωνώ απόλυτα

Μπορώ να εξηγήσω σε τι οφείλεται το αποτέλεσμα που πέτυχα, είτε θετικό είτε αρνητικό.

1 2 3 4 5

Διαφωνώ απόλυτα ☐ ☐ ☐ ☐ ☐ Συμφωνώ απόλυτα

Αισθάνομαι ικανοποιημένος ή ικανοποιημένη με την πορεία που ακολούθησα.

1 2 3 4 5

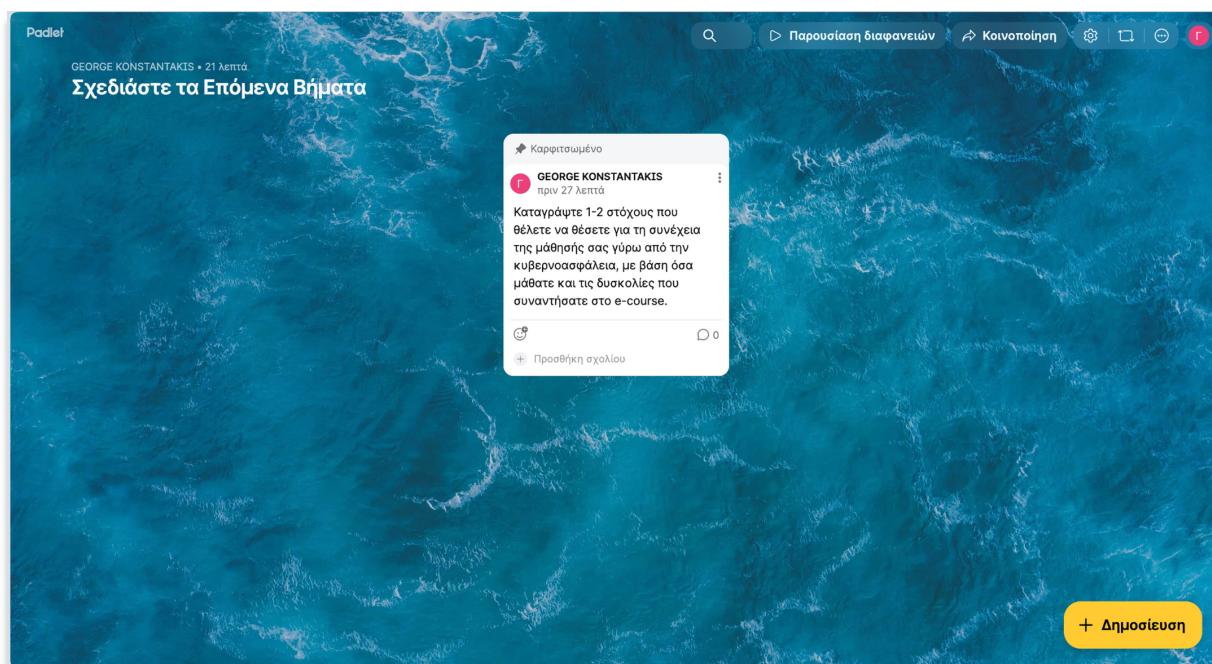
Διαφωνώ απόλυτα ☐ ☐ ☐ ☐ ☐ Συμφωνώ απόλυτα

Εικόνα 42: Ερωτηματολόγιο Αναστοχασμού

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές συμπληρώνουν στο Google Forms ένα σύντομο ερωτηματολόγιο¹⁸ αναστοχασμού, με τέσσερις δηλώσεις τύπου Likert (κλίμακα 1-5), οι οποίες αντιστοιχούν στα δύο θεωρητικά συστατικά της φάσης αναστοχασμού του Zimmerman: την αυτοκρίση, μέσω της αυτοαξιολόγησης της τελικής επίδοσης και της αναζήτησης αιτιωδών αποδόσεων για το αποτέλεσμα, και την αυτοαντίδραση, μέσω της αυτοικανοποίησης από την πορεία που ακολουθήθηκε και της αναπροσαρμογής στρατηγικών για μελλοντική χρήση. Το ερωτηματολόγιο κλείνει με ανοιχτό πεδίο σχολιασμού.

¹⁸ Το πλήρες ερωτηματολόγιο Αναστοχασμού παρατίθεται στο Παράρτημα.

○ Δραστηριότητα 17: Σχεδιασμός επόμενων Βημάτων



Εικόνα 43: Σχεδιασμός Επόμενων Βημάτων

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές καταγράφουν στο εργαλείο Padlet ένα έως δύο στόχους για τη συνέχεια της μάθησής τους γύρω από την κυβερνοασφάλεια, με βάση όσα έμαθαν και τις δυσκολίες που συνάντησαν στο e-course.

○ Δραστηριότητα 18: Skills Self-Check (Post)

Περιγραφή: Στη δραστηριότητα «Skills Self-Check (Post)», στη φάση Self-Reflection, οι φοιτητές συμπληρώνουν εκ νέου το ίδιο ερωτηματολόγιο¹⁹ των 12 δηλώσεων Likert που είχαν συμπληρώσει ως «Skills Self-Check (Pre)» στη φάση Forethought, στην αρχή του e-course. Η επανάληψη της ίδιας φόρμας καθιστά δυνατή τη σύγκριση των αρχικών και τελικών βαθμολογιών ανά δείκτη, αποτυπώνοντας την εξέλιξη των φοιτητών στη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση και την κατανόηση της οπτικής των άλλων μέσα από τη συμμετοχή τους στο e-course.

¹⁹ Το ερωτηματολόγιο Skills Self-Check (Post) είναι πανομοιότυπο με το αντίστοιχο Pre-test που παρατίθεται στο Παράρτημα, και δεν παρατίθεται εκ νέου.

○ Δραστηριότητα 19: Ερωτηματολόγιο Αξιολόγησης Σχεδίου Δράσης

Αξιολόγηση Εκπαιδευτικού Σχεδίου Δράσης

Παρακαλούμε αξιολογήστε την υλοποίηση του εκπαιδευτικού σχεδίου δράσης. Η απάντησή σας είναι σημαντική για τη βελτίωση μελλοντικών παρεμβάσεων.

sipstudlogk@gmail.com [Εναλλαγή λογαριασμού](#)

Δεν κοινοποιήθηκε

ΑΞΟΝΑΣ Α: ΠΕΡΙΕΧΟΜΕΝΟ

	Διαφωνώ απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ/ Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ απόλυτα (5)
Το γνωστικό αντικείμενο του σχεδίου δράσης ήταν συναφές με τους μαθησιακούς στόχους.	☐	☐	☐	☐	☐
Η σαφήνεια των παρουσιαζόμενων εννοιών διευκόλυνε την κατανόηση του γνωστικού αντικειμένου.	☐	☐	☐	☐	☐

Ο βαθμός

Εικόνα 44: Ερωτηματολόγιο Αξιολόγησης Σχεδίου Δράσης

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές συμπληρώνουν στο Google Forms ένα ερωτηματολόγιο²⁰ αξιολόγησης του εκπαιδευτικού σχεδίου δράσης, οργανωμένο σε τρεις άξονες με δηλώσεις τύπου Likert (κλίμακα 1-5): το Περιεχόμενο (συνάφεια με μαθησιακούς στόχους, σαφήνεια εννοιών, καταλληλότητα δυσκολίας, ερεθίσματα για περαιτέρω διερεύνηση, γνωστικό ενδιαφέρον), τη Διαδικασία Υλοποίησης (δομή και οργάνωση, διαχείριση χρόνου, καταλληλότητα μεθοδολογίας, ανατροφοδότηση, ευκαιρίες συμμετοχής), και το Προϊόν και Εργαλεία (ποιότητα παραδοτέων, σαφήνεια διαδικασίας υλοποίησης, χρησιμότητα ψηφιακών εργαλείων, λειτουργικότητα, πρακτική ή ακαδημαϊκή αξία των παραδοτέων). Το ερωτηματολόγιο κλείνει με ανοιχτό πεδίο, όπου οι φοιτητές καταγράφουν προτάσεις βελτίωσης για το σχέδιο δράσης.

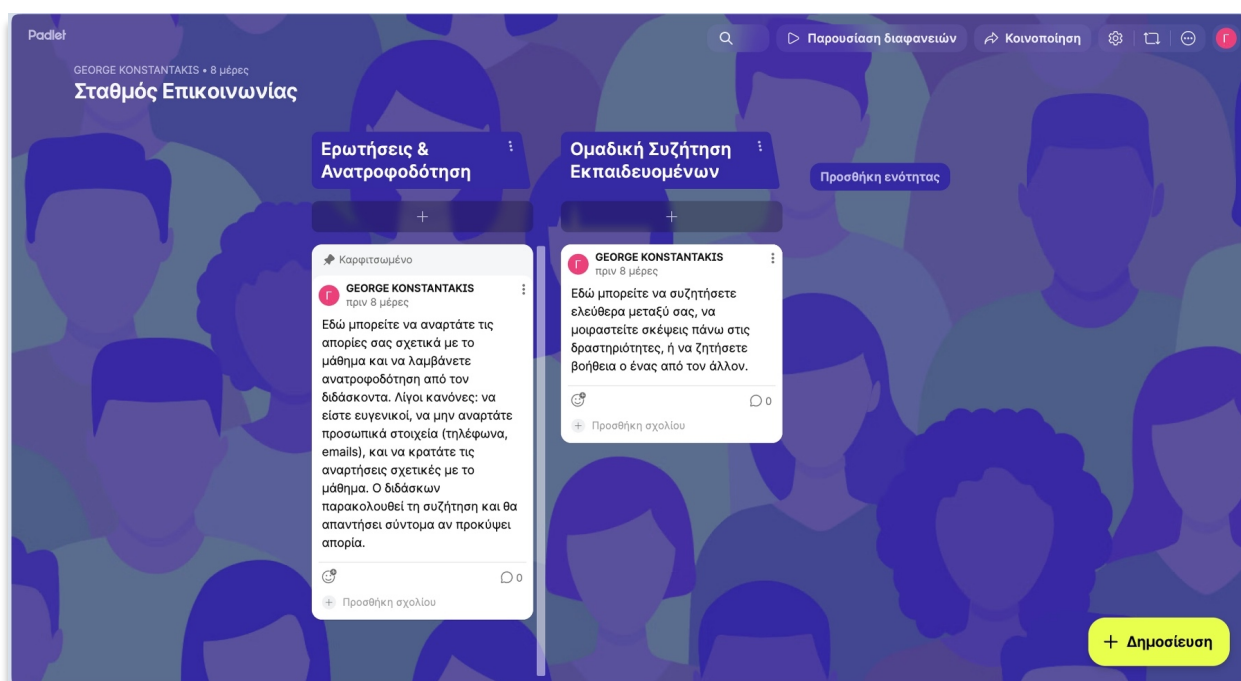
²⁰ Το πλήρες Ερωτηματολόγιο Αξιολόγησης Σχεδίου δράσης διατίθεται στο Παράρτημα.

○ **Δραστηριότητα 20: Παραλαβή Πιστοποιητικού Παρακολούθησης**



Εικόνα 45: Παραλαβή Πιστοποιητικού Παρακολούθησης

Περιγραφή: Στη δραστηριότητα αυτή, οι φοιτητές παραλαμβάνουν το πιστοποιητικό παρακολούθησης, το οποίο αναγνωρίζει την επιτυχή ολοκλήρωση του e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα».



Εικόνα 46: Communication Station

Περιγραφή:

Η σελίδα αυτή αποτελεί την τελευταία επιλογή στο μενού πλοήγησης, μετά τη φάση Self-Reflection, και δεν αποτελεί τμήμα των τριών φάσεων της αυτορρυθμιζόμενης μάθησης και λειτουργεί υποστηρικτικά ως σελίδα επικοινωνίας.

Στη δραστηριότητα αυτή, οι φοιτητές συμμετέχουν στον σταθμό επικοινωνίας μέσω του Padlet, όπου μπορούν να διατυπώνουν απορίες, να ζητούν διευκρινίσεις και να λαμβάνουν ανατροφοδότηση από τον διδάσκοντα. Παράλληλα, στην ενότητα ομαδικής συζήτησης ανταλλάσσουν απόψεις για τις δραστηριότητες, μοιράζονται εμπειρίες και υποστηρίζουν ο ένας τον άλλον, ακολουθώντας βασικούς κανόνες ευγένειας και προστασίας προσωπικών δεδομένων.

3.8 Ερευνητικά Περιβάλλοντα

Η επιλογή του Wix ως ψηφιακού περιβάλλοντος υλοποίησης έγινε με κριτήριο την ευελιξία που προσφέρει στον σχεδιασμό ιστοσελίδων, καθώς και τις δυνατότητες παραμετροποίησης που επιτρέπουν την προσαρμογή του e-course στο προφίλ φοιτητών τριτοβάθμιας εκπαίδευσης. Το σενάριο σχεδιάστηκε ώστε να είναι πλήρως ασύγχρονο με τον φοιτητή να προχωρά μόνος του στον δικό του ρυθμό, μέσα σε επτά εβδομάδες, χωρίς σύγχρονη παρουσία του διδάσκοντα. Δόθηκε ιδιαίτερη βαρύτητα σε ένα απλό και κατανοητό σύστημα πλοήγησης, με σαφές μενού και τις σελίδες Timeline και Road Map, που δείχνουν σαφή εικόνα της πορείας.

Σε αυτό το πλαίσιο εντάχθηκαν οι τρεις φάσεις του μοντέλου της Αυτορρυθμιζόμενης Μάθησης, σε συνδυασμό με τις πέντε ενότητες της προσέγγισης STEAM. Για την επικοινωνία και τη συνεργασία μεταξύ των φοιτητών, ενσωματώθηκε ειδική σελίδα (Communication Station), μέσω της οποίας υποστηρίζονται τόσο η ανταλλαγή αποριών με τον διδάσκοντα όσο και η ελεύθερη συζήτηση μεταξύ των φοιτητών. Παράλληλα, ενσωματώθηκαν επιπλέον ψηφιακά μέσα και εργαλεία, ώστε να εξυπηρετηθούν οι αρχές τόσο της συνεργατικής όσο και της αυτορρυθμιζόμενης μάθησης.

3.9 Τα ψηφιακά μέσα της έρευνας

Τα επιστημονικά άρθρα που τροφοδότησαν τη βιβλιογραφική ενημέρωση της εργασίας αντλήθηκαν κυρίως από το Scopus και το ResearchGate. Το εργαλείο Zotero χρησιμοποιήθηκε καθ' όλη τη διάρκεια της συγγραφής για την καταγραφή και ταξινόμηση των βιβλιογραφικών αναφορών, ενώ το εργαλείο Canva υποστήριξε τη δημιουργία διαγραμμάτων και των πινάκων του κειμένου.

3.10 Τα Ερευνητικά Μέσα

Για τη συλλογή δεδομένων της παρούσας εργασίας, προτείνεται η ενσωμάτωση τεσσάρων ερευνητικών μέσων: ενός εργαλείου μέτρησης δεξιοτήτων, ενός εργαλείου αναστοχασμού, ενός εργαλείου αξιολόγησης του σχεδίου δράσης, και μίας ρουμπρίκας αξιολόγησης παραδοτέων.

3.10.1 Έλεγχος Δεξιοτήτων (Αρχικός/Τελικός)

Το πρώτο εργαλείο είναι ένα ερωτηματολόγιο 12 δηλώσεων τύπου Likert (κλίμακα 1-5), οργανωμένο σε τρεις ενότητες που αντιστοιχούν στους τρεις δείκτες της έρευνας: τη γνωστική εμπλοκή, τη μεταγνωστική παρακολούθηση, και την κατανόηση της οπτικής των άλλων. Το ίδιο ερωτηματολόγιο δίνεται δύο φορές, ως Pre-test στην αρχή της φάσης Forethought και ως Post-test στο τέλος της φάσης Self-Reflection, ώστε να καταστεί δυνατή η σύγκριση των αρχικών και τελικών βαθμολογιών ανά δείκτη (βλ. Παράρτημα).

3.10.2 Ερωτηματολόγιο Αναστοχασμού

Το δεύτερο εργαλείο είναι το ερωτηματολόγιο αναστοχασμού, το οποίο περιλαμβάνει τέσσερις δηλώσεις τύπου Likert, βασισμένες στα δύο θεωρητικά συστατικά της φάσης Self-Reflection: την αυτοκρίση, μέσω της αυτοαξιολόγησης της τελικής επίδοσης και της αναζήτησης αιτιωδών αποδόσεων, και την αυτοαντίδραση, μέσω της αυτοικανοποίησης και της αναπροσαρμογής στρατηγικών. Το ερωτηματολόγιο κλείνει με ανοιχτό πεδίο ελεύθερης απάντησης, το οποίο προσφέρει ποιοτικά δεδομένα προς θεματική ανάλυση (βλ. Παράρτημα).

3.10.3 Ερωτηματολόγιο Αξιολόγησης Σχεδίου Δράσης

Το τρίτο εργαλείο αξιολογεί το ίδιο το εκπαιδευτικό σχέδιο δράσης, μέσω τριών αξόνων με δηλώσεις τύπου Likert: το περιεχόμενο, τη διαδικασία υλοποίησης, το προϊόν και εργαλεία. Το ερωτηματολόγιο κλείνει με ανοιχτό πεδίο προτάσεων βελτίωσης, το οποίο προσφέρει επιπλέον ποιοτικά δεδομένα (βλ. Παράρτημα).

3.10.4 Ρουμπρίκα Αξιολόγησης Παραδοτέων

Για την αξιολόγηση επιλεγμένων ατομικών παραδοτέων των δραστηριοτήτων, προτείνεται ρουμπρίκα αξιολόγησης (βλ. Παράρτημα).

3.11 Αναμενόμενα Ευρήματα

Δεδομένου ότι η παρούσα εργασία επικεντρώνεται στον σχεδιασμό του εκπαιδευτικού σεναρίου και όχι στην πραγματική εφαρμογή του, τα ακόλουθα ευρήματα αποτελούν θεωρητικές προσδοκίες. Σε περίπτωση μελλοντικής εφαρμογής, αναμένεται οι φοιτητές να παρουσιάσουν βελτιωμένες βαθμολογίες στον έλεγχο δεξιοτήτων (Τελικό) σε σχέση με τον αντίστοιχο αρχικό έλεγχο, ιδίως ως προς τη γνωστική εμπλοκή, δεδομένης της συστηματικής έκθεσης σε δραστηριότητες ανάλυσης και αξιολόγησης phishing περιστατικών. Αντίστοιχα, αναμένεται ενίσχυση της μεταγνωστικής παρακολούθησης, ως αποτέλεσμα της συστηματικής χρήσης εργαλείων διαχείρισης χρόνου και αυτοκαταγραφής σε κάθε ενότητα STEAM. Τέλος, αναμένεται θετική αποτίμηση της κατανόησης της οπτικής των άλλων, ενισχυμένη από τις συνεργατικές στρατηγικές (Jigsaw, Πυραμίδα, Think-Pair-Share) που διατρέχουν το σενάριο. Το Ερωτηματολόγιο αξιολόγησης σχεδίου δράσης αναμένεται να αναδείξει θετική συνολική αποτίμηση του σεναρίου, με πιθανά σημεία βελτίωσης να αφορούν τον βαθμό δυσκολίας συγκεκριμένων τεχνικών ενοτήτων.

ΚΕΦΑΛΑΙΟ 4: ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

4.1 Σκοπός του Κεφαλαίου

Το παρόν κεφάλαιο τεκμηριώνει τη χρήση εργαλείων Τεχνητής Νοημοσύνης κατά την εκπόνηση της παρούσας διπλωματικής εργασίας, στο πλαίσιο της διαφάνειας και της ακαδημαϊκής ακεραιότητας, σύμφωνα με την αρχή Human in the Loop (HITL). Η Τεχνητή Νοημοσύνη λειτούργησε ως εργαλείο υποστήριξης της δημιουργικής και επιστημονικής διαδικασίας, με την τελική ευθύνη να παραμένει στον συγγραφέα.

Στη συνέχεια παρουσιάζονται το επίπεδο χρήσης ΤΝ σύμφωνα με το πλαίσιο AI Assessment Scale (AIAS), συνοπτικός πίνακας και αναλυτική περιγραφή των εργαλείων που αξιοποιήθηκαν, ενδεικτικές προτροπές (prompts), τεκμηρίωση των αποφάσεων και παρεμβάσεων του συγγραφέα, καθώς και κριτική αποτίμηση της συνολικής εμπειρίας συνεργασίας με την Τεχνητή Νοημοσύνη.

4.2 Επίπεδο χρήσης της Τεχνητής Νοημοσύνης (AI Assessment Scale – AIAS)

Η παρούσα εργασία εντάσσεται στο AIAS Level 4 (AI Integration), καθώς εργαλεία ΤΝ χρησιμοποιήθηκαν για την παραγωγή αναπόσπαστων στοιχείων του τελικού ψηφιακού μαθήματος, όπως τα βίντεο avatar της ψηφιακής βοηθού «Σοφία», οι φωνητικές αφηγήσεις, οι διαδραστικές εφαρμογές και σελίδες, καθώς και εκπαιδευτικό βίντεο και εικόνες. Ωστόσο, όλες οι παιδαγωγικές αποφάσεις, η επιλογή του περιεχομένου, η αξιολόγηση της ποιότητας και η τελική μορφή του υλικού αποτελούν αποκλειστική ευθύνη του συγγραφέα.

4.3 Συνοπτικός Πίνακας Χρήσης της Τεχνητής Νοημοσύνης

Πίνακας 17: Συνοπτικός Πίνακας Χρήσης της Τεχνητής Νοημοσύνης

Στάδιο εργασίας	Εργαλείο ΤΝ	Σκοπός χρήσης	ΑΙΑΣ ΕΠΙΠΕΔΟ	Ανθρώπινη παρέμβαση
Σχεδιασμός μαθήματος	-	-	Level 1	Καμία εμπλοκή ΤΝ
Δημιουργία εικόνων	ChatGPT	Παραγωγή Εικόνων	Level 4	Επιλογή και επεξεργασία εικόνων
Δημιουργία avatar	Hedra AI	Δημιουργία avatar video ψηφιακής βοηθού «Σοφία»	Level 4	Επεξεργασία εικόνας και μοντάζ
Δημιουργία διαδραστικών εφαρμογών	Lovable AI	Δημιουργία rule-based chatbot οδηγιών, διάγραμμα ακολουθίας	Level 4	Σχεδιασμός ροής, επιλογή περιεχομένου
Δημιουργία διαδραστικών παρουσιάσεων	Base44 AI	Δημιουργία Timeline, Interactive Concept Map, Threat Map	Level 4	Επιλογή περιεχομένου, παιδαγωγικός έλεγχος
Δημιουργία βίντεο	NotebookLM	Παραγωγή εκπαιδευτικού βίντεο	Level 4	Παροχή πηγών και σεναρίου, έλεγχος τελικού βίντεο
Αφήγηση	Google AI Studio	Μετατροπή κειμένου σε ομιλία	Level 4	Επιλογή φωνής και επεξεργασία ήχου
Γλωσσική επιμέλεια	Claude AI	Έλεγχος και επιμέλεια κειμένου ΜΔΕ	Level 3	Έλεγχος επιστημονικής ακρίβειας, τελικές διορθώσεις

4.4 Αναλυτική περιγραφή της χρήσης της Τεχνητής Νοημοσύνης

4.4.1 Δημιουργία Εικόνων (ChatGPT)

Περιγραφή: Το εργαλείο ChatGPT (OpenAI, 2026) χρησιμοποιήθηκε για τη δημιουργία εικόνων που ενσωματώθηκαν στις σελίδες του ψηφιακού μαθήματος στο Wix (Road Map, Forethought, πέντε σελίδες της φάσης Performance στο πλαίσιο STEAM, Self-Reflection), καθώς και για τη δημιουργία της φωτογραφίας avatar της ψηφιακής βοηθού «Σοφία», η οποία χρησιμοποιήθηκε στη συνέχεια ως βάση σε όλα τα βίντεο avatar που παρήχθησαν με το εργαλείο Hedra AI. Λόγω σφαλμάτων στην αρχική παραγωγή, ο συγγραφέας επέλεξε τις εικόνες που κρίθηκαν κατάλληλες και προχώρησε σε περαιτέρω επεξεργασία τους μέσω του εργαλείου Canva, με αναβάθμιση κλίμακας (upscale), βελτίωση ανάλυσης, διόρθωση χρωμάτων και αύξηση της ευκρίνειας. Ο συγγραφέας επέλεξε τις κατάλληλες εικόνες ανάμεσα σε πολλές εναλλακτικές και ολοκλήρωσε ο ίδιος την επεξεργασία τους ώστε να ανταποκρίνονται στις αισθητικές απαιτήσεις του e-course.

4.4.2 Δημιουργία avatar (Hedra AI)

Περιγραφή: Το εργαλείο Hedra AI (Hedra, 2026) χρησιμοποιήθηκε για την παραγωγή τριών βίντεο με την ψηφιακή βοηθό «Σοφία»: ενός βίντεο για τη σελίδα Home Page, ενός εισαγωγικού βίντεο στην ενότητα Engineering της φάσης Performance, και ενός εισαγωγικού βίντεο στη φάση Self-Reflection. Ως είσοδος χρησιμοποιήθηκαν η φωτογραφία-avatar της Σοφίας, παραγόμενη με το ChatGPT, και το ηχητικό αφήγησης κάθε βίντεο, το οποίο δημιουργήθηκε στο Google AI Studio από κείμενο που έγραψε ο συγγραφέας. Στη συνέχεια, τα βίντεο υποβλήθηκαν σε επεξεργασία στο DaVinci Resolve, όπου πραγματοποιήθηκε μοντάζ και επεξεργασία εικόνας, προστέθηκε μουσική υπόκρουση από ελεύθερη πηγή και έγινε η τελική εξαγωγή του αποτελέσματος. Η προετοιμασία του υλικού εισόδου (φωτογραφία, ηχητικό), καθώς και ολόκληρη η μετα-παραγωγή των τριών βίντεο, έγιναν αποκλειστικά από τον συγγραφέα.

4.4.3 Δημιουργία διαδραστικών εφαρμογών (Lovable AI)

Περιγραφή: Το εργαλείο Lovable AI (Lovable, 2026) χρησιμοποιήθηκε για τη δημιουργία του rule-based chatbot οδηγιών του avatar «Σοφία» στην αρχική σελίδα, καθώς και για τη δημιουργία ενός θεωρητικού διαγράμματος ακολουθίας στην ενότητα Engineering της φάσης Performance. Ο συγγραφέας έδωσε αναλυτικό prompt με σαφείς οδηγίες ως προς το περιεχόμενο και τη λειτουργία του κάθε στοιχείου. Στην πορεία εντοπίστηκαν ορισμένα σφάλματα στην αρχική παραγωγή, για τη διόρθωση των οποίων χρειάστηκαν 2-3 διαδοχικές υποδείξεις προς το εργαλείο. Ο συγγραφέας διαμόρφωσε το αρχικό prompt και εντόπισε ο ίδιος τα σφάλματα που χρειάστηκε να διορθωθούν μέχρι το τελικό αποτέλεσμα.

4.4.4 Δημιουργία διαδραστικών παρουσιάσεων (Base44 AI)

Περιγραφή: Το εργαλείο Base44 AI (Base44, 2026) χρησιμοποιήθηκε για τη δημιουργία διαδραστικών σελίδων του ψηφιακού μαθήματος, όπως το Timeline, ο διαδραστικός χάρτης phishing στη φάση Forethought και ο εννοιολογικός χάρτης στην ενότητα Science της φάσης Performance. Για το Timeline δόθηκε αναλυτικό prompt με το ακριβές κείμενο περιεχομένου. Για τους δύο χάρτες, ο συγγραφέας σχεδίασε αρχικά δύο βασικά διαγράμματα στο Canva, τα οποία δόθηκαν ως εικόνες στο εργαλείο για τη δημιουργία των αντίστοιχων διαδραστικών εκδοχών. Χρειάστηκαν ορισμένες διορθώσεις στα γραφικά, καθώς δόθηκαν στο εργαλείο σαφείς οδηγίες ως προς τα χρώματα, ώστε το αποτέλεσμα να εναρμονίζεται αισθητικά με το υπόλοιπο e-course. Ο αρχικός σχεδιασμός του οπτικού υλικού, η διαμόρφωση των prompts, και οι διορθώσεις που οδήγησαν στο τελικό αποτέλεσμα, ήταν ευθύνη του συγγραφέα.

4.4.5 Δημιουργία Βίντεο (NotebookLM)

Περιγραφή: Το εργαλείο NotebookLM (Google, 2026e) χρησιμοποιήθηκε για τη δημιουργία ενός εκπαιδευτικού βίντεο στην ενότητα Science της φάσης Performance. Ο συγγραφέας έδωσε στο εργαλείο αναλυτικό θεωρητικό κείμενο δικής του σύνταξης, βασισμένο σε πηγές, ως υλικό εκκίνησης. Οι πρώτες παραγωγές παρουσίασαν προβλήματα, με το βίντεο να βγαίνει υπερβολικά μεγάλο σε διάρκεια και να περιλαμβάνει μη απαραίτητο περιεχόμενο. Μετά από αρκετές δοκιμές, επιλέχθηκε η εκδοχή που κρίθηκε καταλληλότερη και χρησιμοποιήθηκε στο τελικό μάθημα. Τόσο η σύνταξη του πηγαιού κειμένου όσο και η επιλογή της κατάλληλης εκδοχής ανάμεσα σε πολλαπλές δοκιμές, ήταν απόφαση του συγγραφέα.

4.4.6 Αφήγηση (Google AI Studio)

Περιγραφή: Το εργαλείο Google AI Studio (Google, 2026a) χρησιμοποιήθηκε για τη μετατροπή κειμένου σε ομιλία (text-to-speech), με βάση κείμενο που συνέταξε ο συγγραφέας βασισμένο σε κατάλληλες πηγές. Σε 1-2 περιπτώσεις παρατηρήθηκε λανθασμένος τονισμός ορισμένων λέξεων, χωρίς ωστόσο να προκύψουν ουσιαστικά προβλήματα στην παραγωγή. Τα ηχητικά αρχεία υποβλήθηκαν στη συνέχεια σε επεξεργασία ήχου (EQ, compression, αποθορυβοποίηση όπου χρειάστηκε). Ο συγγραφέας συνέταξε το κείμενο εκκίνησης και επεξεργάστηκε ο ίδιος τον τελικό ήχο.

4.4.7 Γλωσσική Επιμέλεια (Claude AI)

Περιγραφή: Το εργαλείο Claude AI (Anthropic, 2026) χρησιμοποιήθηκε για τη γλωσσική επιμέλεια του κειμένου της παρούσας διπλωματικής εργασίας, με βάση συγκεκριμένες οδηγίες που έδινε ο συγγραφέας ως προς το τι χρειαζόταν βελτίωση σε κάθε σημείο. Το εργαλείο παρουσίασε ορισμένα σφάλματα στις προτάσεις του, τα οποία εντοπίστηκαν και διορθώθηκαν από τον συγγραφέα. Ο έλεγχος των πηγών, η επιστημονική ακρίβεια του περιεχομένου και η τελική διατύπωση παρέμειναν αποκλειστική ευθύνη του συγγραφέα, καθιστώντας την ανθρώπινη παρέμβαση απαραίτητη σε όλα τα στάδια της γλωσσικής επιμέλειας.

4.5 Ενδεικτικά Prompts

4.5.1 Lovable AI

Σκοπός: Δημιουργία rule-based chatbot οδηγίων στην αρχική σελίδα του e-course.

Prompt: «Δημιούργησε έναν προκαθορισμένο rule-based εκπαιδευτικό chatbot στα ελληνικά, που θα λειτουργεί ως ψηφιακός οδηγός ενός ασύγχρονου e-course. Ταυτότητα: Όνομα: Σοφία. Ρόλος: ψηφιακός οδηγός του e-course «Phishing 360°: Από το Συναίσθημα στα Δεδομένα». Στόχος: να βοηθά τους φοιτητές να κατανοήσουν τη δομή του μαθήματος, να πλοηγηθούν στο e-course και να βρίσκουν βασικές πληροφορίες για τις δραστηριότητες, τα εργαλεία και την υποστήριξη. Κανόνες λειτουργίας: Χρησιμοποίησε αποκλειστικά τις πληροφορίες που δίνονται παρακάτω, χωρίς νέο περιεχόμενο ή υποθέσεις. Μην απαντάς σε ερωτήσεις άσχετες με το e-course. Ύφος φιλικό, υποστηρικτικό, σαφές, σε β' πληθυντικό. Ο διάλογος γίνεται αποκλειστικά με κουμπιά επιλογών και προκαθορισμένες απαντήσεις, χωρίς ανοικτές ερωτήσεις ή ελεύθερη πληκτρολόγηση. Μετά από κάθε απάντηση, ο χρήστης επιστρέφει αυτόματα στο βασικό μενού. Μήνυμα καλωσορίσματος: «Γεια σας! Είμαι η Σοφία, ο ψηφιακός οδηγός του e-course Phishing 360°: Από το Συναίσθημα στα Δεδομένα. Μπορώ να σας βοηθήσω με πληροφορίες σχετικά με το μάθημα, την πλοήγηση και τις δραστηριότητες.» Βασικό μενού επιλογών: 1) Καλωσόρισμα στο μάθημα: παρουσίαση του e-course, αναφορά ότι σχεδιάστηκε στο πλαίσιο ΜΔΕ του ΠΜΣ «Ηλεκτρονική Μάθηση» του Πανεπιστημίου Πειραιώς. 2) Τι είναι το Phishing 360°: ασύγχρονο μάθημα κυβερνοασφάλειας για αναγνώριση και αντιμετώπιση phishing μέσα από θεωρία, προσομοιώσεις και συνεργατικές δραστηριότητες. 3) Διάρκεια: 7 εβδομάδες, 14 ώρες συνολικά, αυτορρυθμιζόμενος ρυθμός. 4) Δομή e-course: μοντέλο SRL (Forethought, Performance, Self-Reflection), με τη φάση Performance σε πέντε στάδια κατά STEAM. 5) Πλοήγηση: πάνω μενού, κουμπιά «Previous/Next Page», σύντομη περιγραφή κάθε σελίδας. 6) Μαθησιακά αποτελέσματα: 8 δεξιότητες (αναγνώριση, κατανόηση, εφαρμογή, ανάλυση, αξιολόγηση, δημιουργία, αυτοπαρακολούθηση, συνεργασία). 7) Εργαλεία: Lumi, Base44 AI, Trello, Evernote, Padlet, Mentimeter, Lucidchart, Canva, Genially, Google Docs, Google Forms, Excel. 8) Υποβολή εργασιών: κουμπί «Submit Assignment» προς το Google Classroom. 9) Τεχνικές απαιτήσεις: σταθερή σύνδεση, browser, κωδικός και λογαριασμός Google. 10) Προαπαιτούμενες γνώσεις: όχι, αρκούν βασικές δεξιότητες υπολογιστή/διαδικτύου. 11) Ολοκλήρωση: συμμετοχή σε όλες τις δραστηριότητες εντός 7 εβδομάδων. 12) Προσβασιμότητα: κουμπί «View Transcript» κάτω από κάθε βίντεο,

αποθήκευση σε PDF μέσω Ctrl+P. 13) Βοήθεια: σελίδα Communication Station. 14) Τεχνική υποστήριξη: επικοινωνία με τον διδάσκοντα μέσω email. Σχεδιαστικές προδιαγραφές: Διεπαφή τύπου παραθύρου συνομιλίας με avatar της Σοφίας, φυσαλίδες μηνυμάτων, typing indicator, αυτόματη κύλιση. Μόνιμο «ΒΑΣΙΚΟ ΜΕΝΟΥ ΕΠΙΛΟΓΩΝ» κάτω από τη συνομιλία. Χρωματική παλέτα σε αποχρώσεις μπλε/navy με θεματική κυβερνοασφάλειας, πλήρως responsive σχεδίαση.»

4.5.2 NotebookLM

Σκοπός: Δημιουργία εκπαιδευτικού βίντεο «Η ψυχολογία της Κοινωνικής Μηχανικής» (Ενότητα Science, φάση Performance).

Prompt: «Φτιάξε ένα βίντεο 2,5 λεπτών με αυτήν τη δομή: Η Ψυχολογία της Κοινωνικής Μηχανικής. Η κοινωνική μηχανική εκμεταλλεύεται την ανθρώπινη σκέψη, την εμπιστοσύνη και τη διαδικασία λήψης αποφάσεων. Στόχος του επιτιθέμενου είναι να πείσει το θύμα να ενεργήσει σύμφωνα με το συμφέρον του. 1. Κοινωνική Μηχανική ως Ψυχολογική Επίθεση. Ο επιτιθέμενος δημιουργεί μήνυμα ή αίτημα με σκοπό να πείσει το θύμα να κάνει μια συγκεκριμένη ενέργεια, όπως να εμπιστευτεί ένα μήνυμα ή να αποκαλύψει πληροφορίες. 2. Η Γνωστική Λειτουργία στο Στόχαστρο. Ο επιτιθέμενος προσπαθεί να επηρεάσει γνωστικές διαδικασίες όπως η αντίληψη, η εργαζόμενη μνήμη, ώστε το θύμα να αντιδράσει γρήγορα. 3. Παράγοντες που Αυξάνουν την Ευαλωτότητα. Γνωστικός φόρτος, στρες, μειωμένη προσοχή και επαγρύπνηση. Όταν ο χρήστης έχει πολλά καθήκοντα, πίεση χρόνου ή μειωμένη προσοχή, μπορεί να αγνοήσει σημάδια εξαπάτησης. 4. Ρόλος Γνώσης, Εμπειρίας και Κουλτούρας. Γνώση αντικειμένου, προηγούμενη εμπειρία, κουλτούρα και εξοικείωση με απειλές. Η εμπειρία και η γνώση μειώνουν την ευαλωτότητα, ενώ η έλλειψη γνώσης ή η υπερβολική εμπιστοσύνη μπορεί να οδηγήσουν σε λάθη. 5. Πειθώ στα Μηνύματα Phishing. Τα phishing emails χρησιμοποιούν τεχνικές πειθούς για να φαίνονται αξιόπιστα. Η πειθώ έχει στόχο να αλλάξει στάσεις ή πεποιθήσεις μέσα από επείγον ύφος, επίκληση σε γνωστούς οργανισμούς 6. Βασικές Αρχές Πειθούς. Αυθεντία: Το μήνυμα φαίνεται ότι προέρχεται από ισχυρό ή αξιόπιστο φορέα. Έντονο συναίσθημα: Προκαλεί φόβο, αγωνία ή επείγουσα αντίδραση. Ακεραιότητα: Κάνει το αίτημα να φαίνεται νόμιμο και αξιόπιστο. Ανταπόδοση: Δημιουργεί την αίσθηση ότι πρέπει να ανταποκριθούμε σε μια προσφορά ή βοήθεια. 7. Από τη Συνειδητή Σκέψη στην Αυτόματη Αντίδραση. Όταν ένα μήνυμα φαίνεται σχετικό, επείγον ή αξιόπιστο, ο χρήστης

μπορεί να εστιάσει στο περιεχόμενο του αιτήματος και να παραβλέψει ενδείξεις εξαπάτησης. 8. Τι Πρέπει να Καταλάβει ο Εκπαιδευόμενος. Αναγνωρίζει τότε ένα μήνυμα προσπαθεί να κερδίσει την εμπιστοσύνη του. Εντοπίζει τεχνικές που προκαλούν έντονο συναίσθημα ή επείγουσα αντίδραση. Η κατανόηση της ψυχολογίας της κοινωνικής μηχανικής είναι το κλειδί για την αποφυγή phishing επιθέσεων.»

4.5.3 Base44 AI

Σκοπός: Δημιουργία εννοιολογικού χάρτη στην ενότητα Science της φάσης Performance.

Prompt: «Δημιούργησε έναν εννοιολογικό χάρτη στα ελληνικά με τίτλο «Η Ψυχολογία της Κοινωνικής Μηχανικής». Στο κέντρο βάλε την έννοια «Κοινωνική Μηχανική» και γύρω της οργάνωσε τους βασικούς κλάδους: «Ψυχολογική επίθεση», «Ανθρώπινη γνωστική λειτουργία», «Παράγοντες ευαλωτότητας», «Πειθώ στα phishing emails» και «Απόφαση του χρήστη». Στον κλάδο «Ψυχολογική επίθεση» να παρουσιαστεί ότι η κοινωνική μηχανική προσπαθεί να επηρεάσει το θύμα ώστε να ενεργήσει σύμφωνα με τον στόχο του επιτιθέμενου. Στον κλάδο «Ανθρώπινη γνωστική λειτουργία» να συμπεριληφθούν έννοιες όπως αντίληψη, εργαζόμενη μνήμη, λήψη αποφάσεων και δράση. Στον κλάδο «Παράγοντες ευαλωτότητας» να παρουσιαστούν ο γνωστικός φόρτος, το στρες, η προσοχή/επαγρύπνηση, η γνώση, η εμπειρία και η κουλτούρα. Στον κλάδο «Πειθώ στα phishing emails» να παρουσιαστεί ότι τα παραπλανητικά μηνύματα χρησιμοποιούν τεχνικές πειθούς για να φαίνονται αξιόπιστα και να επηρεάζουν τη συμπεριφορά του χρήστη.

Να συμπεριληφθούν οι έννοιες αυθεντία, έντονο συναίσθημα, ακεραιότητα/συνέπεια και ανταπόδοση, με σύντομη επεξήγηση για καθεμία. Στον κλάδο «Απόφαση του χρήστη» να φανεί πώς οι παραπάνω παράγοντες μπορούν να επηρεάσουν την κρίση του χρήστη και να τον οδηγήσουν σε ενέργειες όπως άνοιγμα μηνύματος, εμπιστοσύνη σε αίτημα ή αποκάλυψη πληροφοριών. Ο χάρτης να είναι σύντομος, καθαρός, ιεραρχικός και κατάλληλος για παρουσίαση σε εκπαιδευτικό e-course. Να μη γραφτεί απλή λίστα, αλλά να φαίνονται οι σχέσεις μεταξύ των εννοιών.»

4.5.4 ChatGPT

Σκοπός: Δημιουργία εικόνας για τη σελίδα Road Map με βάση έτοιμο template από το εργαλείο Canva (Canva, 2026).

Prompt: «Δημιούργησε ένα περιβάλλον κυβερνοασφάλειας, σε οριζόντια σύνθεση 16:9. Στο πάνω κέντρο ένα ανθρωπόμορφο ρομπότ AI με μεταλλικό σώμα και φωτεινά μπλε στοιχεία. Στο κέντρο ένας ψηφιακός κόμβος με μικρή φουτουριστική πόλη και 8 φωτεινές κυκλικές πλατφόρμες γύρω του, συνδεδεμένες με τεχνολογικές διαδρομές σαν roadmap. Νέον μπλε, κυανό και μωβ, ψηφιακός κώδικας και holographic οθόνες στο φόντο. Πολύ λεπτομερές, συμμετρικό, εντυπωσιακό, επαγγελματικό εκπαιδευτικό περιβάλλον. Χωρίς κείμενο, χωρίς λογότυπα, χωρίς κουμπιά.»

4.6 Ανάλυση / Τεκμηρίωση των Αποφάσεων και Παρεμβάσεων

Κατά τη συνεργασία με τα εργαλεία Τεχνητής Νοημοσύνης ο συγγραφέας διατήρησε τον πλήρη έλεγχο των αποφάσεων, εφαρμόζοντας την αρχή Human in the Loop (HITL). Αρκετές από τις αρχικές παραγωγές απορρίφθηκαν εξ ολοκλήρου, όπως συνέβη με τις πρώτες εκδοχές του εκπαιδευτικού βίντεο από το εργαλείο NotebookLM, οι οποίες παρουσίαζαν υπερβολική διάρκεια με περιεχόμενο που δεν εξυπηρετούσε τον στόχο, με αποτέλεσμα να χρειαστούν αρκετές δοκιμές μέχρι να προκύψει η κατάλληλη εκδοχή. Άλλες παραγωγές τροποποιήθηκαν σημαντικά μετά τον έλεγχο του συγγραφέα, όπως τα γραφικά στοιχεία και τα χρώματα των διαδραστικών εφαρμογών που δημιουργήθηκαν με το εργαλείο Base44 AI. Επίσης τροποποιήθηκε και το περιεχόμενο του rule-based chatbot οδηγιών που δημιουργήθηκε από το εργαλείο Lovable AI, όπου εντοπίστηκαν σφάλματα που διορθώθηκαν μέσα από διαδοχικές υποδείξεις.

Ιδιαίτερη προσοχή δόθηκε στον επιστημονικό έλεγχο του βίντεο που παρήχθη από το NotebookLM, με βασικό και καθοριστικό ρόλο του συγγραφέα στην επιλογή και επαλήθευση του περιεχομένου.

Το Claude AI είχε απλώς υποστηρικτικό ρόλο στη γλωσσική επιμέλεια, ενώ η ευθύνη για την επιστημονική ακρίβεια και την τελική διατύπωση του κειμένου παρέμεινε στον συγγραφέα. Ο έλεγχος σε όλες τις περιπτώσεις χρήσης της Τεχνητής Νοημοσύνης ήταν ενδεδειγμένος και ο συγγραφέας βασίστηκε κυρίως σε καλές πρακτικές που αντλήθηκαν από παλαιότερες διπλωματικές εργασίες.

Οι παιδαγωγικές αποφάσεις παρέμειναν καθ' όλη τη διάρκεια αποκλειστική ευθύνη του συγγραφέα. Το στήσιμο του μαθήματος με βάση το μοντέλο SRL, η προσέγγιση STEAM και ο σχεδιασμός των εκπαιδευτικών δραστηριοτήτων αποτέλεσαν αποκλειστικά δική του δουλειά. Στο σύνολο της εργασίας τα εργαλεία ΤΝ διατήρησαν υποστηρικτικό ρόλο, ενώ ο σχεδιασμός, η αξιολόγηση και η τελική μορφή κάθε παραδοτέου προέκυψαν από τη συνειδητή κρίση και τις αποφάσεις του συγγραφέα.

4.7 Κριτική Αποτίμηση της Χρήσης της Τεχνητής Νοημοσύνης

Η αξιοποίηση εργαλείων Τεχνητής Νοημοσύνης κατά την εκπόνηση της παρούσας διπλωματικής εργασίας αποδείχθηκε ιδιαίτερα χρήσιμη κυρίως στην ταχύτητα παραγωγής πολυμεσικού υλικού, όπως τα βίντεο avatar, τα εκπαιδευτικά βίντεο και οι φωνητικές αφηγήσεις. Η δυνατότητα γρήγορης παραγωγής πολλαπλών εναλλακτικών εκδοχών επέτρεψε στον συγγραφέα να δοκιμάσει διαφορετικές προσεγγίσεις και να επιλέξει την καταλληλότερη, κάτι που θα απαιτούσε πολύ περισσότερο χρόνο σε σχέση με παραδοσιακές μεθόδους παραγωγής οπτικοακουστικού υλικού.

Παράλληλα εντοπίστηκαν σημαντικοί περιορισμοί στα εργαλεία που χρησιμοποιήθηκαν. Το βασικότερο πρόβλημα ήταν οι επαναλαμβανόμενες ανακρίβειες και τα σφάλματα στο παραγόμενο περιεχόμενο, τα οποία απαιτούσαν συστηματικό έλεγχο πριν από κάθε χρήση. Χαρακτηριστικό παράδειγμα αποτέλεσε το NotebookLM, όπου οι πρώτες εκδοχές του εκπαιδευτικού βίντεο ήταν υπερβολικά μεγάλες σε διάρκεια και περιείχαν περιεχόμενο εκτός στόχου, με αποτέλεσμα να χρειαστούν πολλαπλές διαδοχικές δοκιμές μέχρι να προκύψει αποδεκτό αποτέλεσμα.

Αντίστοιχα, οι γλωσσικές προτάσεις του Claude AI παρουσίασαν σε ορισμένα σημεία ανακρίβειες που έπρεπε να εντοπιστούν και να διορθωθούν, ενώ τα γραφικά στοιχεία που παρήγαγαν τα εργαλεία Lovable AI και Base44 AI χρειάστηκαν διορθώσεις ώστε να ανταποκρίνονται στις αισθητικές απαιτήσεις του e-course.

Ένας επιπλέον παράγοντας που αναδείχθηκε κατά τη συνεργασία ήταν το γεγονός ότι τα εργαλεία ΤΝ δεν αντιλαμβάνονται κείμενο ή εικόνα με τον τρόπο που τα αντιλαμβάνεται ένας άνθρωπος, καθώς δεν διαθέτουν βιωμένη εμπειρία ή κοινή λογική για να συμπληρώσουν νοερά κενά σε ασαφείς οδηγίες. Για τον λόγο αυτό, η επίτευξη αποτελέσματος που να ανταποκρίνεται πλήρως στις ανθρώπινες απαιτήσεις απαιτούσε ιδιαίτερα σαφές και αναλυτικό prompting, καθώς και, σε αρκετές περιπτώσεις, περισσότερο χρόνο και επαναληπτικές δοκιμές σε σχέση με μια αρχική, γενικόλογη οδηγία.

Η ανθρώπινη παρέμβαση υπήρξε απαραίτητη σε όλα τα στάδια της διαδικασίας, τόσο στον έλεγχο της επιστημονικής ακρίβειας του περιεχομένου όσο και στην αξιολόγηση και επιλογή ανάμεσα σε πολλαπλές παραγόμενες εκδοχές. Από τη συνολική συνεργασία με τα εργαλεία ΤΝ προέκυψε το βασικό δίδαγμα ότι η Τεχνητή Νοημοσύνη λειτουργεί αποτελεσματικά ως εργαλείο επιτάχυνσης και υποστήριξης της δημιουργικής διαδικασίας, χωρίς ωστόσο να μπορεί να υποκαταστήσει την κρίση, τον έλεγχο και την τελική ευθύνη του ανθρώπου. Η αρχή Human in the Loop επιβεβαιώθηκε στην πράξη ως απαραίτητη προϋπόθεση για την παραγωγή ενός επιστημονικά έγκυρου και παιδαγωγικά άρτιου αποτελέσματος.

ΚΕΦΑΛΑΙΟ 5: ANAMENOMENA ΑΠΟΤΕΛΕΣΜΑΤΑ & ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

5.1 Επισκόπηση Αναμενόμενων Ευρημάτων

Η παρούσα εργασία σχεδίασε και ανέπτυξε το e-course «Phishing 360⁰: Από το Συναίσθημα στα Δεδομένα», με στόχο να διερευνήσει τη συμβολή του στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας σε φοιτητές τριτοβάθμιας εκπαίδευσης, μέσα από τρία ερευνητικά ερωτήματα. Καθώς η εργασία παραμένει σε επίπεδο σχεδιασμού, όσα ακολουθούν αποτελούν θεωρητικές προσδοκίες, προς μελλοντική επιβεβαίωση.

Ως προς το RQ1 (γνωστική εμπλοκή), οι φοιτητές αναμένεται να παρουσιάσουν βελτιωμένες βαθμολογίες στον τελικό έλεγχο δεξιοτήτων σε σχέση με τον αρχικό, ως αποτέλεσμα της ενεργού συμμετοχής τους σε δραστηριότητες ανάλυσης αυθεντικών σεναρίων (case studies) phishing. Ως προς το RQ2 (μεταγνωστική παρακολούθηση), αναμένεται ενίσχυση μέσω της συστηματικής χρήσης εργαλείων διαχείρισης χρόνου και αυτοκαταγραφής σε κάθε ενότητα STEAM. Ως προς το RQ3 (κατανόηση της οπτικής των άλλων), αναμένεται θετική επίδραση, ενισχυμένη από τις συνεργατικές στρατηγικές (Jigsaw, Πυραμίδα, Think-Pair-Share) που διατρέχουν το σενάριο. Παράλληλα, το ερωτηματολόγιο αξιολόγησης σχεδίου δράσης αναμένεται να αναδείξει θετική συνολική αποτίμηση του σεναρίου από τους φοιτητές, με πιθανά σημεία βελτίωσης να αφορούν τον βαθμό δυσκολίας συγκεκριμένων τεχνικών ενοτήτων.

5.2 Συζήτηση - Συμπεράσματα, Περαιτέρω Μελέτη και Έρευνα

Τα αναμενόμενα ευρήματα, αν επιβεβαιωθούν, θα υποστήριζαν την αρχική υπόθεση της εργασίας ότι ο συνδυασμός της Αυτορρυθμιζόμενης Μάθησης, του STEAM και υποστηρικτικών εργαλείων Τεχνητής Νοημοσύνης μπορεί να λειτουργήσει συμπληρωματικά για την καλλιέργεια μετρήσιμων δεξιοτήτων κυβερνοασφάλειας. Η συμβολή της εργασίας έγκειται στην πρόταση ενός ολοκληρωμένου, θεωρητικά τεκμηριωμένου παιδαγωγικού πλαισίου, το οποίο μπορεί να αποτελέσει τη βάση για μελλοντική εφαρμογή και έρευνα στο πεδίο.

Η ερμηνεία των παραπάνω οφείλει να λάβει υπόψη ορισμένους περιορισμούς. Η εργασία παραμένει σε επίπεδο σχεδιασμού, χωρίς να έχει δοκιμαστεί σε πραγματικές συνθήκες τάξης, ενώ ο προτεινόμενος σχεδιασμός μίας ομάδας με μετρήσεις πριν και μετά την παρέμβαση, χωρίς ομάδα ελέγχου, περιορίζει την αιτιώδη ερμηνεία τυχόν βελτίωσης. Επιπλέον, το προτεινόμενο δείγμα των 25-30 φοιτητών είναι πολύ μικρό ώστε να επιτρέψει γενίκευση των συμπερασμάτων σε όλο τον πληθυσμό φοιτητών τριτοβάθμιας εκπαίδευσης.

Ως άμεση προτεραιότητα για μελλοντική έρευνα προτείνεται η πραγματική εφαρμογή και αξιολόγηση του e-course σε δείγμα φοιτητών, ώστε να επιβεβαιωθούν ή να αναθεωρηθούν τα θεωρητικά ευρήματα του Κεφαλαίου 3. Στο πλαίσιο αυτό θα ήταν σκόπιμη η υιοθέτηση πειραματικού σχεδιασμού με ομάδα ελέγχου, ώστε να ενισχυθεί η αιτιώδης ερμηνεία των αποτελεσμάτων. Πέρα από την πραγματική εφαρμογή, η βιβλιογραφική επισκόπηση της εργασίας ανέδειξε δύο ευρύτερα κενά που παραμένουν σχετικά ανεπαρκώς μελετημένα: αφενός, τον τρόπο με τον οποίο η Αυτορρυθμιζόμενη Μάθηση και το STEAM μπορούν να συνδυαστούν ουσιαστικά με ψηφιακά εργαλεία σε συγκεκριμένα γνωστικά πεδία και αφετέρου, τον τρόπο με τον οποίο η ουσιαστική ενσωμάτωση εργαλείων Τεχνητής Νοημοσύνης στην εκπαίδευση κυβερνοασφάλειας απαιτεί νέους παιδαγωγικούς σχεδιασμούς. Μελλοντική έρευνα θα μπορούσε να διερευνήσει συστηματικά αυτά τα δύο ζητήματα, τόσο μέσα από το συγκεκριμένο σενάριο όσο και σε ευρύτερα γνωστικά αντικείμενα και εκπαιδευτικά πλαίσια. Επιπλέον, θα είχε ενδιαφέρον η διερεύνηση εξατομικευμένων προσεγγίσεων στο πλαίσιο του σεναρίου, μέσω συστήματος διαχείρισης μάθησης (LMS) που θα προσαρμόζει το περιεχόμενο στο μαθησιακό στυλ κάθε φοιτητή.

BIBΛΙΟΓΡΑΦΙΑ

- Abrahamson, C. E. (1998). Storytelling as a Pedagogical Tool in Higher Education. *Education*, 118(3), 440–452.
- Akamatsu, D., Nakaya, M., & Koizumi, R. (2019). Effects of Metacognitive Strategies on the Self-Regulated Learning Process: The Mediating Effects of Self-Efficacy. *Behavioral Sciences*, 9(12), 128. <https://doi.org/10.3390/bs9120128>
- Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), 168. <https://doi.org/10.3390/fi12100168>
- Alam, A., & Mohanty, A. (2024). Framework of Self-Regulated Cognitive Engagement (FSRCE) for sustainable pedagogy: A model that integrates SRL and cognitive engagement for holistic development of students. *Cogent Education*, 11(1), 2363157. <https://doi.org/10.1080/2331186X.2024.2363157>
- Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science*, 8, e827. <https://doi.org/10.7717/peerj-cs.827>
- Anthropic. (2026). Claude (Version Sonnet 5) [Computer software]. <https://www.anthropic.com/claude>
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Arduin, P.-E., & Costé, B. (2026). Learning to Hack, Playing to Learn: Gamification in Cybersecurity Courses. *Journal of Cybersecurity and Privacy*, 6(1), 16. <https://doi.org/10.3390/jcp6010016>
- Auton, J. C., & Sturman, D. (2025). Persuasion under pressure: The influence of persuasion principles and time constraints on phishing email susceptibility. *Information & Computer Security*, 33(5), 845–859. <https://doi.org/10.1108/ICS-07-2024-0163>
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- Barnard, L., Lan, W. Y., To, Y. M., Paton, V. O., & Lai, S.-L. (2009). Measuring self-regulation in online and blended learning environments. *The Internet and Higher Education*, 12(1), 1–6. <https://doi.org/10.1016/j.iheduc.2008.10.005>
- Base44. (2026). Base44 [Computer software]. <https://base44.com>
- Baylor, A. L. (2011). The design of motivational agents and avatars. *Educational Technology Research and Development*, 59(2), 291–300. <https://doi.org/10.1007/s11423-011-9196-3>
- Blackmagic Design. (2026). DaVinci Resolve [Computer software]. <https://www.blackmagicdesign.com/products/davinciresolve>
- Boland, L., Campbell, D., Fazekas, M., Kitagawa, W., MacIver, L., Rzczkowska, K., & Gillanders, D. (2021). An experimental investigation of the effects of perspective-taking on emotional discomfort, cognitive fusion and self-compassion. *Journal of Contextual Behavioral Science*, 20, 27–34. <https://doi.org/10.1016/j.jcbs.2021.02.004>
- Bouiri, O., Lotfi, S., & Talbi, M. (2023). Metacognition & learning process: Using think-aloud protocol (TAP) to understand students and their teacher's reflection processes during a problem-solving situation. *The Education and Science Journal*, 25(5), 135–154. <https://doi.org/10.17853/1994-5639-2023-5-135-154>
- Broadbent, J., & Poon, W. L. (2015). Self-regulated learning strategies & academic achievement in online higher education learning environments: A systematic review. *The Internet and Higher Education*, 27, 1–13. <https://doi.org/10.1016/j.iheduc.2015.04.007>
- Bui, H. T. T., Amrita, K., & Nguyen, T. T. T. (2025). Exploring the impact of project-based learning with scamper and trello on creative thinking of engineering students. *European Journal of Engineering Education*, 50(5), 948–965. <https://doi.org/10.1080/03043797.2025.2474047>
- Canfield, C. I., Fischhoff, B., & Davis, A. (2019). Better beware: Comparing metacognition for phishing and legitimate emails. *Metacognition and Learning*, 14(3), 343–362. <https://doi.org/10.1007/s11409-019-09197-5>
- Canva. (2026). Canva [Computer software]. <https://www.canva.com>

- Cavanaugh, T. W., Lambkin, M. L., & Hu, H. (Helen). (2012). USING A GENERALIZED CHECKLIST TO IMPROVE STUDENT ASSIGNMENT SUBMISSION TIMES IN AN ONLINE COURSE. *Online Learning*, 16(4). <https://doi.org/10.24059/olj.v16i4.235>
- Çelik, T. İ., & Akay, C. (2025). The Impact of Brainstorming Technique on Academic Achievement and Creative Thinking: A Meta-Analysis Study. *SAGE Open*, 15(3), 21582440251378562. <https://doi.org/10.1177/21582440251378562>
- Chen, J.-L., Ma, Y.-W., & Huang, K.-L. (2020). Intelligent Visual Similarity-Based Phishing Websites Detection. *Symmetry*, 12(10), 1681. <https://doi.org/10.3390/sym12101681>
- Chen, X., Xie, H., Zou, D., & Hwang, G.-J. (2020). Application and theory gaps during the rise of Artificial Intelligence in Education. *Computers and Education: Artificial Intelligence*, 1, 100002. <https://doi.org/10.1016/j.caeai.2020.100002>
- Chi, M. T. H., & Wylie, R. (2014). The ICAP Framework: Linking Cognitive Engagement to Active Learning Outcomes. *Educational Psychologist*, 49(4), 219–243. <https://doi.org/10.1080/00461520.2014.965823>
- Chulan, M., Nayan, S., & Mohd Radzi, N. A. (2025). REFLECTIVE JOURNALING IN HIGHER EDUCATION: A CATALYST FOR HOLISTIC LEARNING AND TEACHING EXCELLENCE IN MALAYSIA. *International Journal of Modern Education*, 7(25), 238–248. <https://doi.org/10.35631/IJMOE.725017>
- Clark, J. M., & Paivio, A. (1987). A Dual Coding Perspective on Encoding Processes. In M. A. McDaniel & M. Pressley (Eds), *Imagery and Related Mnemonic Processes* (pp. 5–33). Springer New York. https://doi.org/10.1007/978-1-4612-4676-3_1
- Cochon Drouet, O., Lentillon-Kaestner, V., & Margas, N. (2023). Effects of the Jigsaw method on student educational outcomes: Systematic review and meta-analyses. *Frontiers in Psychology*, 14, 1216437. <https://doi.org/10.3389/fpsyg.2023.1216437>
- Coiro, J. (2011). Talking About Reading as Thinking: Modeling the Hidden Complexities of Online Reading Comprehension. *Theory Into Practice*, 50(2), 107–115. <https://doi.org/10.1080/00405841.2011.558435>
- Davar, N. F., Dewan, M. A. A., & Zhang, X. (2025). AI Chatbots in Education: Challenges and Opportunities. *Information*, 16(3), 235. <https://doi.org/10.3390/info16030235>
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, 54(8), 1–35. <https://doi.org/10.1145/3469886>
- Dharma, B. A., & Septiana, A. (2023). The Use of WIX as a Learning Media to Support Self-regulated Learning and Learning Activity. In D. T. Kurniawan & I. Zutiasari (Eds), *Proceedings of the BISTIC Business Innovation Sustainability and Technology International Conference (BISTIC 2022)* (Vol. 245, pp. 347–356). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-178-4_35
- Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53–67. <https://doi.org/10.1080/01611194.2019.1623343>
- Double, K. S. (2025). Survey measures of metacognitive monitoring are often false. *Behavior Research Methods*, 57(3), 97. <https://doi.org/10.3758/s13428-025-02621-6>
- Duraman, H., Shahrill, M., & Morsidi, N. (2015). Investigating the Effectiveness of Collaborative Learning in Using the Snowballing Effect Technique. *Asian Journal of Social Sciences & Humanities*, 4, 148–155.
- Esfandiari, M., & Knight, P. (2013). Using Pyramid Discussions in the Task-based Classroom to Extend Student Talking Time. *World Journal of English Language*, 3(3), p20. <https://doi.org/10.5430/wjel.v3n3p20>
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Evernote. (2026). Evernote [Computer software]. <https://evernote.com>
- Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, 125, 19–31. <https://doi.org/10.1016/j.ijhcs.2018.12.004>
- Fillout. (2026). Fillout [Computer software]. <https://www.fillout.com>
- Fink, M. C., Robinson, S. A., & Ertl, B. (2024). AI-based avatars are changing the way we learn and teach: Benefits and challenges. *Frontiers in Education*, 9, 1416307. <https://doi.org/10.3389/feduc.2024.1416307>

- Fredricks, J. A., Blumenfeld, P. C., & Paris, A. H. (2004). School Engagement: Potential of the Concept, State of the Evidence. *Review of Educational Research*, 74(1), 59–109. <https://doi.org/10.3102/00346543074001059>
- García-Senín, S., Arguedas, M., & Daradoumis, T. (2022). Using learning analytics to support STEAM students' academic achievement and self-regulated learning. *Research on Education and Media*, 14(1), 36–45. <https://doi.org/10.2478/rem-2022-0005>
- Garzón, J., Patiño, E., & Marulanda, C. (2025). Systematic Review of Artificial Intelligence in Education: Trends, Benefits, and Challenges. *Multimodal Technologies and Interaction*, 9(8), 84. <https://doi.org/10.3390/mti9080084>
- Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE*, 12(2), e0171620. <https://doi.org/10.1371/journal.pone.0171620>
- Gavrilas, L., & Kotsis, K. T. (2025). The evolution of STEM education and the transition to STEAM/STREAM. *Aquademia*, 9(1), ep25002. <https://doi.org/10.29333/aquademia/16313>
- Genially. (2026). *Genially* [Computer software]. <https://genial.ly>
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, 21(9), 3267. <https://doi.org/10.3390/s21093267>
- Geronimo, D. L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. <https://doi.org/10.1145/3313831.3376600>
- Gialamas, V. (2024). Στατιστικές μέθοδοι και τεχνικές στις κοινωνικές επιστήμες με τη χρήση SPSS. 300. <https://doi.org/10.57713/KALLIPOS-439>
- Google. (2026a). *Google AI Studio* [Computer software]. <https://aistudio.google.com>
- Google. (2026b). *Google Classroom* [Computer software]. <https://classroom.google.com>
- Google. (2026c). *Google Docs* [Computer software]. <https://docs.google.com>
- Google. (2026d). *Google Forms* [Computer software]. <https://forms.google.com>
- Google. (2026e). *NotebookLM* [Computer software]. <https://notebooklm.google>
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. <https://doi.org/10.1145/3173574.3174108>
- Guetterman, T. C., Fetter, M. D., & Creswell, J. W. (2015). Integrating Quantitative and Qualitative Results in Health Science Mixed Methods Research Through Joint Displays. *The Annals of Family Medicine*, 13(6), 554–561. <https://doi.org/10.1370/afm.1865>
- Güldal, H., & Dinçer, E. O. (2025). Can rule-based educational chatbots be an acceptable alternative for students in higher education? *Education and Information Technologies*, 30(3), 3979–4012. <https://doi.org/10.1007/s10639-024-12977-5>
- Hall, L., Paracha, S., Hagan-Green, G., Ure, C., & Jackman, P. (2022). Cyber Eyes Wide Open: Creative Collaboration between Artists, Academics & Cyber Security Practitioners. 35th International BCS Human-Computer Interaction Conference. <https://doi.org/10.14236/ewic/HCI2022.15>
- Halverson, L. R., & Graham, C. R. (2019). Learner Engagement in Blended Learning Environments: A Conceptual Framework. *Online Learning*, 23(2). <https://doi.org/10.24059/olj.v23i2.1481>
- Händel, M., Naujoks-Schober, N., & Dresel, M. (2023). Metacognitive Monitoring via Strategies and Judgments: Different Phases, Different Objects. *Zeitschrift Für Entwicklungspsychologie Und Pädagogische Psychologie*, 55(2–3), 67–76. <https://doi.org/10.1026/0049-8637/a000273>
- Harriss, L., McGill, I., Gray, E., Jaiswal, A., & Aggrawal, S. (2025). Assessing and Characterizing Perspective-Taking Abilities in Undergraduate Students: A Case Study Approach. 2025 ASEE Annual Conference & Exposition Proceedings, 55466. <https://doi.org/10.18260/1-2--55466>
- Hedra. (2026). *Hedra* [Computer software]. <https://www.hedra.com>

- Hesse, F., Care, E., Buder, J., Sassenberg, K., & Griffin, P. (2015). A Framework for Teachable Collaborative Problem Solving Skills. In P. Griffin & E. Care (Eds), *Assessment and Teaching of 21st Century Skills* (pp. 37–56). Springer Netherlands. https://doi.org/10.1007/978-94-017-9395-7_2
- Hobert, S., Følstad, A., & Law, E. L.-C. (2023). Chatbots for active learning: A case of phishing email identification. *International Journal of Human-Computer Studies*, 179, 103108. <https://doi.org/10.1016/j.ijhcs.2023.103108>
- Hutchings, R. J., Simpson, A. J., Sherman, J. W., & Todd, A. R. (2021). Perspective taking reduces intergroup bias in visual representations of faces. *Cognition*, 214, 104808. <https://doi.org/10.1016/j.cognition.2021.104808>
- IBM. (2026). *IBM SPSS Statistics* [Computer software]. <https://www.ibm.com/spss>
- Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1), 8. <https://doi.org/10.1186/s13673-016-0065-2>
- Jacob, T., & Centofanti, S. (2024). Effectiveness of H5P in improving student learning outcomes in an online tertiary education setting. *Journal of Computing in Higher Education*, 36(2), 469–485. <https://doi.org/10.1007/s12528-023-09361-6>
- Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10(1), 33. <https://doi.org/10.1186/s13673-020-00237-7>
- Johnson, D. W., & Johnson, R. T. (2009). An Educational Psychology Success Story: Social Interdependence Theory and Cooperative Learning. *Educational Researcher*, 38(5), 365–379. <https://doi.org/10.3102/0013189X09339057>
- K.C, A., & Aravind, S. (2024). Integrating Google AI: Enhancing Library Services for the Digital Age. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4927222>
- Kekeba, S. K., Gure, A., & Olkaba, T. T. (2024). Effect of Computer Simulation Integrated with Jigsaw Learning Strategy on Students' Attitudes towards Learning Chemistry. *Open Education Studies*, 6(1), 20240052. <https://doi.org/10.1515/edu-2024-0052>
- Kenneth, A., Hayashi, B. B., Lionardi, J., Richie, S., Achmad, S., Junior, F. A., & Nadia. (2023). Phishing Attack Awareness Among College Students. 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), 344–348. <https://doi.org/10.1109/ICE3IS59323.2023.10335412>
- Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. *Information*, 12(10), 417. <https://doi.org/10.3390/info12100417>
- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 905–914. <https://doi.org/10.1145/1240624.1240760>
- Lakens, D. (2013). Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. *Frontiers in Psychology*, 4. <https://doi.org/10.3389/fpsyg.2013.00863>
- Leijenaar, E. L., Milota, M. M., Van Delden, J. J. M., & Van Royen–Kerkhof, A. (2025). Measurement instruments for perspective-taking: BEME Review No. 91. *Medical Teacher*, 47(6), 934–942. <https://doi.org/10.1080/0142159X.2024.2412140>
- López Carrillo, M. D., Calonge García, A., & Lebrón Moreno, J. A. (2024). Self-Regulation of Student Learning in a STEAM Project. *Education Sciences*, 14(6), 579. <https://doi.org/10.3390/educsci14060579>
- Lovable. (2026). *Lovable* [Computer software]. <https://lovable.dev>
- Lucidchart. (2026). *Lucidchart* [Computer software]. <https://lucid.co/lucidchart>
- Lumi. (2026). *Lumi* [Computer software]. <https://lumi.education>
- Luo, R., & Zhou, Y. (2024). The effectiveness of self-regulated learning strategies in higher education blended learning: A five years systematic review. *Journal of Computer Assisted Learning*, 40(6), 3005–3029. <https://doi.org/10.1111/jcal.13052>
- Luse, A., & Burkman, J. (2021). Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering. *Journal of Cybersecurity Education, Research and Practice*, 2020(2). <https://doi.org/10.62915/2472-2707.1072>

- Madiah, M., Ng, K. X., Tan, Y. W., Tan, Z. H., Chong, Z. T., & Chan, J. X. (2024). Wix for Web Development and the Application of the Waterfall Model and Project Based Learning for Project Completion: A Case Study. *Journal of Informatics and Web Engineering*, 3(2), 212. <https://doi.org/10.33093/jiwe.2024.3.2.16>
- Manathunga, K., & Hernández-Leo, D. (2018). Authoring and enactment of mobile pyramid-based collaborative learning activities. *British Journal of Educational Technology*, 49(2), 262–275. <https://doi.org/10.1111/bjet.12588>
- Marôco, J. (2026). The University Student Engagement Inventory (USEI). *Encyclopedia*, 6(8), 166. <https://doi.org/10.3390/encyclopedia6080166>
- Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security*, 139, 103695. <https://doi.org/10.1016/j.cose.2023.103695>
- Martins, L., Fernández-Ferrer, M., & Puertas, E. (2024). Analysing Conversation Pathways with a Chatbot Tutor to Enhance Self-Regulation in Higher Education. *Education Sciences*, 14(6), 590. <https://doi.org/10.3390/educsci14060590>
- Meelu, P., & Malik, S. (2010). RSA and its Correctness through Modular Arithmetic. 463–466. <https://doi.org/10.1063/1.3526259>
- Mentimeter. (2026). Mentimeter [Computer software]. <https://www.mentimeter.com>
- Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, 11, 1755. <https://doi.org/10.3389/fpsyg.2020.01755>
- Morić, Z., Dakić, V., Plečać, M., & Ogrizek Biškupić, I. (2025). Evaluating End-User Defensive Approaches Against Phishing Using Education and Simulated Attacks in a Croatian University. *Journal of Cybersecurity and Privacy*, 5(3), 38. <https://doi.org/10.3390/jcp5030038>
- Mouw, J., Saab, N., Gijlers, H., Hickendorff, M., Van Paridon, Y., & Van Den Broek, P. (2020). The differential effect of perspective-taking ability on profiles of cooperative behaviours and learning outcomes. *Frontline Learning Research*, 8(6), 88–113. <https://doi.org/10.14786/flr.v8i6.633>
- Mundelsee, L., & Jurkowski, S. (2021). Think and pair before share: Effects of collaboration on students' in-class participation. *Learning and Individual Differences*, 88, 102015. <https://doi.org/10.1016/j.lindif.2021.102015>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1), 1609406917733847. <https://doi.org/10.1177/1609406917733847>
- OpenAI. (2026). ChatGPT (ChatGPT Images 2.0) [Computer software]. <https://chatgpt.com>
- Padlet. (2026). Padlet [Computer software]. <https://padlet.com>
- Panadero, E. (2017). A Review of Self-regulated Learning: Six Models and Four Directions for Research. *Frontiers in Psychology*, 8, 422. <https://doi.org/10.3389/fpsyg.2017.00422>
- Panda, P., Mishra, A. K., & Puthal, D. (2022). A Novel Logo Identification Technique for Logo-Based Phishing Detection in Cyber-Physical Systems. *Future Internet*, 14(8), 241. <https://doi.org/10.3390/fi14080241>
- Perignat, E., & Katz-Buonincontro, J. (2019). STEAM in practice and research: An integrative literature review. *Thinking Skills and Creativity*, 31, 31–43. <https://doi.org/10.1016/j.tsc.2018.10.002>
- Pintrich, P. R. (2000). The Role of Goal Orientation in Self-Regulated Learning. In *Handbook of Self-Regulation* (pp. 451–502). Elsevier. <https://doi.org/10.1016/B978-012109890-2/50043-3>
- Pixabay. (2026). Pixabay. <https://pixabay.com/service/license-summary/>
- Quigley, C. F., Herro, D., & Jamil, F. M. (2017). Developing a Conceptual Model of STEAM Teaching Practices. *School Science and Mathematics*, 117(1–2), 1–12. <https://doi.org/10.1111/ssm.12201>
- Rawson, K. A., Thomas, R. C., & Jacoby, L. L. (2015). The Power of Examples: Illustrative Examples Enhance Conceptual Learning of Declarative Concepts. *Educational Psychology Review*, 27(3), 483–504. <https://doi.org/10.1007/s10648-014-9273-3>
- Redmond, P., Heffernan, A., Abawi, L., Brown, A., & Henderson, R. (2018). An Online Engagement Framework for Higher Education. *Online Learning*, 22(1). <https://doi.org/10.24059/olj.v22i1.1175>
- Reyna, J. (2025). *The Potential of Google NotebookLM for Teaching and Learning*.

- Rietveld, T., & Van Hout, R. (2017). The paired t test and beyond: Recommendations for testing the central tendencies of two paired samples in research on speech, language and hearing pathology. *Journal of Communication Disorders*, 69, 44–57. <https://doi.org/10.1016/j.jcomdis.2017.07.002>
- Roediger, H. L., & Karpicke, J. D. (2006). The Power of Testing Memory: Basic Research and Implications for Educational Practice. *Perspectives on Psychological Science*, 1(3), 181–210. <https://doi.org/10.1111/j.1745-6916.2006.00012.x>
- Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345–357. <https://doi.org/10.1016/j.eswa.2018.09.029>
- Salazar Campo, M., & Lant, T. K. (2025). Perspective integration capability: A valid and reliable measurement instrument for assessing knowledge integration readiness in interdisciplinary collaborations. *Journal of Clinical and Translational Science*, 9(1), e93. <https://doi.org/10.1017/cts.2025.54>
- Seban, P., Sikl, R., & Urban, K. (2025). Relationship between monitoring judgments and self-report measures of metacognition in educational research. *International Journal of Educational Research*, 131, 102578. <https://doi.org/10.1016/j.ijer.2025.102578>
- Sembert, P. J., Vermette, P. J., Lyman, F., Bardsley, M. E., & Snell, C. (2021). Think-Pair-Share as a Springboard for Study Buddies in a Virtual Environment. *Excelsior: Leadership in Teaching and Learning*, 14(1). <https://doi.org/10.14305/jn.19440413.2021.14.1.04>
- Serrat, O. (2017). The SCAMPER Technique. In O. Serrat, *Knowledge Solutions* (pp. 311–314). Springer Singapore. https://doi.org/10.1007/978-981-10-0983-9_33
- Sha, J., Shu, H., & Kan, Z. (2021). Analysis of Critical Thinking Path of College Students Under STEAM Course. *Frontiers in Psychology*, 12, 723185. <https://doi.org/10.3389/fpsyg.2021.723185>
- Shi, Y., Chen, M., Wei, Y., Shen, J., Wu, M., & Zhu, K. (2025). Understanding effects of engaging online learning environments on students' cognitive engagement and well-being: The role of academic self-concept and flow. *Frontiers in Psychology*, 16, 1614109. <https://doi.org/10.3389/fpsyg.2025.1614109>
- Shi, Y., Dong, Q., Wei, Y., & Zhu, K. (2026). Cognitive Engagement in Online Learning Environments: A Systematic Review and Future Research. *Journal of Computer Assisted Learning*, 42(3), e70240. <https://doi.org/10.1002/jcal.70240>
- Siddiq, F., Scherer, R., & Tondeur, J. (2016). Teachers' emphasis on developing students' digital information and communication skills (TEDDICS): A new construct in 21st century education. *Computers & Education*, 92–93, 1–14. <https://doi.org/10.1016/j.compedu.2015.10.006>
- Smeda, N., Dakich, E., & Sharda, N. (2014). The effectiveness of digital storytelling in the classrooms: A comprehensive study. *Smart Learning Environments*, 1(1), 6. <https://doi.org/10.1186/s40561-014-0006-3>
- Sokolova, E. V., Blaginin, V. A., & Shatrova, A. Y. (2025). Evolution and Current Trends in STEM Education: A Retrospective and Bibliometric Analysis. *Journal of Hypermedia & Technology-Enhanced Learning*, 3(1), 90–107. <https://doi.org/10.58536/j-hytel.169>
- Spencer, A. (2024). Cyber Science Education within STEM. *Cybersecurity and Innovative Technology Journal*, 2(2), 67–78. <https://doi.org/10.53889/citj.v2i2.330>
- Tian, J. (2025). Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review. *Education Sciences*, 15(11), 1540. <https://doi.org/10.3390/educsci15111540>
- Trello. (2026). *Trello* [Computer software]. <https://trello.com>
- Uzun, Y., Suraworachet, W., Zhou, Q., Gauthier, A., & Cukurova, M. (2025). Engagement with analytics feedback and its relationship to self-regulated learning competence and course performance. *International Journal of Educational Technology in Higher Education*, 22(1), 17. <https://doi.org/10.1186/s41239-025-00515-3>
- Vaassen, C. E., Van Den Broek, T. A., Aldering, H., & Beersma, B. (2026). Increasing empathy and perspective-taking in controversial discussions: A systematic review and future research directions. *Computers in Human Behavior Reports*, 22, 101062. <https://doi.org/10.1016/j.chbr.2026.101062>

- Van Laar, E., Van Deursen, A. J. A. M., Van Dijk, J. A. G. M., & De Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, 72, 577–588. <https://doi.org/10.1016/j.chb.2017.03.010>
- Voogt, J., & Roblin, N. P. (2012). A comparative analysis of international frameworks for 21st century competences: Implications for national curriculum policies. *Journal of Curriculum Studies*, 44(3), 299–321. <https://doi.org/10.1080/00220272.2012.668938>
- Wagener, B. (2016). Metacognitive Monitoring and Academic Performance in College. *College Teaching*, 64(2), 47–54. <https://doi.org/10.1080/87567555.2015.1116056>
- Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks. *Sage Open*, 13(4), 21582440231217720. <https://doi.org/10.1177/21582440231217720>
- Winter, M., Mordel, J., Mendzheritskaya, J., Biedermann, D., Ciordas-Hertel, G.-P., Hahnel, C., Bengs, D., Wolter, I., Goldhammer, F., Drachsler, H., Artelt, C., & Horz, H. (2024). Behavioral trace data in an online learning environment as indicators of learning engagement in university students. *Frontiers in Psychology*, 15, 1396881. <https://doi.org/10.3389/fpsyg.2024.1396881>
- Wood, D., Bruner, J. S., & Ross, G. (1976). THE ROLE OF TUTORING IN PROBLEM SOLVING*. *Journal of Child Psychology and Psychiatry*, 17(2), 89–100. <https://doi.org/10.1111/j.1469-7610.1976.tb00381.x>
- Xue, Y., & Khalid, F. (2026). Investigating the impact of metacognitive regulation on students' academic performance: A quantitative study of Chinese distance learners. *Frontiers in Psychology*, 17, 1726956. <https://doi.org/10.3389/fpsyg.2026.1726956>
- Yakman, G. (2008). *STEAM Education: An overview of creating a model of integrative education*.
- Yulianti, E., Suwono, H., Abd Rahman, N. F., & Phang, F. A. (2024). State-of-the-Art of STEAM Education in Science Classrooms: A Systematic Literature Review. *Open Education Studies*, 6(1), 20240032. <https://doi.org/10.1515/edu-2024-0032>
- Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education*, 16(1), 39. <https://doi.org/10.1186/s41239-019-0171-0>
- Zimmerman, B. J. (1989). A social cognitive view of self-regulated academic learning. *Journal of Educational Psychology*, 81(3), 329–339. <https://doi.org/10.1037/0022-0663.81.3.329>
- Zimmerman, B. J. (2002). Becoming a Self-Regulated Learner: An Overview. *Theory Into Practice*, 41(2), 64–70. https://doi.org/10.1207/s15430421tip4102_2
- Zimmerman, B. J., & Moylan, A. (2009). Self-regulation: Where metacognition and motivation intersect. *Handbook of Metacognition in Education*, 299–315.

ΠΑΡΑΡΤΗΜΑ

Α1: Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων (Φάση Forethought).

Αρχική Φόρμα Αυτοαξιολόγησης Γνώσεων για το Phishing

Παρακαλώ συμπληρώστε την παρακάτω φόρμα για να αξιολογήσετε τις τρέχουσες γνώσεις σας σχετικά με τις επιθέσεις phishing.

1. Γνωρίζω τι σημαίνει ο όρος «phishing».

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

2. Μπορώ να αναγνωρίσω ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

3. Μπορώ να εντοπίσω ύποπτους συνδέσμους σε ένα ψηφιακό μήνυμα.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

4. Γνωρίζω ότι οι επιθέσεις phishing μπορεί να στοχεύουν προσωπικές πληροφορίες, όπως στοιχεία σύνδεσης ή οικονομικά δεδομένα.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

5. Μπορώ να αναγνωρίσω πότε ένα μήνυμα προσπαθεί να δημιουργήσει αίσθηση πίεσης ή επείγοντος.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

6. Γνωρίζω ότι το phishing μπορεί να εμφανιστεί μέσα από διαφορετικά μέσα, όπως email, SMS/MMS, φωνητική επικοινωνία ή διαδίκτυο.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

7. Γνωρίζω βασικές μορφές phishing, όπως smishing, vishing ή spear phishing.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

8. Αισθάνομαι ικανός/ή να αξιολογήσω αν ένα ψηφιακό μήνυμα είναι αξιόπιστο ή ύποπτο.

Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
☐	☐	☐	☐	☐

1 - Διαφωνώ απόλυτα

5 - Συμφωνώ απόλυτα

9. Ποιο θέμα σχετικά με το phishing θα ήθελες να κατανοήσεις καλύτερα μέσα από το e-course;

Google Φόρμες

Skills Self-Check (Pre)

Το ερωτηματολόγιο αποτυπώνει το αρχικό σας επίπεδο σε τρεις δεξιότητες: ανάλυση καταστάσεων, παρακολούθηση μαθησιακής πορείας και συνεργασία. Απαντήστε με ειλικρίνεια.

* Υποδεικνύει απαιτούμενη ερώτηση

1. **Ενότητα Α - Γνωστική Εμπλοκή:** Όταν εξετάζω ένα ύποπτο μήνυμα, αναλύω προσεκτικά τα επιμέρους στοιχεία του.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

2. **Ενότητα Α - Γνωστική Εμπλοκή:** Αξιολογώ την επικινδυνότητα μιας κατάστασης πριν αποφασίσω πώς θα ενεργήσω.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

3. **Ενότητα Α - Γνωστική Εμπλοκή:** Μπορώ να αιτιολογήσω τις αποφάσεις μου με βάση συγκεκριμένα στοιχεία.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

4. **Ενότητα Α - Γνωστική Εμπλοκή:** Νιώθω άνετα να δημιουργώ διαγράμματα ή γραφήματα για να παρουσιάσω μια ιδέα.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

5. **Ενότητα Β - Μεταγνωστική Παρακολούθηση:** Παρακολουθώ συστηματικά τη δική μου μαθησιακή πορεία.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

6. **Ενότητα Β - Μεταγνωστική Παρακολούθηση:** Αναγνωρίζω εύκολα τα σημεία που χρειάζομαι βελτίωση.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

7. **Ενότητα Β - Μεταγνωστική Παρακολούθηση:** Όταν μια στρατηγική δεν αποδίδει, την αλλάζω.
Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

8. **Ενότητα Β - Μεταγνωστική Παρακολούθηση:** Αναστοχάζομαι πάνω στις ενέργειες και τις αποφάσεις μου.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

9. **Ενότητα Γ - Κατανόηση Οπτικής Άλλων:** Ακούω προσεκτικά τις απόψεις των συνεργατών μου πριν διαμορφώσω τη δική μου γνώμη.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

10. **Ενότητα Γ - Κατανόηση Οπτικής Άλλων:** Αναγνωρίζω ότι οι συνεργάτες μου μπορεί να έχουν διαφορετική πληροφορία ή εμπειρία από εμένα.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

11. **Ενότητα Γ - Κατανόηση Οπτικής Άλλων:** Συγκρίνω τη δική μου ερμηνεία με αυτή των άλλων μελών της ομάδας.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου ☐ ☐ ☐ ☐ ☐ Πάρα πολύ

12. **Ενότητα Γ - Κατανόηση Οπτικής Άλλων:** Ενσωματώνω χρήσιμες ιδέες των συνεργατών μου στην τελική λύση.

*

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου

☐ ☐ ☐ ☐ ☐

Πάρα πολύ

Google Φόρμες

Ετεροαξιολόγηση Τεχνικού Διαγράμματος – Sequence Diagram

Η παρούσα φόρμα προορίζεται για την ετεροαξιολόγηση των Sequence Diagrams των ομάδων.
Παρακαλώ αξιολογήστε το διάγραμμα της άλλης ομάδας με βάση τα παρακάτω κριτήρια.

1. Στοιχεία Αξιολόγησης

2. Το διάγραμμα απεικονίζει με σαφήνεια τα βήματα της τεχνικής υποδομής (καταχώρηση domain, server, mail routing) πριν από την αποστολή του email.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Διαφωνώ απόλυτα

☐ ☐ ☐ ☐ ☐

Συμφωνώ απόλυτα

3. Το διάγραμμα περιλαμβάνει σωστά τις παραμέτρους ρύθμισης του phishing email (αποστολέας, θέμα, παραπλανητικός σύνδεσμος).

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Διαφωνώ απόλυτα

☐ ☐ ☐ ☐ ☐

Συμφωνώ απόλυτα

4. Το διάγραμμα απεικονίζει τη δημιουργία και τον ρόλο της ψεύτικης σελίδας σύνδεσης.

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

5. Το διάγραμμα δείχνει με σωστή σειρά τα τρία στάδια ευπάθειας του θύματος (άνοιγμα email, κλικ στον σύνδεσμο, υποβολή στοιχείων).

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

6. Το διάγραμμα απεικονίζει την τελική καταγραφή αποτελεσμάτων/μετρικών.

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

7. Τα βέλη του διαγράμματος δείχνουν με σαφήνεια ποιος στέλνει τι σε ποιον (επιτιθέμενος, σύστημα, θύμα).

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

8. Το διάγραμμα στο σύνολό του είναι τεχνικά ακριβές και ανταποκρίνεται σε όσα παρουσιάστηκαν στην προσομοίωση.

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Διαφωνώ απόλυτα

☐ ☐ ☐ ☐ ☐

Συμφωνώ απόλυτα

9. Σχόλια / Προτάσεις βελτίωσης

Google Φόρμες

Ετεροαξιολόγηση Γραφιστικών

Φόρμα αξιολόγησης των mockups για την εκπαιδευτική δραστηριότητα αναγνώρισης τεχνικών phishing.

1. Ονοματεπώνυμο συμμαθητή που αξιολογείται

2. Ποιο γραφιστικό κόλπο phishing εντοπίζετε στο σχέδιο;

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ Παραποιημένο λογότυπο και χρώματα
- ☐ Ψεύτικο χρονόμετρο (countdown)
- ☐ Στιγμιότυπο ιστοσελίδας ως φόντο
- ☐ Ψευδής ιεράρχηση πληροφοριών

3. Πόσο πειστικό θεωρείτε ότι είναι το σχέδιο ως μήνυμα phishing;

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου πειστικό

☐ ☐ ☐ ☐ ☐

Πολύ πειστικό

4. Τι θα μπορούσε να βελτιώσει ο συμμαθητής στο σχέδιό του για να το κάνει πιο πειστικό;

5. Τι θεωρείτε ότι έκανε ιδιαίτερα καλά στον σχεδιασμό της μακέτας;

Google Φόρμες

Ετεροαξιολόγηση Γραφημάτων SPSS

Ετεροαξιολόγηση Γραφημάτων SPSS

Αξιολόγησε τα γραφήματα ενός συμφοιτητή/τριας σου, βασισμένα στα δεδομένα του ερωτηματολογίου phishing. Η αξιολόγηση είναι ανώνυμη.

1. Όνομα αξιολογούμενου/ης

2. Ανέβασε ή επικόλλησε link προς το αρχείο με τα γραφήματα

3. Ιστόγραμμα ηλικίας - Το γράφημα είναι τεχνικά ορθό (σωστός τύπος γραφήματος, σωστές τιμές, σωστές ετικέτες αξόνων)

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου

☐ ☐ ☐ ☐ ☐

Πλήρως

4. Ιστόγραμμα ηλικίας - Το γράφημα παρουσιάζεται με σαφήνεια (τίτλος, ευανάγνωστο, κατανοητό με την πρώτη ματιά)

Να επισημαίνεται μόνο μία έλλειψη.

1 2 3 4 5

Καθόλου

☐ ☐ ☐ ☐ ☐

Πλήρως

5. Ιστόγραμμα ηλικίας - Ο τύπος γραφήματος που επιλέχθηκε ταιριάζει με το είδος των δεδομένων που παρουσιάζει

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

6. Γράφημα πίτας φύλου - Το γράφημα είναι τεχνικά ορθό (σωστός τύπος γραφήματος, σωστές τιμές, σωστές ετικέτες αξόνων)

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

7. Γράφημα πίτας φύλου - Το γράφημα παρουσιάζεται με σαφήνεια (τίτλος, ευανάγνωστο, κατανοητό με την πρώτη ματιά)

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

8. Γράφημα πίτας φύλου - Ο τύπος γραφήματος που επιλέχθηκε ταιριάζει με το είδος των δεδομένων που παρουσιάζει

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

9. Συγκριτικό γράφημα - Το γράφημα είναι τεχνικά ορθό (σωστός τύπος γραφήματος, σωστές τιμές, σωστές ετικέτες αξόνων)

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

10. Συγκριτικό γράφημα - Το γράφημα παρουσιάζεται με σαφήνεια (τίτλος, ευανάγνωστο, κατανοητό με την πρώτη ματιά)

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

11. Συγκριτικό γράφημα - Ο τύπος γραφήματος που επιλέχθηκε ταιριάζει με το είδος των δεδομένων που παρουσιάζει

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Καθόλου	☐	☐	☐	☐	☐	Πλήρως

12. Σχόλια ή προτάσεις βελτίωσης

Ερωτηματολόγιο Αναστοχασμού

1. Αξιολογώ την τελική μου επίδοση με βάση τα δικά μου κριτήρια επιτυχίας.
Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

2. Μπορώ να εξηγήσω σε τι οφείλεται το αποτέλεσμα που πέτυχα, είτε θετικό είτε αρνητικό.
Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

3. Αισθάνομαι ικανοποιημένος ή ικανοποιημένη με την πορεία που ακολούθησα.
Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

4. Σκέφτομαι ήδη πώς θα τροποποιούσα τις στρατηγικές μου για να μάθω πιο αποτελεσματικά στο μέλλον.

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	☐	☐	☐	☐	☐	Συμφωνώ απόλυτα

5. Ποια στιγμή της πορείας σου θυμάσαι πιο έντονα, και γιατί;

Google Φόρμες

Α7: Ερωτηματολόγιο Αξιολόγησης σχεδίου δράσης (Φάση Self-Reflection).

Αξιολόγηση Εκπαιδευτικού Σχεδίου Δράσης

Παρακαλούμε αξιολογήστε την υλοποίηση του εκπαιδευτικού σχεδίου δράσης. Η απάντησή σας είναι σημαντική για τη βελτίωση μελλοντικών παρεμβάσεων.

1. ΑΞΟΝΑΣ Α: ΠΕΡΙΕΧΟΜΕΝΟ

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Διαφωνώ απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ/ Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ απόλυτα (5)
Το γνωστικό αντικείμενο του σχεδίου δράσης ήταν συναφές με τους μαθησιακούς στόχους.	☐	☐	☐	☐	☐
Η σαφήνεια των παρουσιαζόμενων εννοιών διευκόλυνε την κατανόηση του γνωστικού αντικειμένου.	☐	☐	☐	☐	☐
Ο βαθμός δυσκολίας του περιεχομένου ήταν κατάλληλος για το επίπεδο των φοιτητών.	☐	☐	☐	☐	☐
Το περιεχόμενο του σχεδίου δράσης προσέφερε ερεθίσματα για περαιτέρω ακαδημαϊκή διερεύνηση.	☐	☐	☐	☐	☐
Η θεματική του σχεδίου δράσης προκάλεσε αυξημένο γνωστικό ενδιαφέρον.	☐	☐	☐	☐	☐

2. ΑΞΟΝΑΣ Β: ΔΙΑΔΙΚΑΣΙΑ ΥΛΟΠΟΙΗΣΗΣ

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Διαφωνώ απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ/ Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ απόλυτα (5)
Η δομή και η οργάνωση των μαθημάτων συνέβαλε στη συστηματική προσέγγιση του θέματος.	☐	☐	☐	☐	☐
Η διαχείριση του διαθέσιμου διδακτικού χρόνου ήταν αποτελεσματική για την ολοκλήρωση των δραστηριοτήτων.	☐	☐	☐	☐	☐
Η εφαρμοζόμενη διδασκική μεθοδολογία (π.χ. ομαδοσυνεργατική, διερευνητική) ήταν ενδεδειγμένη.	☐	☐	☐	☐	☐
Η ανατροφοδότηση από τον εκπαιδευτικό ήταν σαφής και υποστηρικτική της μαθησιακής διαδικασίας.	☐	☐	☐	☐	☐
Οι ευκαιρίες για ενεργό συμμετοχή και διάδραση ήταν ικανοποιητικές.	☐	☐	☐	☐	☐

3. ΑΞΟΝΑΣ Γ: ΠΡΟΪΟΝ ΚΑΙ ΕΡΓΑΛΕΙΑ

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Διαφωνώ απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ/ Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ απόλυτα (5)
Η ποιότητα των παραδοτέων εργασιών αντανακλά την επίτευξη των μαθησιακών αποτελεσμάτων.	☐	☐	☐	☐	☐
Η διαδικασία υλοποίησης των τελικών παραδοτέων ήταν σαφώς καθορισμένη.	☐	☐	☐	☐	☐
Η χρήση των ψηφιακών εργαλείων (π.χ. λογισμικά, πλατφόρμες) ενίσχυσε τη μαθησιακή εμπειρία.	☐	☐	☐	☐	☐
Τα χρησιμοποιούμενα εργαλεία ήταν λειτουργικά και υποστήριξαν την υλοποίηση του σχεδίου.	☐	☐	☐	☐	☐
Τα τελικά παραδοτέα του σχεδίου δράσης έχουν πρακτική ή ακαδημαϊκή αξία.	☐	☐	☐	☐	☐

4. ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ

Google Φόρμες

A8: Ρουμπρίκα αξιολόγησης παραδοτέων (Google Classroom).

Τεχνική Ορθότητα

Εξαιρετικό 4 βαθμοί

Όλα τα στοιχεία τεχνικά ακριβή και δικαιολογημένα.

Πολύ καλό 3 βαθμοί

Τα περισσότερα στοιχεία σωστά, με μικρές ανακρίβειες.

Επαρκές 2 βαθμοί

Βασική κατανόηση, με αρκετές ανακρίβειες

Χρειάζεται βελ... 1 βαθμός

Εμφανείς τεχνικές ασυνέπειες

Σαφήνεια Παρουσίασης

Εξαιρετικό 4 βαθμοί

Καθαρό, εύκολα κατανοητό, καλά οργανωμένο

Πολύ καλό 3 βαθμοί

Κατανοητό, με μικρές ασάφειες

Επαρκές 2 βαθμοί

Απαιτεί προσπάθεια για κατανόηση

Χρειάζεται βελ... 1 βαθμός

Ελλιπές

A9: Checklist (Ενότητα Mathematics-Φάση Performance).



Checklist της Πρακτικής Μελέτης

Mission V: Μαθηματικά της Ψηφιακής Απάτης

Ξεκίνα



Checklist

1. Υπολογισμοί

Υπολογισμοί

- ☐ Υπολόγισα το Ποσοστό Κλικ
- ☐ Υπολόγισα το Ποσοστό Επιτυχίας

2. Επιλογή Γραφήματος

Επιλογή Γραφήματος

- ☐ Επέλεξα το καταλληλότερο γράφημα
- ☐ Αιτιολόγησα την επιλογή μου

3. Κρυπτογραφία RSA

Κρυπτογραφία RSA

- ☐ Μελέτησα τη θεωρία του RSA
- ☐ Κατανόησα τον τρόπο δημιουργίας ενός κλειδιού RSA

4. Τελική Άσκηση

Τελική Άσκηση

- ☐ Ολοκλήρωσα την πρακτική μελέτη

Submit

Made with Fillout

Σύνδεσμος e-course : <https://gkonstantakis.wixstudio.com/education>