ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ - WEBINTELLIGENCE

Ανάπτυξη πλαισίου επαγρύπνησης κυβερνοασφάλειας σε σχολικό πληθυσμό

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΝΑΓΙΩΤΙΔΗ ΣΩΤΗΡΙΟΥ (ΑΜ 142021)

Επιβλέπων : ΧΡΗΣΤΟΣ ΗΛΙΟΥΔΗΣ
Καθηγητής, ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Σεπτέμβριος 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Υπόδειγμα φύλλου τίτλου (μπροστινή σελίδα) του αντιτύπου ΜΔΕ

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Ανάπτυξη πλαισίου επαγρύπνησης κυβερνοασφάλειας σε σχολικό πληθυσμό

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΝΑΓΙΩΤΙΔΗ ΣΩΤΗΡΙΟΥ (ΑΜ 142021)

Επιβλέπων : ΧΡΗΣΤΟΣ ΗΛΙΟΥΔΗΣ
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις Choose a date.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Όνομα Επώνυμο	Όνομα Επώνυμο	'Ονομα Επώνυμο
Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Choose a date

(Υπογραφή)

.....

Click here to enter text.

Click here to enter text.

Περίληψη

Η αλόγιστη χρήση κοινωνικών δικτύων από μεγάλο μέρος μαθητών και οι διερευνώμενες επιπτώσεις της στην ψυχική τους υγεία, έχει προκαλέσει ιδιαίτερη ανησυχία σε οικογένεια, σχολείο και κράτος. Ιδιαίτερα σημαντικοί είναι οι κίνδυνοι που διατρέχουν από δημοσιεύσεις και διαδικτυακές συναναστροφές σε αυτά. Η διπλωματική στοχεύει να βοηθήσει στην ευαισθητοποίηση μαθητών στην κυβερνοασφάλεια καθώς αντιμετωπίζουν καταστάσεις χωρίς προηγούμενες εμπειρίες.

Δημιουργήθηκε πλαίσιο επαγρύπνησης στην κυβερνοασφάλεια και αξιολογήθηκε με έρευνα που πραγματοποιήθηκε με 56 μαθητές της Α’ τάξης Λυκείου. Για την έρευνα χρησιμοποιήθηκαν τα εξής εργαλεία: ως σύστημα διαχείρισης μαθημάτων το Wordpress, για τη δημιουργία διαδραστικού βίντεο μαθήματος το πρόσθετο της H5P και τέλος, το πρόσθετο SNORDIAN's H5PxAPIkatchu για συλλογή αναλυτικών πληροφοριών κατά την εκτέλεση του μαθήματος προκειμένου να γίνει η αξιολόγηση της έρευνας. Το μάθημα αποτελούνταν από δύο φάσεις και μία ολιγόλεπτη ενδιάμεση διδακτική παρέμβαση με πληροφορίες αρχαρίου χρήστη OSINT. Το βίντεο του μαθήματος, αποτελούνταν από φωτογραφίες που δημιουργήθηκαν από το DALL-E 2 της OpenAI.

Τα αποτελέσματα έδειξαν ότι στην Β’ Φάση του μαθήματος υπήρξε βελτίωση της βαθμολογίας των χρηστών και του χρόνου που δόθηκαν απαντήσεις σε σχέση με την Α’ Φάση.

Λέξεις Κλειδιά: Πλαίσιο, Κυβερνοασφάλεια, Επαγρύπνηση, Ευαισθητοποίηση, Μαθητές, H5P, Διαδραστικό υλικό, Καλές πρακτικές

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

The excessive use of social media by a large number of students and its investigated impact on their mental health has raised considerable concern among families, schools, and the state. Particularly noteworthy are the risks they face from postings and online interactions on these platforms. This thesis aims to assist in raising students' awareness of cybersecurity as they navigate unprecedented situations.

A cybersecurity vigilance framework was developed and evaluated through a survey of 56 high school freshmen. For the research, the following tools were used: WordPress as a course management system, the H5P plugin for creating interactive video lessons, and the SNORDIAN's H5PxAPIkatchu plugin for collecting detailed information during lesson execution for evaluation purposes. The lesson consisted of two phases with a brief intermediate instructional intervention providing beginner-level OSINT information. The video lesson featured images generated by OpenAI's DALL-E 2.

The results showed that in the second phase of the lesson there was an improvement in users' scores and the time taken to provide answers compared to the first phase.

Keywords: Framework, Cyber Security, Vigilance, Awareness, Students, H5P, Interactive Lesson, Best Practices

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα εικόνων

Λίστα Πινάκων

Λίστα Διαγραμμάτων

1

Εισαγωγή

Η εξάπλωση των Κοινωνικών Δικτύων έφερε αλλαγές σε πλήθος δραστηριοτήτων των κοινωνιών. Οι μορφές επικοινωνίας, η ιδιωτικότητα και οι κοινωνικές συναναστροφές είναι μερικές από αυτές που επηρεάστηκαν ιδιαίτερα, δημιούργησαν όμως νέους κινδύνους στον Κυβερνοχώρο με σοβαρές επιπτώσεις στους ανήλικους. Οι αναφερόμενοι από τα Κοινωνικά Δίκτυα ηλικιακοί περιορισμοί δεν απέδωσαν [1]. Το γεγονός αυτό οδήγησε την Ευρωπαϊκή Επιτροπή να ξεκινήσει την Πράξη για τις Ψηφιακές Υπηρεσίες (Digital Services Act) [2] ως μια προσπάθεια δημιουργίας ασφαλέστερου διαδικτυακού κόσμου για τους ανήλικους και προστασίας, μεταξύ άλλων, και της ψυχικής τους υγείας [3]. Η ταχεία ανάπτυξη της Τεχνητής Νοημοσύνης αναμένεται να βοηθήσει στην προστασία των ανηλίκων. Σε κάθε περίπτωση, η Πολιτεία οφείλει να προσφέρει σε όλους τη δυνατότητα να ενημερωθούν για τις απειλές και τους κινδύνους του διαδικτύου μέσα από κατάλληλο υλικό ευαισθητοποίησης, ώστε να ενδυναμώσουν τον βαθμό επαγρύπνησής τους στην Κυβερνοασφάλεια.

Η παρούσα διπλωματική έλαβε τις απαραίτητες άδειες της Επιτροπή Ηθικής και Δεοντολογίας της Έρευνας (Ε.Η.Δ.Ε.) του Διεθνούς Πανεπιστημίου της Ελλάδος και του σχολείου όπου διεξήχθη η έρευνα.

1.1 Αντικείμενο της διπλωματικής

Η διπλωματική έχει ως αντικείμενο τη δημιουργία πλαισίου επαγρύπνησης στην κυβερνοασφάλεια για μαθητικό πληθυσμό. Θα προτείνει, επομένως, ένα σύνολο ενεργειών, το οποίο, όταν θα εκτελείται, θα εξασφαλίζει τη συνεχή βελτίωση και λειτουργία ενός συστήματος το οποίο θα προσφέρει έναν αποτελεσματικό τρόπο για να επιτευχθεί επαγρύπνηση μαθητικού πληθυσμού. Για την αξιολόγηση του πλαισίου θα δημιουργηθεί μάθημα ευαισθητοποίησης και επαγρύπνησης στην κυβερνοασφάλεια με Διαδραστικό Βίντεο (Interactive Video) της H5P, το

οποίο θα εισαχθεί σε Σύστημα Διαχείρισης Μαθημάτων. Το μάθημα αυτό θα έχει δύο φάσεις και μία ολιγόλεπτη παρέμβαση μεταξύ τους και θα αφορά την Αποκάλυψη Θέση και Ταυτότητας. Σε αυτό το σύστημα θα διεξαχθεί έρευνα με μαθητές Α' τάξης Λυκείου, οι οποίοι θα συνδεθούν στο σύστημα και θα παρακολουθήσουν το διαδραστικό μάθημα, κατά τη διάρκεια του οποίου θα συλλεχθούν αναλυτικά στοιχεία εκτέλεσης (analytics). Από τη σύγκριση των πληροφοριών που θα συλλεχθούν σε κάθε φάση θα αξιολογηθεί η αποτελεσματικότητα του μαθήματος και του προτεινόμενου πλαισίου. Θα διαμοιραστεί και ερωτηματολόγιο με ερωτήσεις κλειστού τύπου για διερεύνηση του ποσοστού έκθεσης σε κινδύνους αποκάλυψης θέσης και ταυτότητας σε κοινωνικά δίκτυα και εφαρμογές συνομιλίας.

1.2 Συνεισφορά

Επιδίωξη της διπλωματικής είναι να συμβάλει στην ενίσχυση του μαθητικού πληθυσμού σε θέματα κυβερνοασφάλειας, προσφέροντας τα εξής:

1. Πλαίσιο με το οποίο οργανισμοί μπορούν να δημιουργήσουν σύστημα για διάθεση μαθημάτων και να εξασφαλίζουν τη συνεχή βελτίωσή του.
2. Πρόταση για χρήση ανοιχτού λογισμικού στη δημιουργία ολοκληρωμένου συστήματος διάθεσης μαθημάτων και παρακολούθησης βαθμού εκτέλεσης μαθημάτων (analytics).
3. Παρουσίαση και χρήση διαδικτυακών μαθημάτων με το εργαλείο H5P για να είναι ελκυστικά σε μαθητικό πληθυσμό
4. Αξιολόγηση επίδοσης του Πλαισίου
5. Χρήση Τεχνητής Νοημοσύνης για παραγωγή επιθυμητών εικόνων του βίντεο του μαθήματος, χωρίς προβλήματα δικαιωμάτων
6. Αποτελέσματα έρευνας με ερωτηματολόγιο με ευρήματα για ποσοστά έκθεσης προσωπικών δεδομένων σε εφαρμογές συνομιλίας (chatting)
7. Καλές πρακτικές

1.3 Δομή της Διπλωματικής

Στο Κεφάλαιο 1 υπάρχει η Εισαγωγή της διπλωματικής, το Αντικείμενο της διπλωματικής. Στο Κεφάλαιο 2 καταγράφηκε το θεωρητικό πλαίσιο και υφιστάμενες προσεγγίσεις. Στο Κεφάλαιο 3 περιλαμβάνει τους ορισμούς και ευρήματα ερευνών σε μαθητές. Στο Κεφάλαιο 4 αναπτύσσεται το προτεινόμενο πλαίσιο της διπλωματικής. Στο Κεφάλαιο 5 υπάρχει η

μεθοδολογία. Στο Κεφάλαιο 6 παρουσιάζονται τα αποτελέσματα των ερευνών και γίνεται η συζήτηση των αποτελεσμάτων. Στο Κεφάλαιο 7 αναπτύσσουμε τα συμπεράσματα των ερευνών και τις καλές πρακτικές. Στο Κεφάλαιο 8 είναι ο Επίλογος, με την σύνοψη ολόκληρης της διπλωματική και με τις μελλοντικές επεκτάσεις.

Στο Κεφάλαιο 9 υπάρχει η βιβλιογραφία. Στο Κεφάλαιο 10 βρίσκονται τα τέσσερα παραρτήματα της διπλωματικής.

2

Θεωρητικό πλαίσιο - Υφιστάμενες προσεγγίσεις

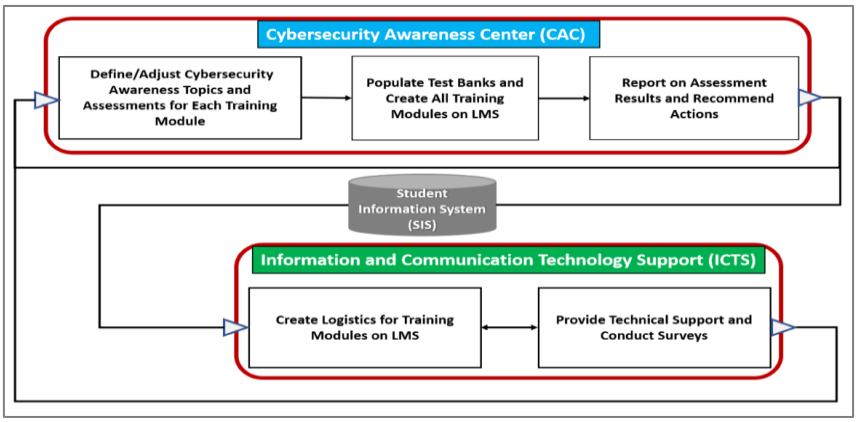
Υπάρχουν διάφοροι τρόποι προσεγγίσεως του θέματος Επαγρύπνησης στην Κυβερνοασφάλεια. Στην εργασία αυτή εξετάστηκαν 2 ειδών, ως προς το θεωρητικό πλαίσιο και ως προς το είδος υλικού ευαισθητοποίησης στην κυβερνοασφάλεια.

2.1 Θεωρητικό υπόβαθρο

2.1.1 Πλαίσιο Κυβερνοασφάλειας

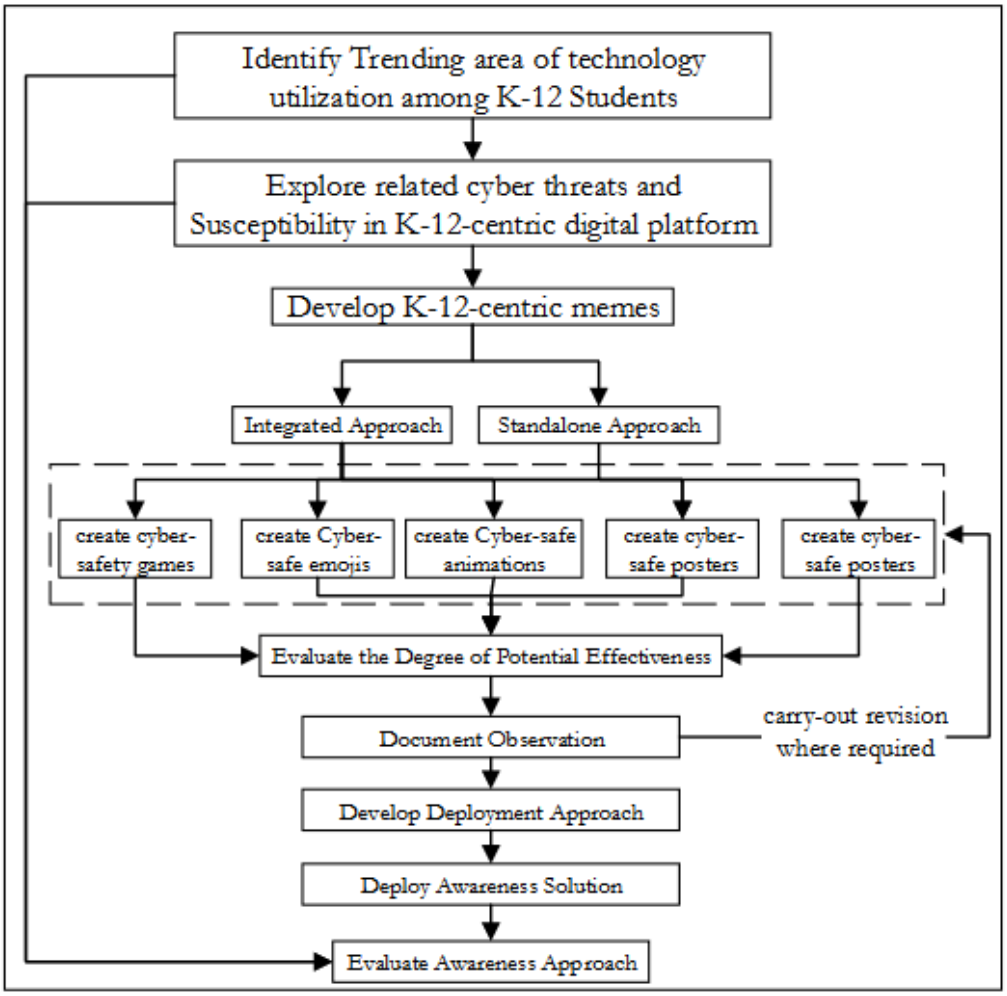
Οι N. Kortjan και R. Solms στην εργασία του 2014 [4] πρότειναν ένα πλαίσιο για την ευαισθητοποίηση και την εκπαίδευση στην κυβερνοασφάλεια της Νοτίου Αφρικής. Χρηματοδοτήθηκε από το Εθνικό Ίδρυμα Ερευνών (NSF) της Νοτίου Αφρικής με στόχο την ευαισθητοποίηση και εκπαίδευση των πολιτών, καθώς και των μικρών και μεσαίων επιχειρήσεων της Νοτίου Αφρικής. Για να φτάσουν στην τελική πρόταση, έκαναν συγκριτική ανάλυση των τρόπων που λειτουργούσαν σε αυτόν τον τομέα οι ΗΠΑ, Αυστραλία, Καναδάς και Βρετανία σε εθνικό επίπεδο. Στη συνέχεια, πήραν συνεντεύξεις και συζήτησαν με ειδικούς πάνω στα αρχικά σχέδια-προτάσεις που είχαν καταλήξει οι συγγραφείς, ζητώντας τους να ελέγξουν και να προτείνουν βελτιώσεις, πολλές από τις οποίες συμπεριλήφθηκαν στην τελική πρόταση Πλαισίου. Για να εξασφαλιστεί ο διαρκείς έλεγχος και η βελτίωση του Πλαισίου, το ανέπτυξαν σύμφωνα με τη μέθοδο Ντέμινγκ (Deming), γνωστή και ως Κύκλος Ντέμινγκ ή PDCA (Plan-Do-Check-Act), μέθοδο που χρησιμοποιήθηκε και στο πρότυπο ISO/IEC 27000 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Το 2021, οι M. Khader, M. Karam και H. Fares [5] επισημαίνουν πως ενώ έγιναν στον βιομηχανικό τομέα έρευνες εγκαθίδρυση για ευαισθητοποίηση στην κυβερνοασφάλεια, δεν έγινε το ίδιο και στον Ακαδημαϊκό τομέα όπου εστίασαν στην κατανόηση συμπεριφορών και στάσεων των φοιτητών. Για τον σκοπό αυτόν, πρότειναν το Πλαίσιο Ευαισθητοποίησης στην Κυβερνοασφάλεια για Ακαδημαϊκά Ιδρύματα, CAFA (Cybersecurity Awareness Framework for Academia), απευθύνεται σε όλες τις επιστήμες με διαφορετικό υλικό ευαισθητοποίησης. Το πλαίσιο αποτελείται από δύο τμήματα, το Κέντρο Ευαισθητοποίησης Κυβερνοασφάλειας (CAC) και το τμήμα Υποστήριξης Πληροφορικής και Επικοινωνιών (ICTS), και προβλέπει ύπαρξη Διασφάλισης της Ποιότητας, ώστε να γίνεται συνεχής έλεγχος και βελτίωσή του.



Εικόνα 1 Σχηματικά αναπαράσταση Πλαισίου CAFA (Cybersecurity Awareness Framework for Academia)

Η εργασία των M. Al-Tajer και I. Adeyemi του 2022 [6] προτείνει ένα πλαίσιο επαγρύπνησης κυβερνοασφάλειας για μαθητές λυκείου του Κατάρ. Διαπίστωσαν πως το βασικό μάθημα πληροφορικής στα σχολεία δεν αρκεί να καλύψει την ανάγκη για αντιμετώπιση σύγχρονων καταστάσεων στο διαδίκτυο και πως η ύπαρξη σχετικού μαθήματος κυβερνοασφάλειας στο πρόγραμμα σπουδών θα πρόσφερε αποτελεσματικότερη ευαισθητοποίηση των μαθητών. Έπειτα από μελέτη διάφορων προσεγγίσεων ευαισθητοποίησης Κυβερνοασφάλειας πρότειναν ένα πλαίσιο με τέσσερις κύριες φάσεις, της Αναγνώρισης Απειλών, Ανακάλυψης Υπάρχουσας Ευαισθητοποίησης, Δημιουργίας Προσέγγισης Ευαισθητοποίησης και Αξιολόγησης.



Εικόνα 2 Προτεινόμενο Πλαίσιο Επαγρύπνησης Κυβερνοασφάλειας για μαθητές λυκείου του Κατάρ

2.1.2 Περιεχόμενο μαθημάτων

Οι L. Zhang-Kennedy και S. Chiasson στην εργασία τους (2020) [7] πραγματοποίησαν συστηματική ανασκόπηση σε βάθος 20ετίας των πολυμεσικών εργαλείων για την ευαισθητοποίηση και εκπαίδευση στην Κυβερνοασφάλεια μη έμπειρων ατόμων. Η S. Chiasson χρηματοδοτήθηκε από το Συμβούλιο Έρευνας Φυσικών Επιστημών και Μηχανικής του

Καναδά. Εξέτασαν 119 εργαλεία από τα οποία τα 91 ήταν διαδικτυακά προσβάσιμα και κάλυπταν ποικιλία θεμάτων της κυβερνοασφάλειας, από απλά, όπως δημιουργία κωδικών και ηλεκτρονικό ψάρεμα, έως σύνθετα προβλήματα του χώρου. Βρήκαν πως υπήρχε έλλειμα στην αξιολόγηση που είχαν τα εργαλεία αυτά, καθώς σε πολλά υπήρχε απλά μια δοκιμή. Στα συμπεράσματά τους έγραψαν πως η χρήση πολυμέσων είναι από τις υποσχόμενες προσεγγίσεις ευαισθητοποίησης και πως μπορεί να συμβάλει στην αύξηση προστασίας των χρηστών. Προτρέπουν τους δημιουργούς νέων εργαλείων ευαισθητοποίησης να ακολουθήσουν τις εξής τρεις προτάσεις:

1. Προσαρμοστικότητα, να μπορεί να προσαρμόζεται εύκολα στους τρέχοντες κινδύνους κυβερνοασφάλειας, να έχει εύκολη και γρήγορη πρόσβαση, χωρίς ανάγκη νέου υλικού υπολογιστή και εγκατάσταση προγραμμάτων, και τέλος να έχει χαμηλό κόστος σε χρήμα αλλά και χρόνο παραγωγής.
2. Χρηστικότητα, να μπορεί να χρησιμοποιηθεί από τους χρήστες σε ελάχιστο χρόνο και προσπάθεια, η εκμάθηση να πετυχαίνετε σε λογικό χρόνο, να έχει αξία για τον χρήστη η επανάληψή του.
3. Μάθηση, να υποστηρίζει ενεργή συμμετοχή των χρηστών με αλληλεπίδραση και ανατροφοδότηση, να υποστηρίζει συνεργατική μάθηση, όταν χρειάζεται, να υπάρχει αξιολόγηση της ποιότητας μάθησης από χρήστες και αξιολογητές μέσω ανατροφοδότησης και ανάλυσης δεδομένων από εσωτερικά εργαλεία.

Στο Πανεπιστήμιο του Wollongong της Αυστραλίας το 2020, οι G. Jiang et al. [8] διενήργησαν έρευνα κατά τη διάρκεια της πανδημίας του Covid-19 για να αξιολογήσουν το εργαλείο Διαδραστικό Βίντεο που προσφέρει η H5P μέσα σε περιβάλλον Moodle. Το διαδραστικό υλικό αφορούσε μάθημα ειδικότητας του τμήματος Μηχανικών Περιβάλλοντος την Άνοιξη του 2020. Κατά την έρευνα συνέκριναν τα αποτελέσματα προπτυχιακών και μεταπτυχιακών φοιτητών σε κουίζ και αναφορές μετά από παρακολούθηση βιντεοσκοπημένων μαθημάτων και μετά από υλικό Διαδραστικού Βίντεο (Interactive Video), Διαφανειών (Slides) και Ερωτήσεις Γνώσεων (Quiz) της H5P. Μετά από άδεια του Πανεπιστημίου, συλλέχτηκαν στατιστικά από το βαθμολόγιο και τα αρχεία καταγραφής (log files) του Moodle, στα οποία υπήρχε αδυναμία εξακρίβωσης για το αν ολοκληρώθηκε η προβολή κάθε βίντεο. Στο υλικό Διαδραστικού Βίντεο H5P υπάρχουν τα σημεία ελέγχου, υποβολής και σύνοψης, τα οποία αποδεικνύουν την ολοκλήρωση των δραστηριοτήτων. Τα αποτελέσματα από τη χρήση H5P ήταν ενθαρρυντικά, καθώς αποδείχτηκε ότι προκαλεί την παρακολούθηση βίντεο σε σημαντικά μεγαλύτερο βαθμό από την προβολή των συμβατικών βίντεο μαθημάτων, βοηθώντας και στην επίτευξη καλύτερης βαθμολογίας στα κουίζ, η οποία ήταν παρόμοια με της διδασκαλίας πρόσωπο με πρόσωπο. Επίσης, βρέθηκε ισχυρή συσχέτιση (συντελεστής συσχέτισης r=0,8388) μεταξύ του 95% όσων παρακολούθησαν βίντεο και του βαθμού τους στα κουίζ, οπότε τα Διαδραστικά Βίντεο H5P

είναι ιδιαίτερα χρήσιμα. Η δημιουργία όμως τέτοιου υλικού σε H5P απαιτεί 50% επιπλέον χρόνο προετοιμασίας από ότι ένα συμβατικό βίντεο, όμως, θα μπορούν να επαναχρησιμοποιηθούν με τροποποίηση των μηνυμάτων και των ζητούμενων μέσα σε αυτά.

2.2 Προσέγγιση ως προς το είδος υλικού ευαισθητοποίησης

Στην ενότητα αυτή εξετάστηκε το είδος του εκπαιδευτικού υλικού ευαισθητοποίησης που απευθύνεται σε μαθητές/τριες από την προσχολική ηλικία έως λυκείου, καλύπτοντας τους κινδύνους του διαδικτύου. Ανάλογα με την ηλικία προσφέρονται από απλά κόμικς και φτάνουν στη Παιχνιδοποίηση (Gamification) και τις Μαθησιακές Ενότητες για να πετύχουν τον σκοπό τους. Από τη μελέτη εργασιών [7], [9], [10] προέκυψε ο πίνακας με τους τρόπους προσέγγισης Κυβερνοασφάλειας ως προς το είδος υλικού ευαισθητοποίησης με τα θετικά και αρνητικά σημεία του.

Πίνακας 1 Αξιολόγηση προσεγγίσεων επαγρύπνησης κυβερνοασφάλειας

Τρόπος Προσέγγισης επαγρύπνησης Κυβερνοασφάλειας	**Θετικά σημεία**	**Αρνητικά σημεία**
Ψηφιακά παιχνίδια (Digital games)	Διασκέδαση, αφοσίωση, άμεση ανατροφοδότηση, αφήγηση, διαδικαστική ρητορική (procedural rhetoric)	Εμπειρικά έχουν μη αξιόπιστα εκπαιδευτικά αποτελέσματα
Επιτραπέζια παιχνίδια (Tabletop games)	Φυσική-κοινωνική αλληλεπίδραση παικτών, προσιτά σε άτομα με χαμηλές γνώσεις στους υπολογιστές, φτηνά, αλλαγή και αποδοχή κανόνων, δίνουν κριτική σκέψη	Απαιτούν κοινωνική αλληλεπίδραση
Ταινίες μικρού μήκους και Κινούμενη Εικόνα (Short films and animation)	Μη ξεκάθαρα ερευνητικά αποτελέσματα, προάγουν την κατανόηση, οι μικρές απαιτούν συντομότερο χρόνο αφοσίωσης από τις άλλες προσεγγίσεις.	Μη ξεκάθαρα ερευνητικά αποτελέσματα, αποσπούν την προσοχή από τη διαδικασία μάθησης, παθητική παρακολούθηση.
Κόμικς (Comics)	Προσβασιμότητα, νοητικά μοντέλα, αύξηση αφοσίωσης, κατανόηση και απομνημόνευση πληροφοριών ασφάλειας και απορρήτου.	Λόγω της απλοποίησης εννοιών που έχουν, υπάρχει κίνδυνος να παραλειφθούν κρίσιμα σημεία.

Μαθησιακές ενότητες (Learning modules)	Ατομική και συνεργατική μάθηση, στηρίζονται σε πολυμέσα, επιλογή ρυθμού από μαθητή. Δυνατότητα διαφορετικών στυλ παρακολούθησης. Παιχνιδοποίηση.	Δύσκολη υλοποίηση για όλα τα επίπεδα χρηστών. Μονότονα.

Οι προσεγγίσεις που βρέθηκαν και τα θετικά και αρνητικά τους στις εργασίες [7], [9], [11] είναι τα εξής:

α. Τα ψηφιακά παιχνίδια (digital games) μπορούν να συμβάλουν στην επιτυχία των σκοπών τους γιατί προσφέρουν στους χρήστες διασκέδαση, αφοσίωση, άμεση ανατροφοδότηση και αφήγηση. Επίσης, ερευνητές που χρησιμοποίησαν διαδικαστική ρητορική (procedural rhetoric) στη σχεδίαση των παιχνιδιών, την ύπαρξη δηλαδή μηνυμάτων που προκύπτουν από τους κανόνες του παιχνιδιού, διαπίστωσαν ότι μπορεί να αλλάξει με επιτυχία συμπεριφορές των παικτών. Όμως, εμπειρικά στοιχεία έδειξαν πως δεν είναι αξιόπιστα για επιτυχή εκπαιδευτικά αποτελέσματα. Υπάρχουν πολλά στο διαδίκτυο δωρεάν [12], [13].

β. Τα επιτραπέζια παιχνίδια (tabletop games) είναι ένας παραδοσιακός τρόπος παιχνιδιού που υποστηρίζει τη φυσική αλληλεπίδραση των παικτών. Όπως είναι αναμενόμενο, έχουν καλύτερα αποτελέσματα από τα ψηφιακά στο κοινωνικό παιχνίδι (παιδιά που αλληλοεπιδρούν άμεσα). Είναι προσιτά σε άτομα με χαμηλές γνώσεις στους υπολογιστές και φτηνά για χρήση τους σε τάξεις. Τέλος, επιτρέπουν την αλλαγή και αποδοχή κανόνων του παιχνιδιού και αυτό ενισχύει την κριτική σκέψη και τη δέσμευση με το περιεχόμενο του παιχνιδιού. Πολλές ιστοσελίδες ενημέρωσης για την επαγρύπνηση στην κυβερνοασφάλεια προσφέρουν τέτοια παιχνίδια [14].

γ. Οι ταινίες μικρού μήκους και η κινούμενη εικόνα (short films and animation) δίνουν μεικτά αποτελέσματα. Κάποια ερευνητικά αποτελέσματα δείχνουν πως η κινούμενη εικόνα προάγει την κατανόηση, ενώ άλλες πως αποσπά από τη μαθησιακή διαδικασία και πως συχνά είναι πολύπλοκη ή γρήγορη για να γίνει αντιληπτή. Οι ταινίες μικρού μήκους απαιτούν συντομότερο χρόνο αφοσίωσης από τις υπόλοιπες προσεγγίσεις, αλλά το περιεχόμενό τους είναι παθητικό και δεν υπάρχει κάποια διάδραση με τους μαθητές. Είναι από τους συνηθέστερους τρόπους προειδοποίησης για κινδύνους [15], [16].

δ. Τα κόμικς (comics) προσφέρουν μεγάλη προσβασιμότητα, δημιουργούν νοητικά μοντέλα (εσωτερικές αναπαραστάσεις, της ιστορίας του κόμικ εδώ), αυξάνουν την αφοσίωση στο περιεχόμενο, βοηθούν στην κατανόηση και απομνημόνευση πληροφοριών. Χρησιμοποιούνται για την επισήμανση σημαντικών πληροφοριών.

Συμπερασματικά, λόγω της φύσης της στατικής εικόνας εγκυμονεί κίνδυνος παράλειψης κρίσιμων σημείων. Είναι ιδιαίτερα ελκυστικά σε όλες τις ηλικίες και υπάρχουν πολλά διαθέσιμα με περιεχόμενο αρχαρίων αλλά και προχωρημένων [17], [18], [19].

ε. Οι μαθησιακές ενότητες (learning modules) ομαδοποιούν πληροφορίες και δίνονται τμηματικά, με τον επιθυμητό ρυθμό και με τη χρήση πολυμέσων στους μαθητές. Μπορούν να χρησιμοποιηθούν τόσο για ατομική όσο και για συνεργατική μάθηση. Ερευνητές ισχυρίζονται πως είναι κατάλληλες για χρήση στην τάξη, καθώς συνοδεύονται από υποστηρικτικό υλικό, όπως βιβλίο καθηγητή, σχέδια μαθημάτων και δραστηριότητες. Όσες έχουν διαδραστικό περιεχόμενο και δραστηριότητες αποκαλούνται ορισμένες φορές ως «παιχνίδια», έννοια που δεν ανταποκρίνεται στην πραγματικότητα, γιατί δεν ενσωματώνουν μηχανισμούς κανόνων παιχνιδιού ούτε χρησιμοποιούν μάθηση μέσω παιχνιδιού (game based). Έχουν τη δυνατότητα να προσφέρουν διαφορετικούς τρόπους παρακολούθησης.

3

Κυβερνοασφάλεια και Ευαισθητοποίηση Σχολικού Πληθυσμού

Ο σημερινός σχολικός πληθυσμός είναι οι μελλοντικοί πολίτες μιας κοινωνίας που θα βασίζεται πολύ περισσότερο στο διαδίκτυο από αυτή που ζούμε τώρα. Η επιδίωξη αναγνώρισης και αυτοπροβολής των μαθητών στον περίγυρό τους είναι αναμενόμενη, οι τρόποι που συχνά προσπαθούν να το πετύχουν αυτό εγκυμονούν κινδύνους που πιθανώς να δημιουργήσουν προβλήματα στην καθημερινότητα των ίδιων και των οικογενειών τους. Θα απαιτηθεί, επομένως, από μέρους τους η απόκτηση δεξιοτήτων ασφαλούς περιήγησης και αλληλεπίδρασης στον Κυβερνοχώρο, που θα επιτρέψει να έχουν αυτοί και οικογένειές τους ηρεμία στην τρέχουσα αλλά και μελλοντική ζωή τους.

3.1 Ορισμοί

Πριν αναφερθούν λεπτομέρειες που δείχνουν την αναγκαιότητα προστασίας είναι σημαντικό να δοθούν σημαντικοί ορισμοί όρων.

Ο όρος Κυβερνοασφάλεια (Cyber security) [20], [21], [22] αναφέρεται σε πρακτικές με τις οποίες προστατεύονται συστήματα υπολογιστών, δικτύων και δεδομένων από απειλές.

Ασφάλεια στο Διαδίκτυο (Cyber safety) [23], [24] είναι η προστασία των χρηστών στο διαδίκτυο από κινδύνους όπως η υποκλοπή προσωπικών πληροφοριών, ο εκφοβισμός, κακόβουλο λογισμικό κλπ.

Ο όρος Ευαισθητοποίηση στην Κυβερνοασφάλεια (Cybersecurity Awareness) [25] [26] [27] αναφέρεται στην ανάδειξη των κινδύνων που εγκυμονεί η σύνδεση και η συμμετοχή ατόμων σε δραστηριότητες στο διαδικτύου και στην αποφυγή τους.

Η Επαγρύπνηση στην Κυβερνοασφάλεια (Cybersecurity Vigilance) [28] αναφέρεται στην αναγνώριση και σωστή αντίδραση απέναντι στους κινδύνους του διαδικτύου. Είναι, επομένως, Ευαισθητοποίηση και Επαγρύπνηση δυο σημαντικά και αλληλένδετα χαρακτηριστικά που πρέπει να κατέχουν οι ενδιαφερόμενοι, με την ευαισθητοποίηση να προηγείται της επαγρύπνησης.

Διαδικτυακός εκφοβισμός (Cyberbullying) [29] συντελείται στις περιπτώσεις που ένα άτομο γίνεται στόχος απειλών ή ταπείνωσης στο διαδίκτυο, είναι συμπεριφορά επαναλαμβανόμενη, γίνεται με πρόθεση και επιδρά ψυχολογικά στον στόχο.

Διαδικτυακή αποπλάνηση (Grooming) [29] είναι η προσπάθεια που γίνεται, συνήθως από μέρους ενός ενήλικα, να δημιουργήσει κλίμα εμπιστοσύνης με τον ανήλικο χρήστη, με σκοπό τη σεξουαλική εκμετάλλευση του τελευταίου.

Sexting [29] είναι η αποστολή σεξουαλικών μηνυμάτων ή φωτογραφιών μέσω κινητών τηλεφώνων ή μέσων κοινωνικής δικτύωσης.

Προσωπικά δεδομένα [29] είναι οι πληροφορίες που αναφέρονται σε ένα άτομο. Ευαίσθητα προσωπικά δεδομένα είναι όσα αφορούν την υγεία του, την προσωπική ζωή, το θρήσκευμα, πολιτικές πεποιθήσεις κλπ.

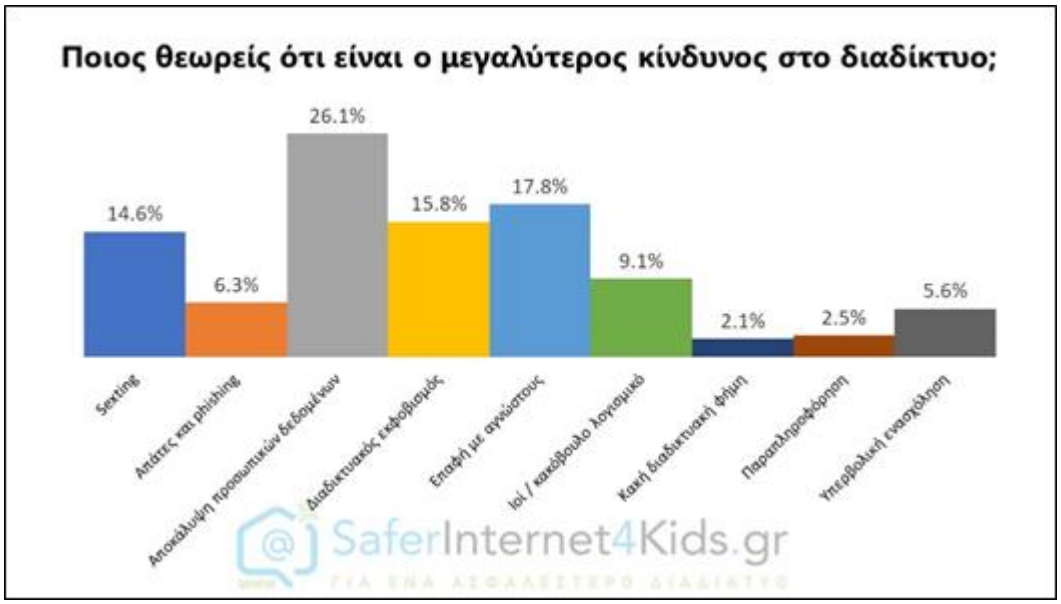
3.2 Έρευνες σε μαθητικό πληθυσμό

Η εύρεση έγκυρων στατιστικών στοιχείων είναι ο σημαντικότερος παράγοντας προκειμένου να εξαχθούν συμπεράσματα για την κατάσταση που επικρατεί στο αντικείμενο της έρευνας. Στη χώρα μας, από τους εγκυρότερους οργανισμούς που διενεργεί έρευνες σε μαθητικό πληθυσμό αλλά και τον ενημερώνει για όλα τα θέματα διαδικτύου είναι το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου [30].

Πίνακας 2 Επιλεγμένα στατιστικά Ερευνών SaferInternet4kids.gr (2018-24)

Ερώτηση έρευνας	**2018-19** [31]	**2020** [1]	**2021-22** [32]	**2023-24** [33]
1. Κάνει αποδοχή αιτημάτων φιλίας από αγνώστους	41 %	24 %	46 %	-
2. Συνομιλεί με αγνώστους	-	38 %	59 %	-
3. Έπεσαν θύμα παρενόχλησης	21 %	33 %	-	-
4. Έπεσαν θύμα εκφοβισμού	-	5 %	6 %	15 %
5. Δε νιώθει ασφάλεια στο διαδίκτυο	-	-	-	46 %

Στον Πίνακας 2 παρατηρούμε ότι δεν υπάρχουν απαντήσεις σε όλες τις στήλες, διότι δεν είχε τεθεί τέτοιο ερώτημα στην αντίστοιχη έρευνα. Στην Ερώτηση 1 του πίνακα διαπιστώνουμε ότι υπάρχει μεγάλη μείωση του ποσοστού αποδοχής αιτημάτων φιλίας από αγνώστους κατά 17%, στην Ερώτηση 2 υπάρχει αύξηση κατά 19% των μαθητών που συνομιλούν με αγνώστους, ενώ στην Ερώτηση 3 ο αριθμός όσων έπεσαν θύματα παρενόχλησης αυξήθηκε κατά 12%. Στην Ερώτηση 4 φαίνεται συνεχόμενη αύξηση επί τρεις συνεχόμενες έρευνες, με την τελευταία να φτάνει το 9%. Τέλος, στην Ερώτηση 5 το 46% των μαθητών δεν νιώθει ασφάλεια στο διαδίκτυο.



Εικόνα 3 Ποιος θεωρείς ότι είναι ο μεγαλύτερος κίνδυνος στο διαδίκτυο – Έρευνα 2021-22

Το διάγραμμα της Εικόνα 3 απεικονίζει τα αποτελέσματα της έρευνας του 2021-22 του Saferinternet4kids [32]**,** κατά την οποία οι μαθητές κλήθηκαν να επιλέξουν ποιον από τους παραπάνω θεωρούν τον μεγαλύτερο κίνδυνο στο διαδίκτυο. Από τις εννέα επιλογές, οι τέσσερις που συγκέντρωσαν τα μεγαλύτερα ποσοστά ήταν η Αποκάλυψη προσωπικών δεδομένων, η Επαφή με αγνώστους, ο Διαδικτυακός εκφοβισμός και το Sexting, οι οποίες έφτασαν αθροιστικά το 74%. Οι τέσσερες αυτοί κίνδυνοι αλληλεπιδρούν μεταξύ τους και μπορούν να οδηγήσουν σε δυσάρεστες καταστάσεις τους μαθητές. Παράδειγμα, από τα στατιστικά του Πίνακας 2 προκύπτει ότι, σύμφωνα με την έρευνα του 2021-22, το 59% συνομιλεί με αγνώστους, γεγονός που μπορεί να το εκμεταλλευτεί κακόβουλος διαδικτυακός “φίλος” και να προβεί σε απόσπαση προσωπικών δεδομένων, σε sexting και σε εκφοβισμό.

4

Πλαίσιο επαγρύπνησης

Όπως διαπιστώθηκε από τις προαναφερθείσες έρευνες του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου στο Κεφάλαιο 3, υπάρχουν προβλήματα και φόβοι στον σχολικό πληθυσμό που αναδεικνύουν την ανάγκη συνεχούς ευαισθητοποίησής του σε θέματα κυβερνοασφάλειας. Οι μαθητές είναι αναμενόμενο να αλλάζουν ενδιαφέροντα στη ζωή τους, αναζητώντας ανάλογες νέες εφαρμογές, και αυτό θα τους φέρνει αντιμέτωπους με νέες απειλές.

Με βάση τη μελέτη των εργασιών που παρουσιάστηκαν στο Κεφάλαιο 2, για τους τρόπους υλοποίησης πλαισίων κυβερνοασφάλειας και τους τρόπους δημιουργίας αποτελεσματικών διαδικτυακών μαθημάτων, σχεδιάστηκε το προτεινόμενο Πλαίσιο Επαγρύπνησης στην Κυβερνοασφάλεια για Μαθητικό Πληθυσμό, έχοντας ως στόχο:

1. τον οργανωμένο τρόπο συνεχούς επίβλεψης και καταγραφής των υπαρχουσών και νέων απειλών
2. την έγκαιρη δημιουργία υλικού ευαισθητοποίησης ανάλογου κάθε ηλικιακής ομάδας εκπαίδευσης
3. την αξιολόγηση της αποτελεσματικότητας του υλικού και την τροποποίησή του αν χρειάζεται
4. τη συνεχή ευαισθητοποίηση και επαγρύπνηση του σχολικού πληθυσμού στον κυβερνοχώρο.

4.1 Πρόταση Πλαισίου Επαγρύπνησης Κυβερνοασφάλειας Μαθητικού Πληθυσμού

Το προτεινόμενο Πλαίσιο Επαγρύπνησης Κυβερνοασφάλειας Μαθητικού Πληθυσμού αποτελείται από τα εξής στάδια:

1. Αναζήτηση απειλών
2. Επιλογή νέων απειλών για μαθητικό πληθυσμό
3. Ανάλυση απειλών, Κατηγοριοποίησή τους και Σχεδίαση ανάλογου μαθήματος ευαισθητοποίησης
4. Δημιουργία μαθήματος ευαισθητοποίησης
5. Ενσωμάτωση νέου μαθήματος στο Σύστημα Διαχείρισης Μαθημάτων Ευαισθητοποίησης
6. Συλλογή αναλυτικών στοιχείων εκτέλεσης μαθημάτων (Analytics) και συλλογή αναφορών προβλημάτων που υπέβαλαν οι μαθητές για μαθήματα
7. Εξέταση και Ερμηνεία των αναλυτικών στοιχείων και αναφορών προβλημάτων από μαθητές
8. Αναθεώρηση μαθημάτων

Είναι απαραίτητο να δοθεί η επεξήγηση του τρόπου λειτουργίας του πλαισίου:

Στάδιο 1, η αναζήτηση απειλών για μαθητές γίνεται στα ευρήματα ερευνών αλλά και οπουδήποτε αλλού. Υπάρχουν επίσημα Κέντρα Ασφαλούς Διαδικτύου στις χώρες της Ευρωπαϊκής Ένωσης [34] που επικεντρώνονται σε θέματα ευαισθητοποίησης μαθητών και διενεργούν επίσημες έρευνες σε μεγάλο αριθμό μαθητικού πληθυσμού, συνήθως ανά τακτά χρονικά διαστήματα του ενός ή δύο ετών. Λόγω των μεγάλων διαστημάτων που μεσολαβούν μεταξύ αυτών των ερευνών, απειλές μπορούν να αναζητηθούν και σε άλλες έρευνες που θα εμφανιστούν, καθώς και σε τηλεόραση, κοινωνικά δίκτυα και εξειδικευμένες ιστοσελίδες κ.λπ.

Στάδιο 2, από τις απειλές που θα ανακαλυφθούν στο προηγούμενο βήμα, θα επιλεχθούν οι νέες που αφορούν μαθητικό πληθυσμό.

Στάδιο 3, κάθε νέα απειλή θα αναλυθεί, ώστε να αποφασιστεί σε ποια ενότητα ευαισθητοποίησης ανήκει (Αποκάλυψη θέσης, Συμπεριφορά στο διαδίκτυο, Προσωπικά δεδομένα κ.λπ.) και ποιες ηλικίες – τάξεις αφορά (Α-Γ Δημοτικού, Β Γυμνασίου, Α’ Λυκείου κ.λπ.), ώστε να σχεδιαστεί μάθημα σε ανάλογο τύπο (Διαδραστικό Βίντεο, Χάρτη Παιχνιδιού κ.λπ.). Αυτές οι πληροφορίες θα είναι συνοδευτικές και θα χρησιμοποιηθούν στη συνέχεια, στο στάδιο ενσωμάτωσης στο Σύστημα Διαχείρισης των Μαθημάτων.

Στάδιο 4, η δημιουργία του μαθήματος ευαισθητοποίησης, θα γίνει με εργαλεία και τεχνικές, που παρουσιάστηκαν στο Κεφάλαιο 2, για να κάνουν ελκυστικό το μάθημα και να βοηθούν τους μαθητές να κατανοήσουν τα νοήματα και να αναπτύξουν δεξιότητες σωστής ανταπόκρισης. Παράδειγμα, στην ευαισθητοποίηση για την Αποκάλυψη Θέσης, μέσα από ένα διαδραστικό βίντεο να μπορούν να ανακαλύψουν πώς η θέση τους μπορεί να αποκαλυφθεί εύκολα από μια απρόσεχτη φωτογραφία ή από συνδυασμό πληροφοριών που έχουν δώσει προηγουμένως αυτοί ή φίλοι τους, αν κάποιος κακόβουλος έχει λίγες γνώσεις OSINT [35] με απλή χρήση δωρεάν εργαλείων, όπως αναζήτησης με αναγνώριση φωτογραφίας και χαρτών.

Στάδιο 5, στην ενσωμάτωση του μαθήματος στο Σύστημα Διαχείρισης Μαθημάτων, θα χρησιμοποιηθούν οι συνοδευτικές πληροφορίες από το προηγούμενο στάδιο, δημιουργίας του μαθήματος, για να ενταχθεί σε ανάλογες κατηγορίες με Ετικέτες (Tags) :

i. Ηλικίες – Τάξεις που αφορά
ii. Τύπο μαθήματος (Διαδραστικό βίντεο, κ.λπ.)
iii. Ενότητα που αφορά (Αποκάλυψη θέσης, κ.λπ.)

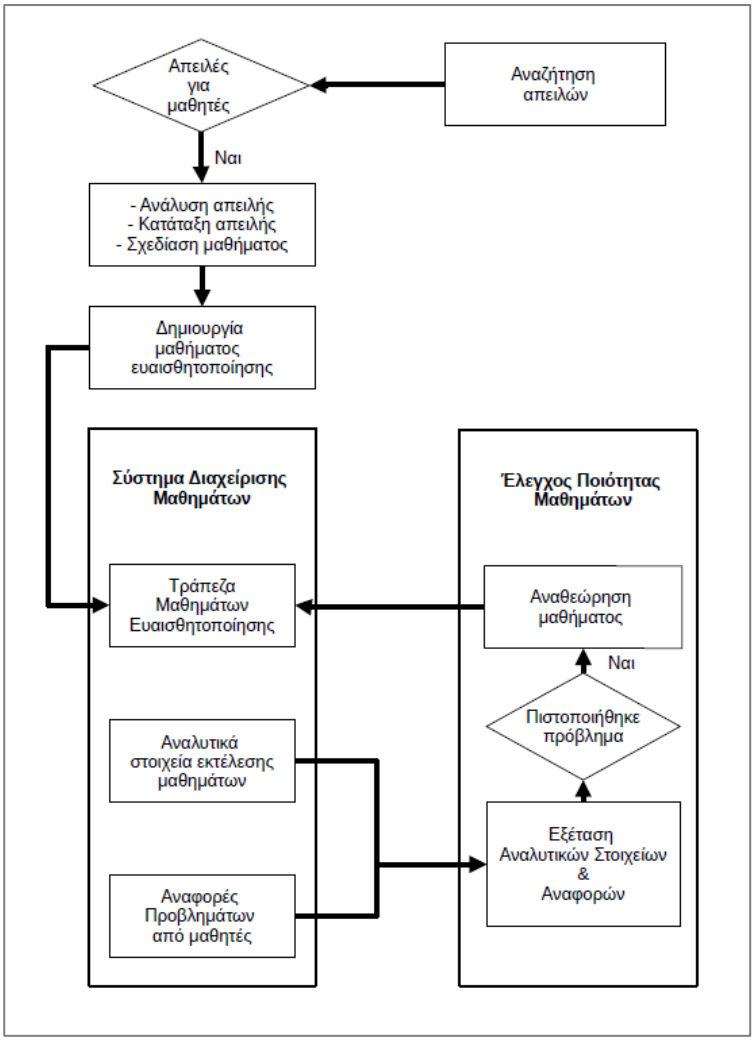
Με αυτό τον τρόπο θα μπορούν να επιλέγουν εύκολα οι μαθητές το επιθυμητό μάθημα.

Στάδιο 6, συλλογής στοιχείων εκτέλεσης μαθημάτων (Analytics) και αναφορών προβλημάτων από μαθητές, θα συλλέγονται στοιχεία, μεταξύ των οποίων θα περιλαμβάνονται πληροφορίες όπως συνολική βαθμολογία, απάντηση που δόθηκε ανά ερώτημα, αριθμός επαναλήψεων, χρόνος που απαιτήθηκε σε κάθε προσπάθεια, αριθμός ανολοκλήρωτων προσπαθειών κ.λπ.

Στάδιο 7, θα αναλυθούν οι πληροφορίες που συλλέχθηκαν στο προηγούμενο στάδιο. Από τις πληροφορίες αυτές θα μπορεί να ελεγχθεί, για παράδειγμα, αν υπάρχουν μαθήματα με υψηλό βαθμό αποτυχίας ή ανολοκλήρωτων προσπαθειών, ώστε να αναζητηθούν οι αιτίες. Σε αυτό μπορεί να συμβάλει και η διάθεση στους μαθητές της επιλογής καταχώρησης αναφοράς προβλημάτων που αντιμετώπισαν σε μάθημα. Αν υπάρχουν μαθήματα τα οποία δεν έχουν τα επιθυμητά ποσοστά, τότε θα προχωρήσει στο επόμενο στάδιο, παρέμβασης βελτίωσης στο μάθημα.

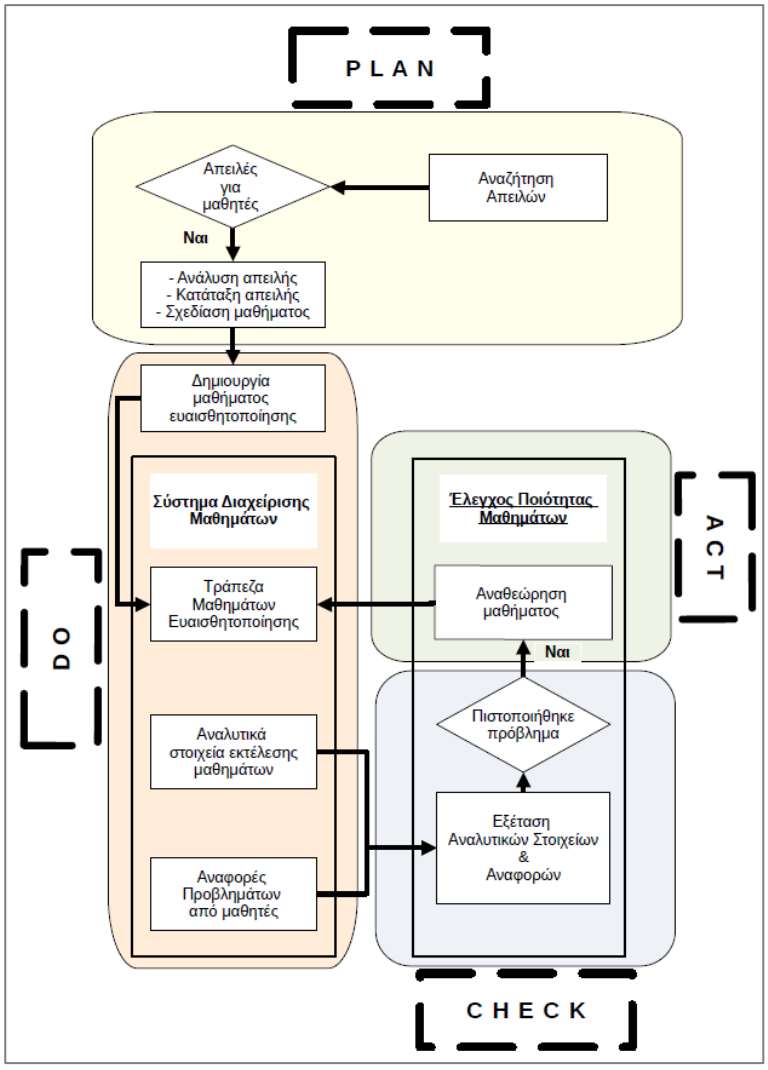
Στάδιο 8, της αναθεώρησης μαθήματος. Αν στο προηγούμενο Στάδιο κριθεί απαραίτητο, τότε θα επανεξεταστεί και θα βρεθούν και εφαρμοστούν οι απαιτούμενες αλλαγές για να επανενταχθεί στη συνέχεια στο Σύστημα Διαχείρισης Μαθημάτων.

Η επανάληψη των Σταδίων αυτών θα γίνεται σε τακτά χρονικά διαστήματα ή όποτε προκύψει νέα απειλή, όπως περιγράφετε στο Στάδιο 1.



Εικόνα 4 Πλαίσιο Επαγρύπνησης Κυβερνοασφάλειας σε Μαθητικού Πληθυσμού

Στην Εικόνα 4 απεικονίζεται σχηματικά το προτεινόμενο Πλαίσιο Επαγρύπνησης με τα στάδια από τα οποία αποτελείται.



Εικόνα 5 Τα τμήματα του προτεινόμενου Πλαισίου και μέθοδος PDCA

Στην Εικόνα 5 παρουσιάζονται τα στάδια του προτεινόμενου Πλαισίου πάνω στον Κύκλο Ντέμιγκ (PDCA), με τον οποίο διασφαλίζεται η διαρκής βελτίωση του συστήματος από την συνεχή επανάληψή του.

5

Μεθοδολογία

Από τη μελέτη των πανελλαδικών στατιστικών του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου της Εικόνα 3, φαίνεται πως αθροιστικά το 74% του σχολικού πληθυσμού θεωρεί μεγαλύτερο κίνδυνο στο διαδίκτυο την αποκάλυψη προσωπικών δεδομένων, τον διαδικτυακό εκφοβισμό, την επαφή με αγνώστους και το sexting. Λόγω του ότι αυτοί οι κίνδυνοι είναι αλληλένδετοι και μπορούν να οδηγήσουν σε αποκάλυψη ταυτότητας και θέσης, επιλέχθηκαν ως σημείο αναφοράς για την έρευνα που θα διενεργηθεί.

Με βάση τα παραπάνω, διατυπώνουμε ως ερευνητικούς στόχους:

- Την υλοποίηση διαδραστικού υλικού ευαισθητοποίησης για προστασία αποκάλυψης θέσης και ταυτότητας.
- Να ελέγξουμε αν μπορούν να χρησιμοποιηθούν υποδομές του Πανελλήνιου Σχολικού Δικτύου με το διαδραστικό υλικό.

Με βάση τους στόχους, θέσαμε το ερευνητικά ερωτήματα:

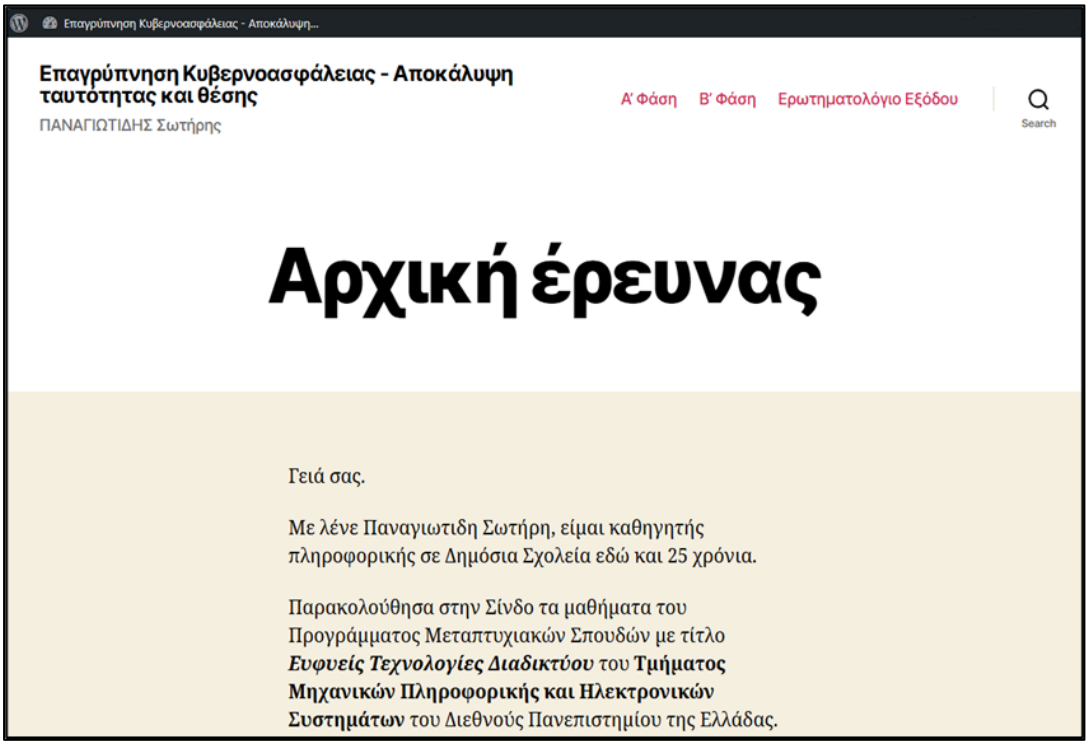
- E1: Βελτίωσε το διαδραστικό υλικό H5P και η μαθησιακή παρέμβαση την ικανότητα των μαθητών να εντοπίζουν προβληματικά σημεία σε αναρτήσεις που θα μπορούσαν να οδηγήσουν σε αποκάλυψη θέσης και ταυτότητας;
- E2: Μπορεί να χρησιμοποιηθεί παρόμοιο διαδραστικό υλικό στις υποδομές του Πανελλήνιου Σχολικού Δικτύου για ευαισθητοποίηση και επαγρύπνηση στην κυβερνοασφάλεια σχολικού πληθυσμού;

5.1 Μεθοδολογία έρευνας

Η έρευνα ήταν ποσοτική, γιατί θέλαμε μέτρηση της αντίληψης των μαθητών με ερωτήσεις πάνω στις προβαλλόμενες αναρτήσεις και τη στατιστική ανάλυση των απαντήσεων. Η συλλογή δεδομένων έγινε με δύο τρόπους. Αρχικά μέσα από το διαδραστικό υλικό H5P στο WordPress

και στο τέλος, προαιρετικά, μέσα από το ερωτηματολόγιο εξόδου 10 ερωτήσεων σε Google Forms. Η χρήση του διαδραστικού υλικού έγινε σε δύο φάσεις, την Α' Φάση και τη Β' Φάση, με διαφορετικό διαδραστικό βίντεο σε κάθε μία. Μεταξύ των φάσεων έγινε μια ολιγόλεπτη παρουσίαση με βιντεοπροβολέα και συζήτηση ευαισθητοποίησης του μαθητικού πληθυσμού για την προστασία θέσης και ταυτότητας στον κυβερνοχώρο. Η έρευνα πραγματοποιήθηκε σε σχολικό εργαστήριο πληροφορικής που είχε σε κοντινή απόσταση μεταξύ τους 15 θέσεις εργασίας σε λειτουργία και ανάλογος αριθμός μαθητών προσερχόταν για την έρευνα κάθε φορά. Η έρευνα ολοκληρώθηκε σε τέσσερις επαναλήψεις, για να προσέλθουν και οι 56 μαθητές της παρακάτω διαδικασίας.

Πρώτα καλούνταν με τη σειρά οι εθελοντές από κάθε τμήμα της Α' τάξης μέχρι να συμπληρωθούν 15. Επέλεγαν έναν από τους ανοιχτούς υπολογιστές και ένα ζευγάρι ονόματος



Εικόνα 6 Αρχική σελίδα έρευνας με τις επιλογές των Φάσεων Α' και Β'

χρήστη/κωδικού κόβοντάς το από σελίδα Α4 κατάλληλα προετοιμασμένη. Μετά μετέβαιναν και συνδέονταν στην ιστοσελίδα της έρευνας που ήταν η αρχική στους 3 φυλλομετρητές, Edge, Firefox και Chrome, κάθε υπολογιστή. Το αναγκαίο υλικό της έρευνας είχε τοποθετηθεί σε 3 σελίδες του WordPress και η κάθε μία είχε ξεχωριστό κωδικό πρόσβασης (password protected). Για διευκόλυνση στην πρόσβαση μπήκαν σε οριζόντιο μενού στο πάνω δεξί μέρος της σελίδας. Κατόπιν, τους καλούσα να πατήσουν τον σύνδεσμο που ήθελα και τους έδινα τον κωδικό εισόδου κάθε σελίδας.

Στην Α’ Φάση προβλήθηκε το 1ο διαδραστικό βίντεο 25 δευτερολέπτων, στο οποίο εμφανίζονταν με σταθερή σειρά 5 ερωτήσεις, κλειστού τύπου, σε επιλεγμένα σημεία του βίντεο με φωτογραφία ή κείμενο υποτιθέμενης ανάρτησης. Το βίντεο σταματούσε σε κάθε ερώτηση και περίμενε μέχρι να επιλέξουν οι μαθητές μία από τις τέσσερις προβαλλόμενες επιλογές, χωρίς αυτόματο χρονικό όριο απάντησης αλλά με παράκληση προφορική να αφιερώσουν λιγότερο του 1 λεπτού σε κάθε εικόνα. Μετά την επιλογή απάντησης το βίντεο προχωρούσε μέχρι την επόμενη ερώτηση έως την εμφάνιση και απάντηση των 5 ερωτήσεων. Οι απαντήσεις καταγράφηκαν μέσα στην πλατφόρμα WordPress.

Μετά το τέλος της Α’ Φάσης προβλήθηκε στον βιντεοπροβολέα της αίθουσας η παρουσίαση διάρκειας περίπου δέκα (10) λεπτών με ενημερωτικό υλικό σχετικό με την ευαισθητοποίηση και επαγρύπνηση κυβερνοασφάλειας για την αποκάλυψη θέσης και ταυτότητας στον κυβερνοχώρο. Περιείχε πληροφορίες και παραδείγματα που έδειχναν πώς μπορεί κάποιος τρίτος, με δωρεάν διαθέσιμα εργαλεία, να εντοπίσει την τοποθεσία ή και την ταυτότητα κάποιου μέσα από απρόσεκτες φωτογραφίες και κείμενα αναρτημένα στα οποία είχε πρόσβαση, για παράδειγμα ως φίλος σε κοινωνικό δίκτυο. Τέλος, έγινε συζήτηση επί των λύσεων της Α’ Φάσης.

Ακολούθησε η Β’ Φάση με το 2ο διαδραστικό βίντεο 25 δευτερολέπτων, με διαφορετική θεματολογία και καίρια σημεία, στο οποίο εμφανίζονταν και πάλι με σταθερή σειρά 5 ερωτήσεις, κλειστού τύπου, σε επιλεγμένα σημεία του βίντεο με φωτογραφία ή κείμενο υποτιθέμενης ανάρτησης. Το βίντεο σταματούσε σε κάθε ερώτηση και περίμενε, χωρίς χρονικό όριο, μέχρι να επιλέξουν οι μαθητές μία από τις τέσσερις προβαλλόμενες επιλογές. Μετά προχωρούσε μέχρι στην επόμενη ερώτηση έως την ολοκλήρωση και των 5 ερωτήσεων. Οι απαντήσεις καταγράφηκαν μέσα στην πλατφόρμα WordPress.

Σημαντική λεπτομέρεια των δύο Φάσεων ήταν η προσπάθεια αποφυγής επανάληψης παρόμοιου προβληματικού σημείου ανάρτησης όταν ήταν δυνατό. Παράδειγμα, δεν υπήρχαν δύο φωτογραφίες που να περιείχαν άγαλμα.

Τέλος, οι συμμετέχοντες κλήθηκαν να συμπληρώσουν ένα ερωτηματολόγιο εξόδου με 10 ερωτήσεις κλειστού τύπου σχετικό με την παρουσία τους σε κοινωνικά δίκτυα και την αίσθηση βελτίωσης γνώσεων.

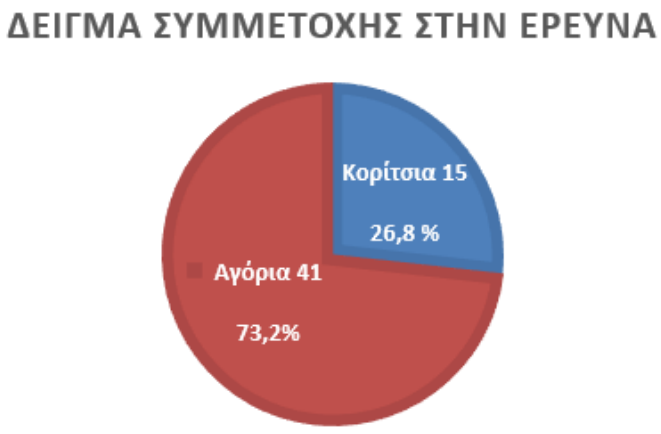
Ο συνολικός χρόνος απασχόλησης κάθε μαθητή ήταν περίπου 20’. Ο χρόνος αλλαγής τμημάτων κυμαινόταν από 5-10 λεπτά γιατί όταν τελείωνε το ένα τμήμα και έβγαινε από την αίθουσα τότε καλούσα το επόμενο τμήμα.

5.2 Δείγμα

Η έρευνα πραγματοποιήθηκε με εθελοντική συμμετοχή μαθητών/τριών της Α' τάξης πρωινού Λυκείου. Το σχολείο επιλέχθηκε βάσει του αριθμού μαθητών της Α' τάξης και της διάθεσης πραγματοποίησης της έρευνας τη συγκεκριμένη χρονική περίοδο και ήταν το μοναδικό που πληρούσε τα δύο αυτά κριτήρια. Η τάξη είχε συνολικό αριθμό 120 παιδιών χωρισμένων σε 6 τμήματα. Λόγω της ηλικίας τους, απαιτούνταν, προκειμένου να λάβουν μέρος στην έρευνα, η ενημέρωση και συγκατάθεση των κηδεμόνων τους. Για τον λόγο αυτόν, δόθηκε σε όλους σχετικό έγγραφο παροχής συγκατάθεσης. Το έγγραφο συγκατάθεσης το επέστρεψαν υπογεγραμμένο 57 παιδιά, από τα οποία το ένα απέσυρε τη συμμετοχή του για άγνωστο λόγο, και συμμετείχαν τελικά στην έρευνα 56 παιδιά (n=56), από τα οποία 41 αγόρια και 15 κορίτσια.

Πίνακας 3 Δείγμα συμμετοχής στην έρευνα

	Αριθμός	Ποσοστό συνόλου
Αγόρια	41	73 %
Κορίτσια	15	27 %
Σύνολο	56	100 %



Διάγραμμα 1 Ποσοστά συμμετοχής ανά φύλο

Στο Διάγραμμα 1 και στον Πίνακας 3 βλέπουμε ότι πήραν μέρος στην έρευνα 41 αγόρια, ποσοστό 73% και 15 κορίτσια, ποσοστό 27%. Η ηλικία όλων ήταν 15-16 ετών ως μαθητές της Α' Λυκείου.

5.3 Σύστημα έρευνας και δημιουργία μαθήματος

5.3.1 Σχεδίαση συστήματος έρευνας

Στην Ενότητα αυτή περιγράφεται η σχεδίαση του συστήματος με το οποίο έγινε η συλλογή των δεδομένων της έρευνας και ο τρόπος επιλογής των συστατικών του. Το σημαντικότερο συστατικό γύρω από το οποίο έγιναν όλες οι δοκιμές ήταν το δωρεάν εργαλείο ανάπτυξης διαδραστικού υλικού H5P. Ακολουθούν όλα τα κριτήρια επιλογής για το σύστημα:

- αν είναι ανοιχτού κώδικα,
- αν είναι εύκολη η χρήση του συστήματος από αρχάριους
- τη συμβατότητα με H5P

Εργαλείο Ανάπτυξης Περιεχομένου.

Ως εργαλείο ανάπτυξης του περιεχόμενου της έρευνας επιλέχθηκε η H5P [36] για τους εξής λόγους:

a. παρέχεται δωρεάν για χρήση [37] και έχει πλούσια βιβλιοθήκη, συνολικά 54 εργαλεία δημιουργίας Δραστηριοτήτων (Activities), όπως απλά Κουίζ, Χάρτη Παιχνιδιού (για παιχνιδοποίηση) και Διαδραστικά Βίντεο [38] [8].
b. υποστηρίζει WordPress, Moodle, OpenEclass.
c. έχει εύκολη δημιουργία περιεχομένου (content) μέσα από τον ενσωματωμένο διορθωτή (editor) που περιέχει το πρόσθετο της H5P στην πλατφόρμα που χρησιμοποιήθηκε (WordPress, Moodle, OpenEclass) αλλά και τοπικά με την δωρεάν εφαρμογή LUMI [39].
d. το περιεχόμενο H5P μπορεί να επαναχρησιμοποιηθεί και να τροποποιηθεί, να εξαχθεί και να εισαχθεί σε κάθε πλατφόρμα που το υποστηρίζει. Παράδειγμα, ένα διαδραστικό βίντεο, που στηρίζεται σε ένα τοπικό βίντεο ή σε βίντεο Youtube, μπορούν να προστεθούν και να τροποποιηθούν τα σημεία ερωτήσεων και οι απαντήσεις τους, να προστεθούν επισημάνσεις, καθώς και να μεταφερθεί ο μαθητής σε άλλο σημείο του βίντεο ανάλογα με την απάντηση (Action on wrong) και να τελειώσει η προβολή στο επιθυμητό σημείο του βίντεο.
e. προσφέρει βαθμολογία και ανατροφοδότηση του μαθητή τη στιγμή που επιλέγει απάντηση.
f. της σύστασής του από έρευνες [8], [40], [41]
g. την προσωπική εμπειρία που είχα από τη χρήση του στις πλατφόρμες OpenEclass [42] και e-Me [43] του Ελληνικού Πανελλήνιου Σχολικού Δικτύου.

Πλατφόρμα υλοποίησης

Για πλατφόρμα υλοποίησης της έρευνας εξετάστηκαν 3 διαφορετικές ανοιχτού λογισμικού (open source). Η ευρύτατα χρησιμοποιούμενη από τα ελληνικά εκπαιδευτικά ιδρύματα πλατφόρμα ηλεκτρονικής μάθησης OpenEclass [44], το παγκοσμίως αναγνωρισμένο σύστημα διαχείρισης μάθησης Moodle [45] και, τέλος, το διασημότερο σήμερα σύστημα διαχείρισης διαδικτυακού περιεχομένου WordPress [46].

OpenEclass

Όπως φαίνεται και στον Πίνακας 4, το OpenEclass επιτρέπει την εκτέλεση και δημιουργία περιεχομένου H5P. Δεν υπάρχει όμως η δυνατότητα λήψης και εμφάνισης των βαθμών όσων χρηστών εκτέλεσαν κάποια δραστηριότητα H5P. Μετά από ηλεκτρονική επικοινωνία με την υποστήριξη του OpenEclass δήλωσαν πως αυτό είναι στα μελλοντικά σχέδιά τους. Απορρίφθηκε, λόγω έλλειψης δυνατότητας εμφάνισης βαθμών χρηστών.

Moodle

Στο Moodle v4.3.1 η εγκατάσταση του πρόσθετου, η εκτέλεση και η δημιουργία περιεχομένου H5P έγινε χωρίς πρόβλημα. Οι τελικές βαθμολογίες πέρασαν στο βαθμολόγιο και υπήρχε η δυνατότητα προβολής των απαντήσεων που έδωσε ο χρήστης, όμως έδειχνε μία κάθε φορά. Για εκτεταμένες δυνατότητες προβολής αποτελεσμάτων θα έπρεπε να γίνει χρήση εξωτερικών ειδικών πλατφορμών που αποθηκεύουν τα δεδομένα μαθησιακών δραστηριοτήτων LRS (Learning Record Store) [47]. Οι πλατφόρμες αυτές, όταν προσφέρουν και δωρεάν χρήση τους, τότε έχουν περιορισμένες δυνατότητες και επίσης δεν είναι εύκολη πάντα η διασύνδεσή τους με το Moodle και σε συνδυασμό με την πολυπλοκότητα του Moodle απορρίφθηκε.

Wordpress

Τέλος, δοκιμάστηκε το WordPress v6.4.4, στο οποίο η εγκατάσταση και χρήση του πρόσθετου H5P έγινε χωρίς κανένα πρόβλημα. Οι βαθμολογίες κάθε χρήστη, αλλά και όλων των δραστηριοτήτων που υπήρχαν ανεβασμένα στο WordPress, μπορούσαν να βρεθούν στην περιοχή διαχείρισης του WordPress (wp-admin), στο σημείο H5P Content / All H5P Content. Για οποιαδήποτε άλλη προβολή περισσότερων λεπτομερειών των αποτελεσμάτων, εκτός των LRS που προτείνονταν και για το Moodle, υπήρχε ένα ακόμη πρόσθετο που προτείνει ο Οργανισμός H5P, το δωρεάν H5PxAPIkatchu [47], [48]. Το H5PxAPIkatchu καταγράφει όλα τα συμβάντα xAPI (Experience API) [49] που συμβαίνουν στην H5P μέσα στα αποτελέσματα και είναι πολλά περισσότερα σε σχέση με το πρότυπο SCORM. Το H5PxAPIkatchu εγκαταστάθηκε και λειτούργησε άψογα. Οι ρυθμίσεις του γίνονται από την περιοχή Διαχείρισης του WordPress (wp-admin) στο υπομενού *Ρυθμίσεις / H5PxAPIkatchu.* Μετά από

δοκιμή προβλήθηκαν τα αποτελέσματα των κινήσεων που έκανε ένας χρήστης μέσα σε μία δραστηριότητα, όπως τι απάντησε σε κάθε ερώτηση, πόσο χρόνο έκανε, πόσες φορές και τι βαθμολογία πήρε κάθε φορά. Το μειονέκτημα του H5PxAPIkatchu είναι πως όλες αυτές οι πληροφορίες μπορούν να ληφθούν τοπικά σε μορφή CSV, που σημαίνει πως θα πρέπει να αφιερωθεί χρόνος επεξεργασίας τους για να εξαχθούν τα επιθυμητά στοιχεία.

Η αποτελεσματικότητα H5P και H5PxAPIkatchu στο WordPress κρίθηκε ικανοποιητική και επιλέχθηκε για τη διενέργεια της έρευνας.

Πίνακας 4 Σύγκριση εργαλείων για υλοποίηση συστήματος με υποστήριξη H5P

	OpenEclass 3.15	**Moodle 4.2.1**	**WordPress 6.4.4**
Πού έγινε η δοκιμή	Στο eclass.sch.gr	Προσωπικό διακομιστή	Προσωπικό διακομιστή
Υποστήριξη H5P εκτέλεσης και δημιουργίας περιεχομένου	ΝΑΙ	ΝΑΙ (με εγκατάσταση του πρόσθετου H5P)	ΝΑΙ (με εγκατάσταση του πρόσθετου H5P)
Εμφάνιση τελικής βαθμολογίας των χρηστών	ΟΧΙ	ΝΑΙ	ΝΑΙ
Εμφάνιση απαντήσεων που δόθηκαν ανά ερώτηση χωρίς άλλο πρόσθετο	ΟΧΙ	ΝΑΙ, μία απάντηση για έναν χρήστη κάθε φορά	ΟΧΙ
Εμφάνιση όλων των κινήσεων κάθε χρήστη (χρόνους απαντήσεων, κ.λπ.)	ΟΧΙ	Μόνο μέσω εξωτερικού LRS (Learning Record Store)	1. εσωτερικά με πρόσθετο SNORDIAN's H5PxAPIkatchu (CSV) 2. μέσω εξωτερικού LRS
Υποστηρίζεται από το Ελληνικό Πανελλήνιο Σχολικό Δίκτυο	ΝΑΙ	ΝΑΙ	ΝΑΙ
Εύκολη χρήση από αρχάριο	7/20	5/10	9/10

Επιλεγμένη σύνθεση του συστήματος για την υλοποίηση της έρευνας

Πίνακας 5 Σύνθεση συστήματος διενέργειας της έρευνας

Λειτουργίες	**Ονομασία και έκδοση που χρησιμοποιήθηκε**
Πλατφόρμα διαχείρισης περιεχομένου.	WordPress v6.4.4
Πρόσθετο του WP για δημιουργία, εκτέλεση δραστηριοτήτων H5P (core) με ενσωματωμένο διορθωτή.	H5P v1.15.7
Δραστηριότητα βιβλιοθήκης H5P για τη δημιουργία του διαδραστικού βίντεο.	Interactive Video v.1.16.30
Πρόσθετο του WP για καταγραφή των κινήσεων των χρηστών εντός των δραστηριοτήτων της H5P και εξαγωγή τους σε CSV.	H5PxAPIkatchu v0.4.13
Πρόσθετο του WP για μαζική δημιουργία χρηστών από CSV	Import and export users and customers v1.26.8

5.3.2 Δημιουργία περιεχομένου της έρευνας.

Για κάθε διαδραστικό βίντεο της H5P δημιουργήθηκε βίντεο διάρκειας 25 δευτερολέπτων που κατασκευάστηκε με τη δωρεάν εφαρμογή Microsoft Cliphamp σε Windows 11. Για τη δημιουργία κάθε βίντεο χρησιμοποιήθηκαν πέντε (05) εικόνες με περιεχόμενο κάποια υποτιθέμενη συνομιλία ή φωτογραφία που ανέβηκε σε κοινωνικό δίκτυο. Κάθε εικόνα επιλέχθηκε με τυχαία σειρά να προβάλλεται για 5 δευτερόλεπτα μέσα στο βίντεο. Έτσι, από τις 5 διαφορετικές φωτογραφίες δημιουργήθηκε ένα βίντεο 25 δευτερολέπτων για κάθε μία από τις δύο Φάσεις. Όλες οι φωτογραφίες ήταν δικής μου δημιουργίας ή δημιουργήθηκαν με τη βοήθεια του DALL-E 2 της OpenAI, που, σύμφωνα με τους όρους χρήσης, μου ανήκουν [50]. Προτιμήθηκε η δημιουργία και προβολή βίντεο για να χρησιμοποιηθεί η βιβλιοθήκη Διαδραστικό Βίντεο (Interactive Video) της H5P και η χρήση των δυνατοτήτων που προσφέρει αυτή. Τέλος, τα δυο διαδραστικά βίντεο ονομάστηκαν, αντίστοιχα, Α’ Φάση και Β’ Φάση και χρησιμοποιήθηκαν στις αντίστοιχες δύο Φάσεις της έρευνας.

5.3.3 Συλλογή δεδομένων φάσεων και ερωτηματολογίου

Η συλλογή δεδομένων έγινε με δύο τρόπους:

A. Από τα διαδραστικά βίντεο H5P Α’ Φάσης και Β’ Φάσης

   Κατά την εκτέλεση κάθε διαδραστικού βίντεο H5P στο WordPress από συνδεμένους χρήστες, καταχωρούνται τα αποτελέσματα στο πρόσθετο H5P και ο Διαχειριστής του WordPress μπορεί να δει τους βαθμούς όλων όσων εκτέλεσαν κάθε δραστηριότητα. Δεν υπάρχει επιλογή εξαγωγής μόνο της βαθμολογίας, αλλά μπορεί να επιλεχθούν εύκολα.

   Για να ληφθούν όλες οι λεπτομέρειες από τις ενέργειες ενός συνδεμένου χρήστη, όπως απαντήσεις ανά ερώτηση, πόσες φορές την απάντησε και πώς την απάντησε, θα χρειαστεί ο Διαχειριστείς να μεταβεί και επιλέξει το πρόσθετο H5PxAPIkatchu στο διαχειριστικό περιβάλλον του WordPress, όπου μπορεί να δει όλες τις ενέργειες όλων των χρηστών που είχαν κάποια διάδραση με περιεχόμενο H5P, αλλά και να κάνει λήψη τους σε μορφή CSV.

Εικόνα 7 Διαχειριστικό περιβάλλον H5PxAPIkatchu για H5P Analytics

Η Εικόνα 7 δείχνει τις επιλογές που έχει ο Διαχειριστής πάνω στα δεδομένα καταγραφής των ενεργειών των χρηστών H5P δραστηριοτήτων μεταξύ των οποίων είναι η Λήψη τους και το φιλτράρισμα. Φαίνεται περιορισμένος αριθμός στηλών.

Β. Από το Ερωτηματολόγιο Εξόδου, Google Forms, συνολικά 10 ερωτήσεων (Παράρτημα Δ).

Το Ερωτηματολόγιο εξόδου δημιουργήθηκε στο Google Form, είχε συνολικά 10 ερωτήσεις σχετικές με συνήθειές τους σε κοινωνικά δίκτυα και την ικανοποίησή τους από όσα έμαθαν κατά τη διάρκεια της έρευνας.

6

Αποτελέσματα ερευνών και Συζήτηση Αποτελεσμάτων

Στο Κεφάλαιο αυτό περιγράφονται οι περιορισμοί και τα προβλήματα που συναντήθηκαν για τη διεκπεραίωση της έρευνας, τα αποτελέσματα που ελήφθησαν από τις Φάσεις Α' και Β', καθώς και από το ερωτηματολόγιο εξόδου, και στο τέλος της γίνεται η συζήτηση των αποτελεσμάτων.

6.1 Εισαγωγή

Η συλλογή δεδομένων έγινε πρώτα για την αποτελεσματικότητα του υλικού που παρουσιάστηκε κατά την Α' Φάση και Β' Φάση με διαδραστικό περιεχόμενο H5P στο WordPress και λήφθηκε σε μορφή CSV για να γίνει επεξεργασία και διαγράμματα με το Microsoft Excel 365. Κατόπιν, δεδομένα συλλέχθηκαν και από ερωτηματολόγιο εξόδου σε Google Forms, με 10 ερωτήσεις σχετικές με συνήθειές τους σε κοινωνικά δίκτυα και το βαθμό ικανοποίησης από το μάθημα παρουσίαση. Η εξαγωγή τους έγινε σε μορφή XSLX και η επεξεργασία και τα διαγράμματα με το Microsoft Excel 365.

6.2 Περιορισμοί και προβλήματα

Περιορισμός ήταν η άδεια διεξαγωγής της έρευνας που ήταν αναγκαία από το Σχολείο και την επιτροπή ΕΗΔΕ. Η άδεια του σχολείου δόθηκε από τον Διευθυντή του σχολείου, σύμφωνα με ισχύουσα νομοθεσία, αλλά και από την Επιτροπή Ηθικής και Δεοντολογίας της Έρευνας (Ε.Η.Δ.Ε.) του Διεθνούς Πανεπιστημίου της Ελλάδος (ΔΙ.ΠΑ.Ε.).

Περιορισμός υπήρχε και για τη συμμετοχή των ανήλικων μαθητών, για την οποία προβλεπόταν να δοθεί υποχρεωτικά έντυπη έγκριση από τους κηδεμόνες τους, αφού προηγουμένως είχαν εγγράφως ενημερωθεί για όλα όσα προβλέπει το Υπουργείο Παιδείας και η Επιτροπή Ηθικής και Δεοντολογίας της Έρευνας του ΔΙ.ΠΑ.Ε.

Περιορισμός είχε τεθεί στον συνολικό χρόνο ολοκλήρωσης και απασχόλησης των μαθητών από το σχολείο, ο οποίος δεν έπρεπε να υπερβαίνει τις δύο διδακτικές ώρες συνολικά. Αυτό δημιούργησε πίεση και στο υλικό που θα μπορούσε να προβληθεί για ευαισθητοποίηση αλλά και στο διαδραστικό βίντεο που θα δινόταν κατά τη διάρκεια των Φάσεων Α' και Β'. Δεν μπορούσε να γίνει ταυτόχρονα σε όλους τους μαθητές. Στο εργαστήριο μπορούσαν να συνδεθούν μέχρι δεκαπέντε μαθητές, ενώ συνολικά συμμετείχαν πενήντα έξι μαθητές, και θα έπρεπε να γίνει εναλλαγή τους τρεις φορές. Επομένως, θα χρειαζόταν πολύτιμος χρόνος και για τις αλλαγές. Άρα, θα διαμορφώνονταν 4 τμήματα που θα λάμβαναν μέρος, μέσα σε 2 ώρες μαζί με τα διαλλείματα. Τελικά θα ήταν διαθέσιμα περίπου 30' για κάθε τμήμα, χρόνος στον οποίο συμπεριλαμβάνονται η αλλαγή τμήματος και η σύνδεση στο σύστημα WP. Οι αλλαγές και το διάλλειμα ήταν ένα επιπλέον πρόβλημα, εξαιτίας της επαφής ατόμων που πήραν μέρος με αυτά που δεν είχε έρθει ακόμη η σειρά τους.

Εντός του εργαστηρίου πληροφορικής που έγινε η έρευνα, οι θέσεις εργασίας βρίσκονταν σε απόσταση τέτοια που θα μπορούσε να δει κάποιος και τις οθόνες των διπλανών υπολογιστών.

Εν δυνάμει πρόβλημα ανάλογων εφαρμογών βαθμολόγησης περιεχομένου είναι η εκτέλεσή τους τοπικά στον φυλλομετρητή. Οι σωστές απαντήσεις, δηλαδή, βρίσκονται στις πληροφορίες που έχουν κατέβει στον φυλλομετρητή και ίσως μπορέσουν να αποκτηθούν από τους χρήστες.

Σημαντικό πρόβλημα ήταν και η εύρεση κατάλληλου φωτογραφικού υλικού, χωρίς περιορισμούς, που να περιέχει θέμα ανάλογο με αυτό που χρειαζόταν από τα κρισιμότερα. Για παράδειγμα, πού θα μπορούσε να βρεθεί φωτογραφία παρέας νεαρών ατόμων να κάθονται σε καφετέρια, πίσω τους να έχει μεγάλα παράθυρα, από τα οποία να φαίνονται ένα άγαλμα, πάρκο και ένα γωνιακό νεοκλασικό κτίριο. Η λύση προέκυψε από την OpenAI με το DALL-E 2, που μπορεί και δημιουργεί εικόνες σύμφωνα με τις προτροπές (prompts) και παραχωρεί τα δικαιώματα σε αυτούς που έδιναν τις προτροπές [50].

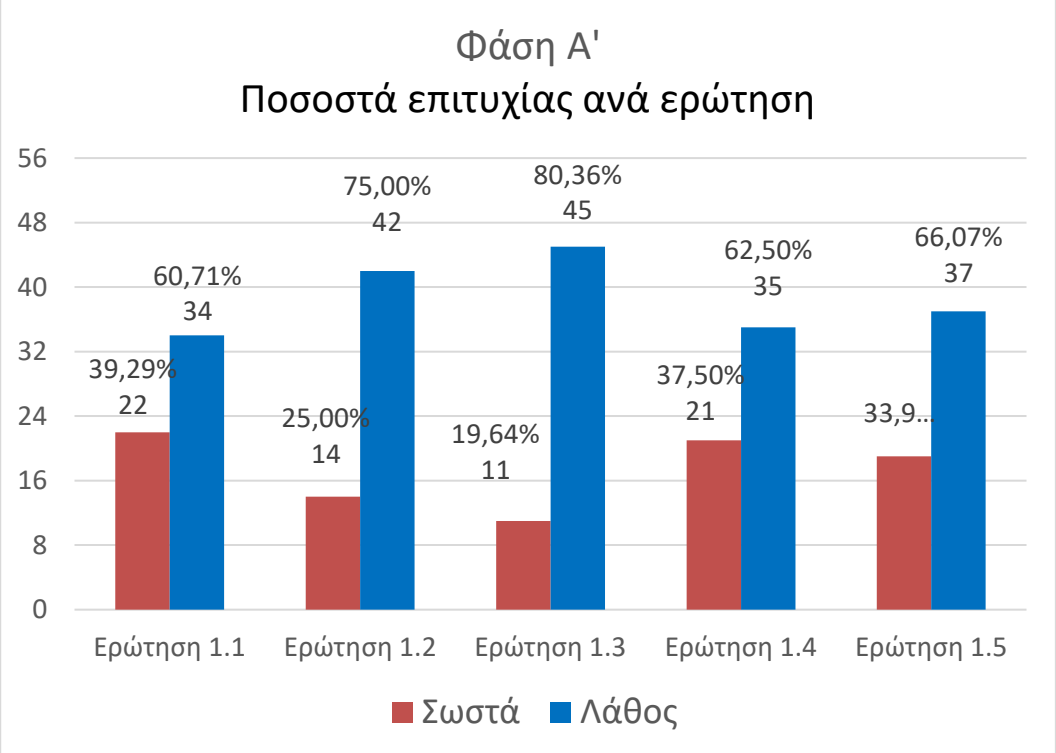
6.3 *Αποτελέσματα μετρήσεων Α' και Β' Φάσης*

6.3.1 *Αποτελέσματα Α' Φάσης*

Πίνακας 6 Συγκεντρωτικός πίνακας αποτελεσμάτων Α' Φάσης

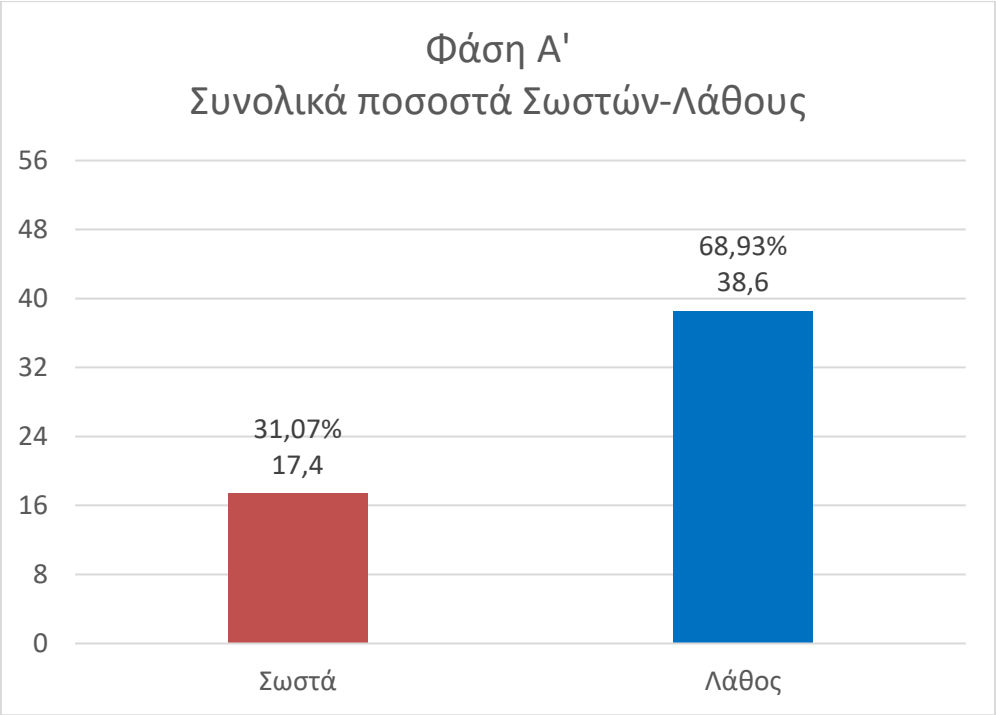
Φάση Α				
	Σωστά	**Λάθος**	**Σωστά %**	**Λάθος %**
Ερώτηση 1.1	22	34	39,29%	60,71%
Ερώτηση 1.2	14	42	25,00%	75,00%
Ερώτηση 1.3	11	45	19,64%	80,36%
Ερώτηση 1.4	21	35	37,50%	62,50%
Ερώτηση 1.5	19	37	33,93%	66,07%
Μέσος Όρος	17,4	38,6	**31,07%**	**68,93%**

Στον Πίνακα 5 βλέπουμε τον αριθμό και τα ποσοστά ανά ερώτηση της Α' Φάσης. Παρατηρούμε πως το ποσοστό επιτυχίας των Σωστών κυμάνθηκε μεταξύ 19,64 – 39,29% με Μέσο Όρο 31,07% και αντίστοιχα των Λανθασμένων κυμάνθηκε μεταξύ 60,71 – 80,36%, με Μέσο Όρο 68,93%. Από τον πίνακα συμπεραίνουμε πως απαντήθηκαν 5 ερωτήσεις από 56 άτομα.



Διάγραμμα 2 Συγκεντρωτικά αποτελέσματα ανά ερώτηση Α' Φάσης

Στο Διάγραμμα 2 μπορούμε να δούμε τη διαφορά μεταξύ των σωστών και λάθους κάθε μίας από τις πέντε ερωτήσεις της Α’ Φάσης. Παρατηρούμε πως η Ερώτηση 1.1 είχε το υψηλότερο ποσοστό επιτυχίας 29,42% από 22 άτομα ενώ η Ερώτηση 1.3 είχε το χαμηλότερο ποσοστό επιτυχίας από 19,64% από 11 άτομα.



Διάγραμμα 3 Συνολικά ποσοστά και αριθμός Σωστών/Λάθους Α' Φάσης

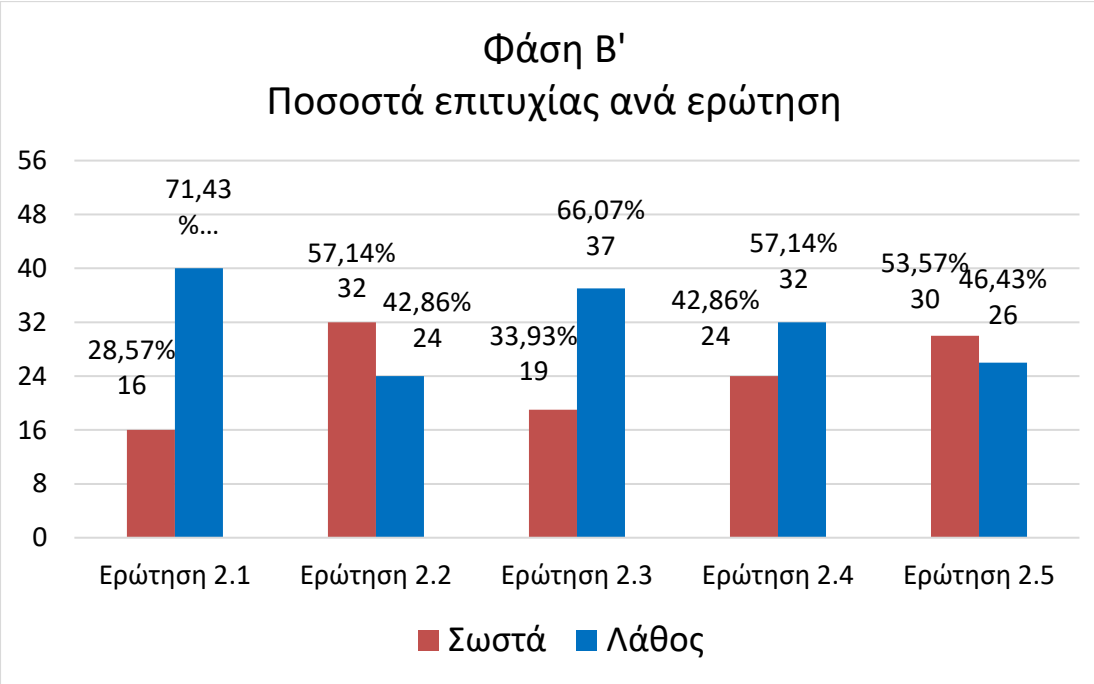
Το Διάγραμμα 3 εμφανίζει τον μέσο όρο αριθμού απαντήσεων των Σωστών και των Λανθασμένων της Α’ Φάσης με τον ΜΟ Σωστών να είναι 17,4 (31,07%) και τον ΜΟ των Λανθασμένων να ήταν 38,6 (68,93%).

6.3.2 Αποτελέσματα Β' Φάσης

Πίνακας 7 Συγκεντρωτικός πίνακας αποτελεσμάτων Β' Φάσης

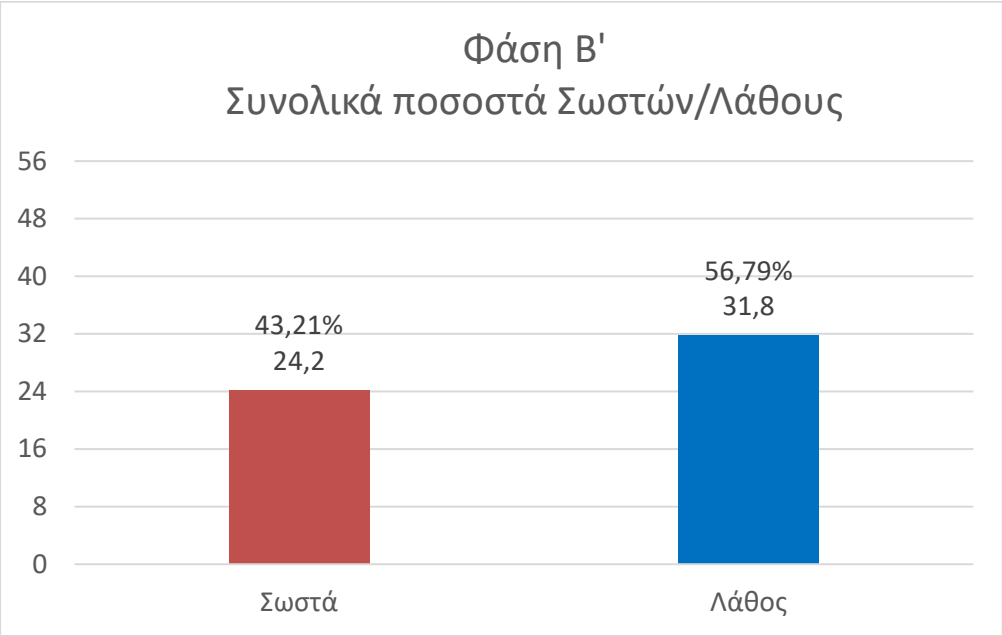
Φάση Β'				
	Σωστά	**Λάθος**	**Σωστά %**	**Λάθος %**
Ερώτηση 2.1	16	40	28,57%	71,43%
Ερώτηση 2.2	32	24	57,14%	42,86%
Ερώτηση 2.3	19	37	33,93%	66,07%
Ερώτηση 2.4	24	32	42,86%	57,14%
Ερώτηση 2.5	30	26	53,57%	46,43%
ΜΟ	24,2	31,8	**43,21%**	**56,79%**

Στον Πίνακα 6 βλέπουμε τον αριθμό και τα ποσοστά ανά ερώτηση της Β' Φάσης. Παρατηρούμε πως το ποσοστό επιτυχίας των Σωστών κυμάνθηκε μεταξύ 28,57 – 57,14% με Μέσο Όρο 43,21% και αντίστοιχα των Λανθασμένων κυμάνθηκε μεταξύ 42,86 – 71,43%, με Μέσο Όρο 56,79%. Στον πίνακα βλέπουμε πως 5 ερωτήσεις απαντήθηκαν από 56 άτομα.



Διάγραμμα 4 Συγκεντρωτικά αποτελέσματα ανά ερώτηση Β' Φάσης

Στο Διάγραμμα 4 βλέπουμε τη διαφορά μεταξύ των σωστών και λάθους κάθε μίας από τις πέντε ερωτήσεις της Β' Φάσης. Παρατηρούμε πως η Ερώτηση 2.2 είχε το υψηλότερο ποσοστό επιτυχίας με 32 Σωστές (57,14%) ενώ η Ερώτηση 2.1 είχε το χαμηλότερο ποσοστό επιτυχίας 16 Σωστές (28,57%).



Διάγραμμα 5 Συνολικά ποσοστά Σωστών/Λάθους Β' Φάσης

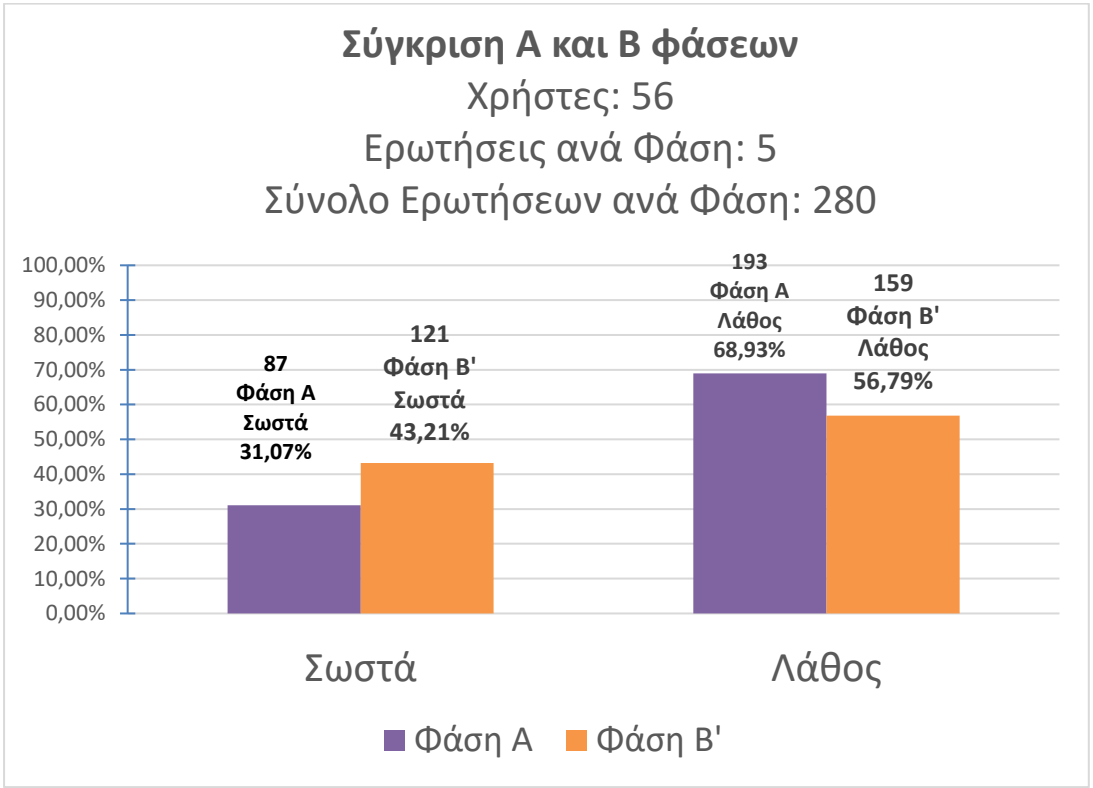
Το Διάγραμμα 5 εμφανίζει τον μέσο όρο των Σωστών και των Λανθασμένων απαντήσεων της Β’ Φάσης, με τις Σωστές να είναι κατά ΜΟ 24,2 ποσοστό 43,21%, ενώ οι Λάθος να είναι κατά ΜΟ 31,8 ποσοστό 56,79%.

6.3.3 Σύγκριση αποτελεσμάτων Α' και Β' Φάσης

Πίνακας 8 Συγκριτικός πίνακας αποτελεσμάτων Α' και Β' Φάσεων

	Σωστά	**Λάθος**
Φάση Α	**31,07%**	**68,93%**
Φάση Β'	**43,21%**	**56,79%**
Ποσοστιαία Μεταβολή Β' Φάσης	+12,14%	

Στον Πίνακα 7 βλέπουμε τη σύγκριση των ποσοστών μεταξύ των δύο Φάσεων και παρατηρούμε πως υπήρξε βελτίωση με αύξηση των Σωστών κατά 12% στη Β' Φάση σε σχέση με την Α' Φάση.



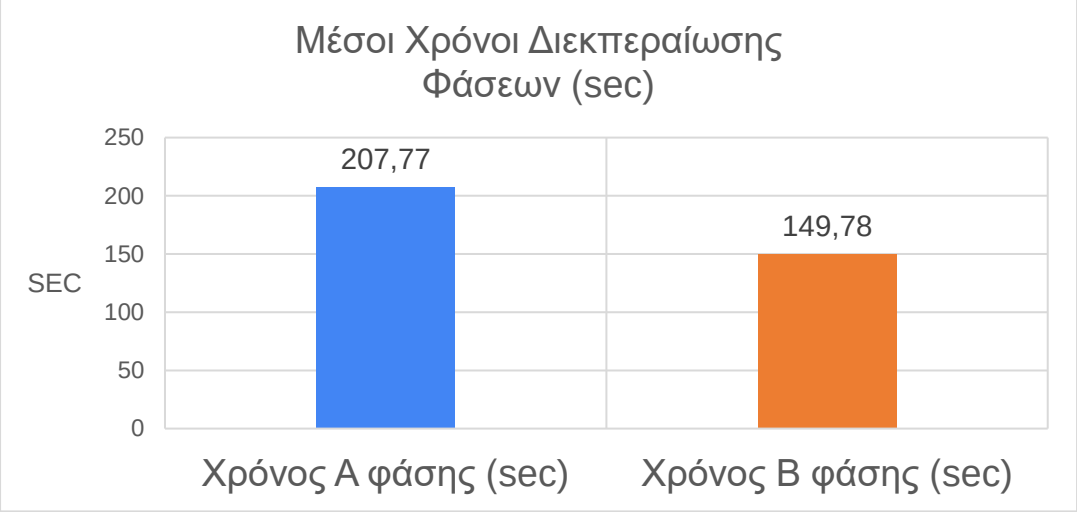
Διάγραμμα 6 Συγκριτικό διάγραμμα Σωστών/Λάθους Α' και Β' Φάσης

Το Διάγραμμα 6 μας δίνει τη δυνατότητα να δούμε εύκολα τη βελτίωση των Σωστών της Β' Φάσης σε σχέση με της Α' Φάσης. Η βελτίωση εύρεσης των Σωστών ήταν 12% κατά τη Β' Φάση.

Πίνακας 9 Συγκριτικός πίνακας Μέσων Χρόνων διεκπεραίωσης Α' και Β΄ Φάσης

	Χρόνος Α’ φάσης (sec)	Χρόνος Β’ φάσης (sec)
Μέσος Χρόνος Διεκπεραίωσης Φάσης	207,77	149,78
Βελτίωση Μέσου Χρόνου Β φάσης		**27,91 %**

Ο Πίνακας 8 μας δίνει τους Μέσους Χρόνους διεκπεραίωσης κάθε Φάσης από τους χρήστες. Παρατηρούμε τη σημαντική μείωση του χρόνου διεκπεραίωσης της Β’ Φάσης κατά 27,91%. Τα άτομα απαντούσαν γρηγορότερα στις ερωτήσεις που τους τέθηκαν.



Διάγραμμα 7 Συγκριτικό διάγραμμα Μέσου Χρόνου διεκπεραίωσης Α' και Β' Φάσης

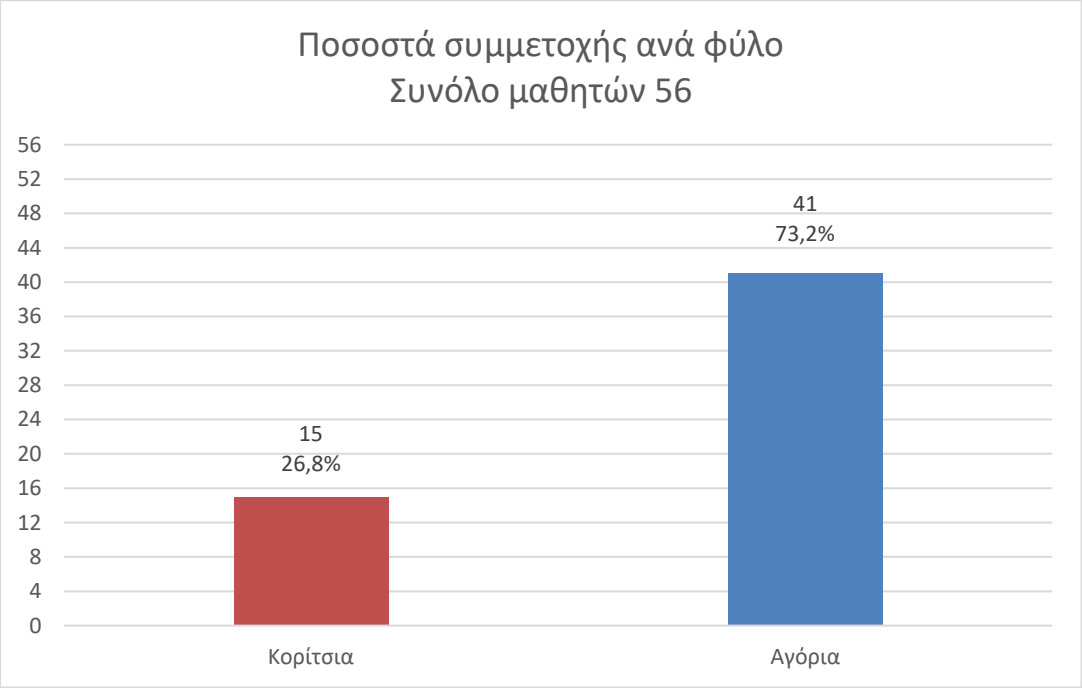
Στο Διάγραμμα 7 βλέπουμε την οπτική αναπαράσταση του Μέσου Χρόνου διεκπεραίωσης κάθε Φάσης με εμφανή τη μείωση του απαιτούμενου χρόνου κατά 27,91%.

6.4 *Αποτελέσματα ερωτηματολόγιου εξόδου*

Πίνακας 10 Αριθμός συμμεχώντων ανά φύλο

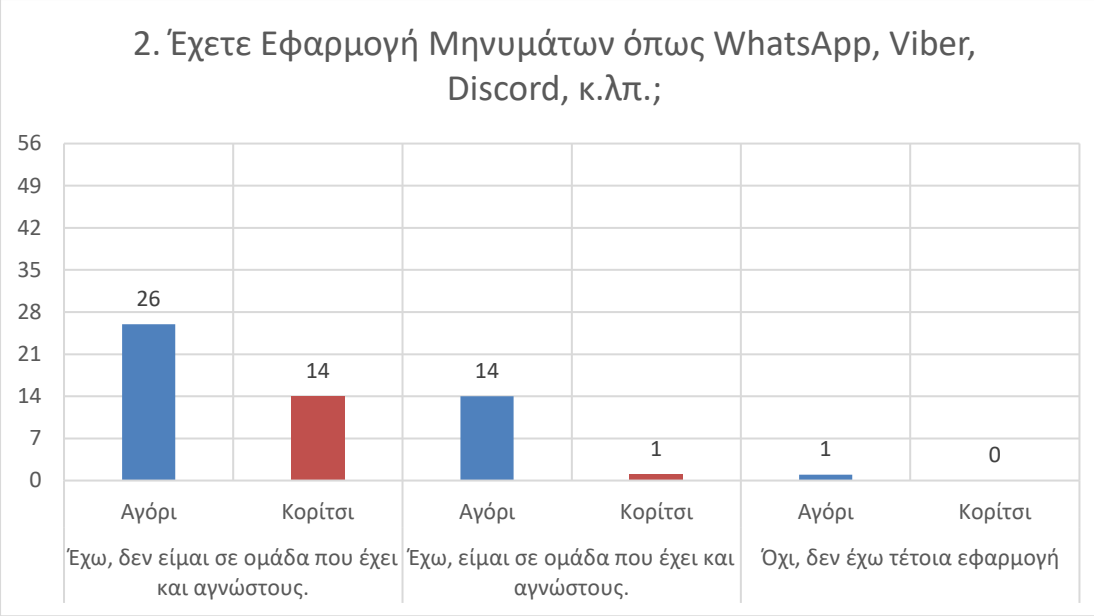
	Αριθμός	Ποσοστό συνόλου
Αγόρια	41	73.2 %
Κορίτσια	15	26.8 %
Σύνολο	56	100 %

Στον Πίνακα 9 βλέπουμε τον συνολικό αριθμό μαθητών και το ποσοστό αγοριών και κοριτσιών που πήρε μέρος στην έρευνα. Συνολικά ήταν 56 μαθητές, με τα αγόρια να ήταν 41, ποσοστό 73,2 %, και τα κορίτσια 15, ποσοστό 26,8%



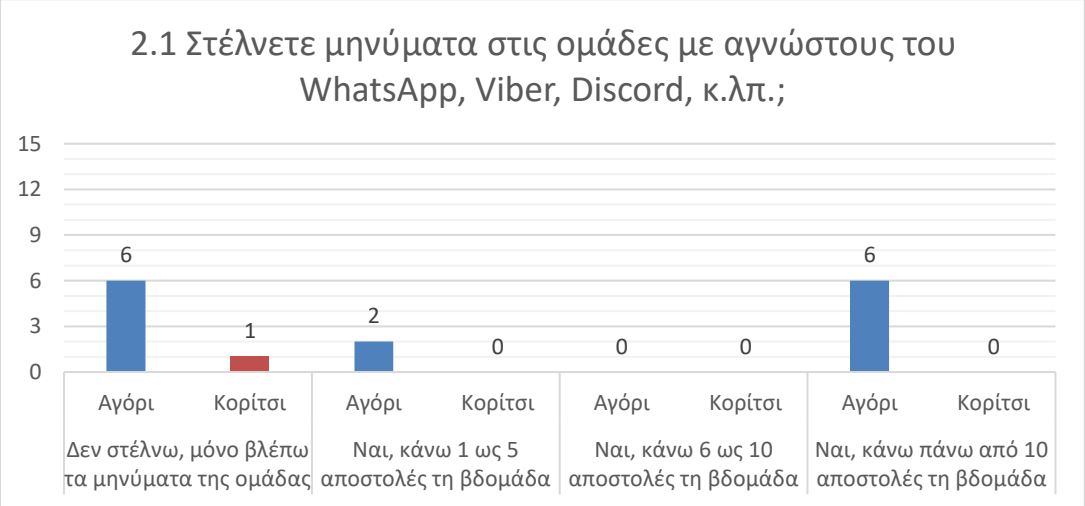
Διάγραμμα 8 Ερώτηση 1 Φύλο

Το Διάγραμμα 8 δείχνει τον συνολικό αριθμό μαθητών (56) που πήρε μέρος στην έρευνα ανά φύλο. Τα αγόρια ήταν 41, ποσοστό 73,2 %, και τα κορίτσια 15, ποσοστό 26,8%.



Διάγραμμα 9 Ερώτηση 2 - Έχετε Εφαρμογή Μηνυμάτων όπως WhatsApp, Viber, Discord, κ.λπ.

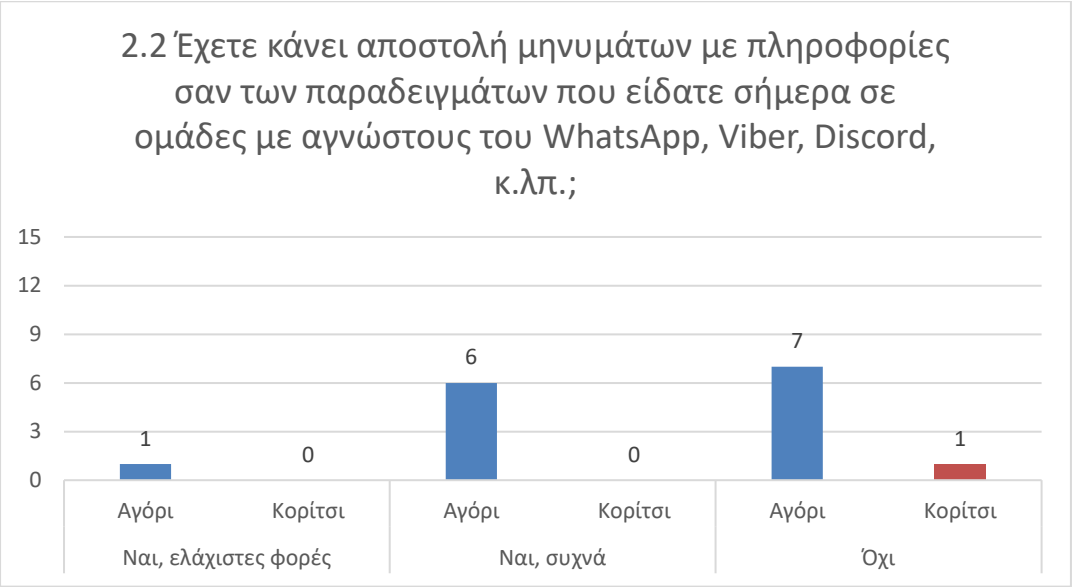
Στο Διάγραμμα 9 βλέπουμε τα ποσοστά αγοριών και κοριτσιών που έχουν ή δεν έχουν εφαρμογή μηνυμάτων με Ομάδες και Κανάλια. Παρατηρούμε πως συνολικά 55 στους 56 ποσοστό 98,2% έχουν τέτοια εφαρμογή. Οι 40 στους 55 με την εφαρμογή (72,72%) αν και έχουν την εφαρμογή δεν συμμετέχουν σε ομάδες με αγνώστους και στα κορίτσια το ποσοστό αυτό φτάνει στο 93% (14 στα 15). Τα 15 άτομα από τα 55 με την εφαρμογή (27,27%) συμμετέχουν σε ομάδες με αγνώστους και ένα μόνο αγόρι δεν έχει τέτοια εφαρμογή μηνυμάτων.



Διάγραμμα 10 Ερώτηση 2.1 Στέλνετε μηνύματα στις ομάδες με αγνώστους του WhatsApp, Viber, Discord, κ.λπ.

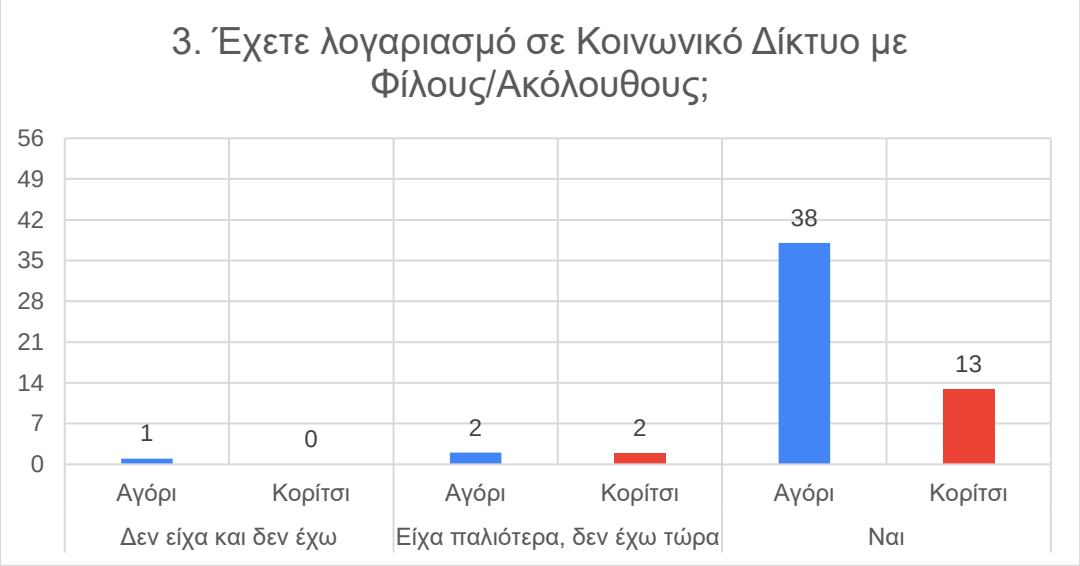
Στο Διάγραμμα 10 βλέπουμε πως από τους 15 (από τις απαντήσεις Ερώτησης 2) που είναι σε ομάδες με αγνώστους οι 7, σχεδόν 47%, δεν στέλνουν μηνύματα, αλλά απλά διαβάζουν τι γράφουν οι άλλοι. Δήλωσαν 2 αγόρια, σχεδόν 13%, πως κάνουν από 1-5 αποστολές τη

βδομάδα. Κανένα (0) Αγόρι και Κορίτσι δεν απάντησε πως κάνει από 6 έως 10 αποστολές, ενώ πάνω από 10 μηνύματα τη βδομάδα στέλνουν 6 αγόρια, ποσοστό 40%.



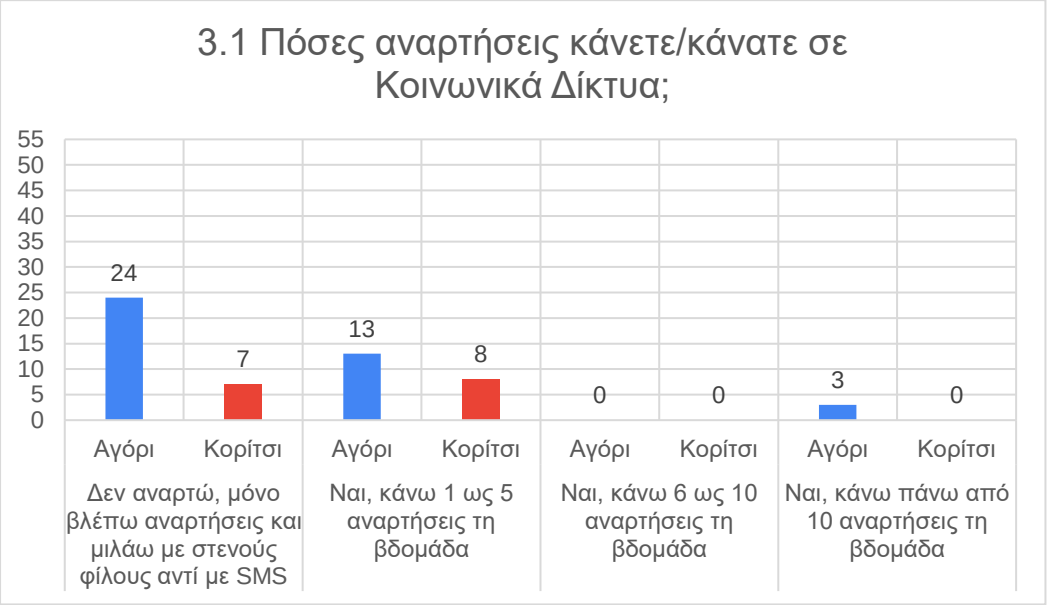
Διάγραμμα 11 Ερώτηση 2.2 Έχετε κάνει αποστολή μηνυμάτων με πληροφορίες σαν των παραδειγμάτων που είδατε σήμερα σε ομάδες με αγνώστους του WhatsApp, Viber, Discord, κ.λπ.

Στο Διάγραμμα 11 βλέπουμε πως από τα 15 άτομα που συμμετέχουν σε ομάδες με αγνώστους, το 1 άτομο (6.6%), που ήταν αγόρι, στέλνει ελάχιστες φορές, συχνά στέλνουν 6 άτομα (40%) και τα 6 αγόρια, ενώ τα 8 άτομα (53,3%), εκ των οποίων τα 7 αγόρια και το 1 κορίτσι, από τους 15 δεν έχουν κάνει αποστολή τέτοιων μηνυμάτων με περιεχόμενο επικίνδυνο για αποκάλυψη θέσης και ταυτότητας.



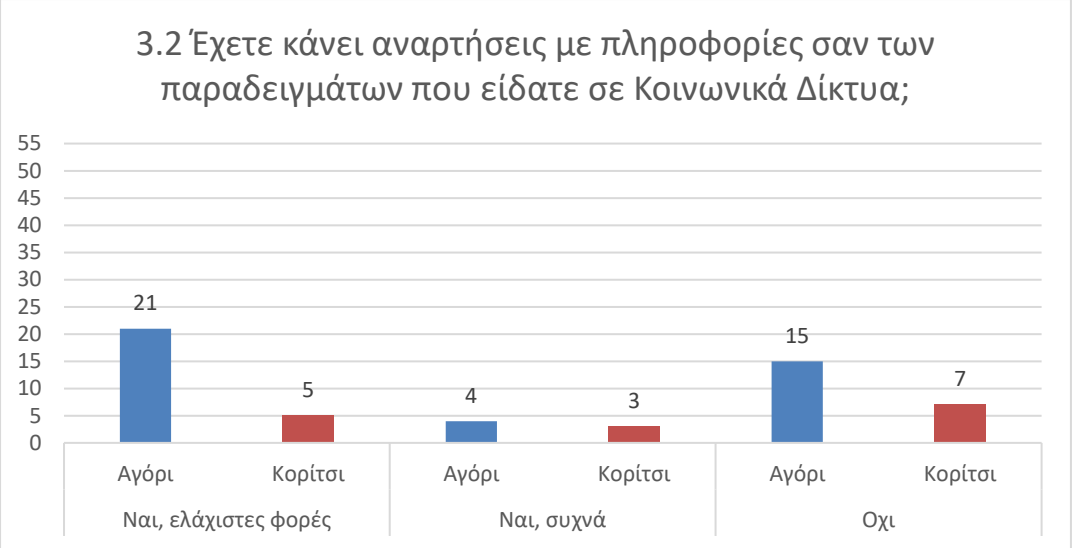
Διάγραμμα 12 Ερώτηση 3. Έχετε λογαριασμό σε Κοινωνικό Δίκτυο με Φίλους/Ακόλουθους

Στο Διάγραμμα 12 παρατηρούμε πως από τα 56 συνολικά άτομα, τα 51 (91%) έχουν λογαριασμό σε Κοινωνικό Δίκτυο με φίλους και ακολούθους, 4 άτομα είχαν, αλλά τώρα δεν έχουν και 1 αγόρι δεν είχε ποτέ και δεν έχει τέτοιο λογαριασμό.



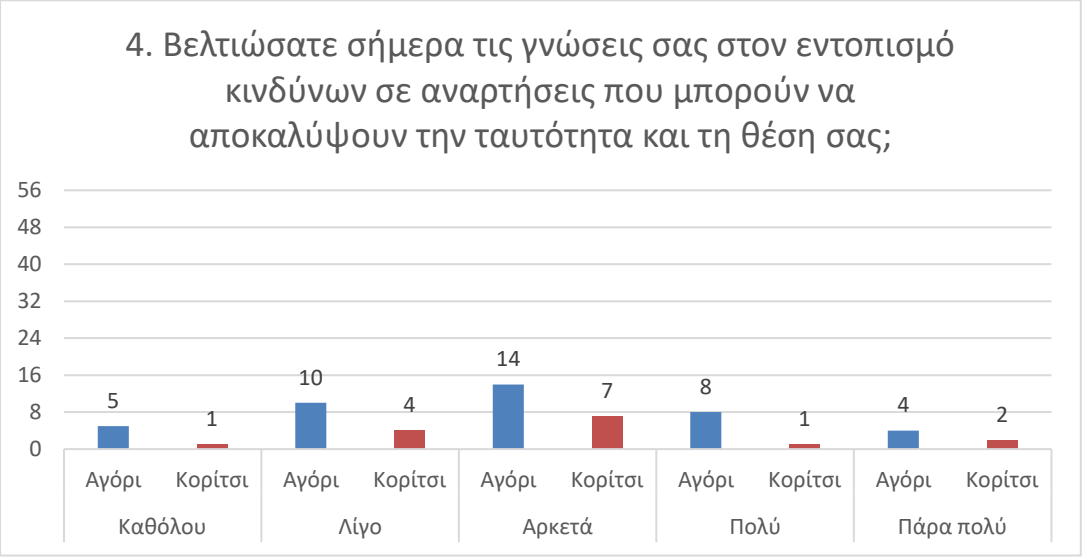
Διάγραμμα 13 Ερώτηση 3.1 Πόσες αναρτήσεις κάνετε σε Κοινωνικά Δίκτυα;

Στο Διάγραμμα 13 παρατηρούμε πως από τα 55 (μαζί με τα 4 που έκλεισαν τον λογαριασμό) τα 31 άτομα (56,36%), εκ των οποίων 24 αγόρια και 7 κορίτσια, αν και έχουν λογαριασμό σε Κοινωνικά Δίκτυα δεν κάνουν αναρτήσεις, αλλά μόνο βλέπουν αναρτήσεις και συνομιλούν με στενούς φίλους αντί για SMS. Επίσης, 21 άτομα (38,1%), εκ των οποίων 13 αγόρια και 8 κορίτσια, κάνουν από 1-5 αναρτήσεις, κανένα άτομο δεν κάνει 6-10 αναρτήσεις και 3 άτομα (5,45%), αγόρια, κάνουν πάνω από 10 αναρτήσεις τη βδομάδα.



Διάγραμμα 14 Ερώτηση 3.2 Έχετε κάνει αναρτήσεις με πληροφορίες σαν των παραδειγμάτων που είδατε σε Κοινωνικά Δίκτυα

Στο Διάγραμμα 14 βλέπουμε πως από τα 55 άτομα με Κοινωνικό Δίκτυο (με τους 4 που το έκλεισαν) τα 26 (47,27%), εκ των οποίων 21 αγόρια και 5 κορίτσια, έχουν κάνει ελάχιστες φορές ανάρτηση με περιεχόμενο επικίνδυνο για αποκάλυψη θέσης και ταυτότητας. Τα 7 από τα 55 (12,73%), εκ των οποίων 4 αγόρια και 3 κορίτσια, έχουν κάνει συχνά τέτοιες αναρτήσεις. Τέλος, τα 22 άτομα (40%), εκ των οποίων 15 αγόρια και 7 κορίτσια, δεν έχουν κάνει τέτοιες αναρτήσεις σε Κοινωνικά Δίκτυα.



Διάγραμμα 15 Ερώτηση 4. Βελτιώσατε σήμερα τις γνώσεις σας στον εντοπισμό κινδύνων σε αναρτήσεις που μπορούν να αποκαλύψουν την ταυτότητα και τη θέση σας

Στο Διάγραμμα 15 βλέπουμε τα αποτελέσματα στην ερώτηση αν οι συμμετέχοντες νιώθουν πως βελτίωσαν τις γνώσεις τους στο θέμα αποκάλυψης ταυτότητας και θέσης. Παρατηρούμε πως αθροιστικά από Αρκετά έως Πάρα Πολύ απάντησαν 36 άτομα, ποσοστό 64,28%.

Αναλυτικότερα, Αρκετά απάντησαν 21 άτομα, ποσοστό 37,5%, Πολύ απάντησαν 9 άτομα, ποσοστό 16,07% και Πάρα Πολύ απάντησαν 6 άτομα, ποσοστό 10,71%. Επίσης, 14 άτομα, ποσοστό 25%, απάντησε Λίγο και 6 άτομα, ποσοστό 10,71%, απάντησε πως δεν βελτίωσε Καθόλου τις γνώσεις του.

Διάγραμμα 16 Ερώτηση 5. Πόσο πιθανό είναι να εφαρμόσετε τις γνώσεις αυτές στην καθημερινή σας ζωή στο διαδίκτυο

Το Διάγραμμα 16 δείχνει τις απαντήσει που δόθηκαν στην ερώτηση πόσο πιθανό είναι να εφαρμόσουν τις γνώσεις που πήραν.

Δήλωσαν πως δεν θα τις εφαρμόσουν τα 10 (αγόρια) από τα 56 άτομα, ποσοστό 17,85%. Πως μάλλον θα τις εφαρμόσουν απάντησαν τα 32 άτομα, ποσοστό 57,14%, και πως θα τις εφαρμόσουν σίγουρα δήλωσαν 14 άτομα, ποσοστό 25%.

Διάγραμμα 17 Ερώτηση 6. Έχει συμβεί ποτέ κάποιο περιστατικό στο διαδίκτυο που σας αναστάτωσε

Το Διάγραμμα 17 δείχνει πως αθροιστικά σε 22 άτομα από τα 56, ποσοστό 39,29%, τους έχει συμβεί ή γνωρίζουν κάποιον που του έχει συμβεί κάτι στο διαδίκτυο που τους αναστάτωσε.

Αναλυτικότερα, 2 άτομα (3,57%) δήλωσαν πως έχει συμβεί και σε αυτούς και σε γνωστό τους. 13 άτομα (23,21%) δήλωσαν πως έχει συμβεί μόνο σε γνωστό τους, ενώ 7 άτομα (12,5%) δήλωσαν πως συνέβη μόνο σε αυτούς. Τέλος, 34 άτομα (60,71%) δήλωσαν πως δεν γνωρίζουν και δεν τους έχει συμβεί κάτι που να τους αναστάτωσε.

6.5 Συζήτηση αποτελεσμάτων

Στην ενότητα αυτή διεξάγεται η συζήτηση των αποτελεσμάτων, αρχικά των Φάσεων Α' & Β' και μετά αυτής του Ερωτηματολογίου εξόδου.

6.5.1 Συζήτηση των αποτελεσμάτων των Α' και Β' Φάσεων

Από τα αποτελέσματα των δυο φάσεων παρατηρήθηκε η βελτίωση της ικανότητας εντοπισμού προβληματικών σημείων σε εικόνες και κείμενα υποτιθέμενων αναρτήσεων που θα μπορούσαν να οδηγήσουν σε αποκάλυψη θέσης και ταυτότητας. Η σύγκριση των αποτελεσμάτων έδειξε ελαφριά βελτίωση στον εντοπισμό των σωστών σημείων κατά 12 %, από ποσοστό επιτυχίας 31% στην Α' Φάση ανήλθε στο 43% στη Β' Φάση.

Η βελτίωση κατά 12% είναι ικανοποιητική όχι όμως ξεκάθαρη για την αποτελεσματικότητά της. Αυτό γιατί πρέπει να λάβουμε υπόψη μας πως σε κάθε απάντηση των διαδραστικών βίντεο της H5P υπάρχει, και είναι μη απενεργοποιήσιμη, άμεση οπτική ένδειξη (√, X) αν η απάντηση που δόθηκε ήταν σωστή ή λάθος, πριν προχωρήσει στην επόμενη ερώτηση. Άρα, η κοντινή απόσταση υπολογιστών θα μπορούσε να επιτρέψει σε διπλανά άτομα να δουν το αποτέλεσμα και να απαντήσουν ανάλογα. Επίσης, ακόμη ένα σημείο που θα μπορούσε να συμβάλει σε αλλοίωση ήταν η επαφή των παιδιών στο σχολικό διάλλειμα μεταξύ των 2 διδακτικών ωρών που διήρκησε η έρευνα, θα μπορούσαν δηλαδή να συζητήσουν επ' αυτού συμμαθητές που είδαν τις δραστηριότητες με κάποιους που δεν είχε έρθει ακόμη η σειρά τους για την έρευνα.

Η ελάττωση του μέσου χρόνου διεκπεραίωσης κατά 28% μπορεί να ερμηνευτεί ως ένδειξη ότι κατάλαβαν ποια σημεία πρέπει να ψάχνουν στις εικόνες και στα κείμενα. Σε αυτή την περίπτωση θα ήταν ικανοποιητική η βελτίωση. Θα μπορούσε όμως να συμβεί σε περιπτώσεις που αδιαφορούσαν για τις ερωτήσεις και επέλεγαν γρήγορα απαντήσεις για να τελειώσει η διαδικασία ή σε περιπτώσεις που είχε μεσολαβήσει συνομιλία στο διάλλειμα μεταξύ τους. Οι ερωτήσεις ήταν μόνο 5 και είχαν σταθερή σειρά εμφάνισης.

6.5.2 Συζήτηση των αποτελεσμάτων του ερωτηματολογίου εξόδου

Ενθαρρυντικά ήταν τα αποτελέσματα του ερωτηματολογίου εξόδου στην ερώτηση αν βελτιώθηκαν οι γνώσεις τους στον εντοπισμό επικίνδυνων σημείων σε εικόνες και κείμενα που θα μπορούσαν να οδηγήσουν στην αποκάλυψη Θέσης και Ταυτότητας. Αθροιστικά, από την ομάδα στόχο ποσοστό 64% απάντησε *πως νιώθει ότι βελτιώθηκαν από Αρκετά έως Πάρα Πολύ*, το 25% απάντησε *λίγο* και το 11% απάντησε *καθόλου*.

Παρόμοια και στην ερώτηση αν νομίζουν πως θα εφαρμόσουν τις γνώσεις αυτές στην καθημερινή τους ζωή, αθροιστικά το 82% δήλωσε πως *Μάλλον θα τις εφαρμόσει* και *Θα τις εφαρμόσει σίγουρα*, ενώ το 18% δήλωσε πως *δεν θα τις εφαρμόσει*.

Εφαρμογές μηνυμάτων που διαθέτουν Ομάδες (Groups) και Κανάλια (Channels) έχουν στην κατοχή τους 55 άτομα στα 56, ποσοστό 98%. Διευκρίνηση, οι Ομάδες (Groups) εμφανίζουν τον αριθμό τηλεφώνου του συμμετέχοντα, πχ Viber και Whatsapp, ενώ τα Κανάλια (Channels) δεν εμφανίζουν τον αριθμό τηλεφώνου, πχ Viber, Whatsapp, Discord. Εδώ υπάρχει πιθανώς μία παρανόηση, γιατί ενδεχομένως στον ευρύ πληθυσμό δεν είναι ξεκάθαρο λέγοντας Ομάδα αν εννοούν Group ή Channel, διότι το βλέπουν από την πλευρά της μαζικής αποστολής και εμφάνισης των μηνυμάτων. Αν λοιπόν αυτό συνδυαστεί με το ότι 15 άτομα από τα 55, ποσοστό 27%, δηλώνει πως είναι μέσα σε τέτοιες Ομάδες (Groups) τότε είναι ιδιαίτερα επικίνδυνο για την προστασία από Αποκάλυψη Θέσης και Ταυτότητας, καθώς έχει ήδη αποκαλυφθεί σημαντικότατο προσωπικό δεδομένο, ο αριθμός τηλεφώνου.

Λογαριασμό σε Κοινωνικά Δίκτυα έχουν ή είχαν 55 από τους 56. Το Διάγραμμα 14, Ερώτηση 3.2, δείχνει ότι 33 από τους 55 που έχουν ή είχαν λογαριασμό σε Κοινωνικά Δίκτυα, ποσοστό 60%, δημοσίευσαν αναρτήσεις με υλικό που θα μπορούσε να οδηγήσει σε αποκάλυψη ταυτότητας ή θέσης. Είναι πολύ σημαντικό το ποσοστό, διότι μελλοντική προσθήκη φίλου που είναι κακόβουλος, θα μπορεί να οδηγήσει σε αποκάλυψη κρίσιμων πληροφοριών θέσης και ταυτότητας.

7

Συμπεράσματα ερευνών – Καλές Πρακτικές

7.1.1 Συμπεράσματα ερευνών

Από τα αποτελέσματα που πήραμε μπορούμε να απαντήσουμε στα ερευνητικά ερωτήματα.

Στο πρώτο ερώτημα «Ε1: Βελτίωσε το διαδραστικό υλικό H5P και η μαθησιακή παρέμβαση την ικανότητα των μαθητών να εντοπίζουν προβληματικά σημεία σε αναρτήσεις που θα μπορούσαν να οδηγήσουν σε αποκάλυψη θέσης και ταυτότητας;»

Η απάντηση είναι ναι, βελτίωσε αυτή την ικανότητα των μαθητών σε ποσοστό 12%. Η βελτίωση κατά 12% δεν ήταν ανάλογη της μείωσης του χρόνου απόκρισης στον εντοπισμό επικίνδυνων σημείων που ήταν 28%. Σύμφωνα με τις απαντήσεις του ερωτηματολογίου εξόδου, το 64% νιώθει πως έμαθε από Αρκετά έως Πάρα Πολλά για το θέμα μέσα από τις δραστηριότητες και το μάθημα ευαισθητοποίησης.

Στο δεύτερο ερώτημα «Ε2: Μπορεί να χρησιμοποιηθεί παρόμοιο διαδραστικό υλικό στις υποδομές του Πανελλήνιου Σχολικού Δικτύου για την επαγρύπνηση στην κυβερνοασφάλεια σχολικού πληθυσμού» η απάντηση είναι ναι μπορεί στα εξής περιβάλλοντα:

1. Στο eClass.sch.gr [44] που βασίζεται στο OpenEclass, χωρίς λήψη βαθμολογίας χρηστών, προς το παρόν, μόνο εκτέλεση και δημιουργία.
2. Στο e-me.edu.gr [43] που βασίζεται σε WordPress, λειτουργεί η βαθμολογία χρηστών και την ονομάζει Δραστηριότητα Χρήστη. Δεν προσφέρει όμως εκτεταμένες πληροφορίες όπως αυτές του H5PxAPIkatchu ή κάποιου LRS.
3. Επίσης, το Πανελλήνιο Σχολικό Δίκτυο διαθέτει σε εκπαιδευτικούς υπηρεσία φιλοξενίας ιστοτόπων (Web Hosting) και τη δυνατότητα να εγκαταστήσουν στον δικό τους WordPress ή Moodle, όπου μπορούν να εγκαταστήσουν βάλουν τα απαιτούμενα πρόσθετα H5P και H5PxAPIkatchu αν δεν υποστηρίζονται από το κεντρικό WordPress του Σχολικού Δικτύου [51] ή Moodle [52].

7.1.2 Καλές πρακτικές

Κατά τη διερεύνηση κατάλληλου και δωρεάν περιβάλλοντος με H5P για την διενέργεια αυτής της έρευνας, προέκυψαν χρήσιμες πληροφορίες και οι οποίες καταγράφηκαν για να αποτελέσουν πρόταση καλής πρακτικής σε όποιους επιθυμούν να αναπτύξουν παρόμοιο σύστημα.

Καλές πρακτικές ανάπτυξης Συστήματος Διαχείρισης διαδραστικών μαθήματων με H5P

Εγκατάσταση Πλατφόρμας

Ανάλογα με τον με τον πάροχο φιλοξενίας ιστοσελίδων, είναι διαθέσιμος κεντρικός πίνακας ελέγχου (control panel) από τον οποίο μπορείς με λίγα κλικ να εγκαταστήσεις την επιθυμητή πλατφόρμα, παράδειγμα Wordpress, Moodle κ.λπ. Το σχολικό δίκτυο προσφέρει τον πίνακα ελέγχου Plesk [53], στον οποίο είναι διαθέσιμες για εγκατάσταση οι δύο προαναφερθείσες πλατφόρμες, δεν είναι όμως και το OpenEclass. Για την τελευταία θα χρειαστεί να ακολουθήσετε τις οδηγίες του οργανισμού που το παρέχει [44].

Εγκατάσταση πρόσθετου H5P στην Πλατφόρμα

Πρόσθετο της H5P είναι διαθέσιμο προς εγκατάσταση για Wordpress (Πίνακας ελέγχου/Πρόσθετα/Προσθήκη νέου) και για το Moodle (Διαχείριση ιστότοπου/Πρόσθετα/ Εγκατάσταση Πρόσθετου). Στο OpenEclass δεν χρειάζεται εγκατάσταση γιατί είναι ενσωματωμένο από την έκδοση 3.12 και μετά.

Δημιουργία μαθημάτων με H5P

Με το πρόσθετο αυτό μπορείς να δημιουργήσεις μαθήματα επιλέγοντας μια από τις άνω των 50 διαφορετικών ειδών βιβλιοθήκες που διαθέτει. Σημαντική βοήθεια στην κατασκευή υλικού με εικόνες και βίντεο για τα μαθήματα ευαισθητοποίησης μπορεί να δοθεί από την Τεχνητή Νοημοσύνη. Αυτό συντομεύει τον χρόνο και το κόστος δημιουργίας διαδραστικών μαθημάτων καθώς δεν απαιτείται η αναζήτηση γραφίστα και παραγωγούς βίντεο.

Η δημιουργία και τροποποίηση είναι ίδια και στις τρεις πλατφόρμες, Wordpress (από δικαιώματα Συνδρομητή και άνω), Moodle (από Εκπαιδευτή και άνω), OpenEclass (από Εκπαιδευτικού και άνω). Διατεθείτε κατατοπιστική βοήθεια βήμα-βήμα με εικόνες και βίντεο [54].

Τα μαθήματα που δημιουργούνται με H5P μπορούν να εξαχθούν από μια πλατφόρμα και να εισαχθούν και τροποποιηθούν σε κάποια άλλη πλατφόρμα που την υποστηρίζει.

Απλή παρακολούθηση βαθμολογιών μαθημάτων H5P

Απλή παρακολούθηση βαθμολογιών σημαίνει εμφάνιση του βαθμού μαθήματος, ημερομηνία και ώρα έναρξης και λήξης μαθήματος και τον συνολικό χρόνο που διήρκησε. Επισημαίνεται πως ο βαθμός μαθητή που φαίνεται εδώ είναι πάντα αυτός της τελευταίας προσπάθειας στο μάθημα. Γενικά, οι πληροφορίες που παρέχονται εδώ, δεν μπορούν να βοηθήσουν στον εντοπισμό προβληματικών ερωτήσεων του μαθήματος, όπως για παράδειγμα ποια ερώτηση την απαντούν όλοι λάθος.

Η απλή εμφάνιση του βαθμολόγιου στο Wordpress μπορεί να γίνει από τον Πίνακα Ελέγχου / H5P Content / All H5P Content / Results. Κάτω από αυτή θα εμφανιστούν τα ονόματα χρηστών όσων μαθητών εκτέλεσαν το μάθημα

Στο Moodle οι βαθμοί κάθε μαθητή πηγαίνουν στο Βαθμολόγιο της πλατφόρμας.

Το OpenEclass δεν υποστηρίζει μέχρι σήμερα συγκέντρωση βαθμών από H5P στο Βαθμολόγιο της πλατφόρμας αλλά ούτε και σε άλλο σημείο.

Παρακολούθηση αναλυτικών ενεργειών εκτέλεσης μαθημάτων

Αναλυτικές ενέργειες εκτέλεσης μαθήματος σημαίνει πως θα καταγραφούν πληροφορίες για όλες τις ενέργειες κάθε χρήστη μέσα στο μάθημα. Επομένως, εκτός από τον βαθμό, θα καταγραφούν και ενέργειες που μπορεί να είναι το πόσες φορές ξεκίνησε ένας μαθητής το μάθημα αλλά δεν το ολοκλήρωσε, τι απάντηση έδωσε σε κάθε ερώτηση και όποια άλλη πληροφορία θέλει ο εκπαιδευτικός για να ελέγξει το μάθημα. Είναι δηλαδή ένα εξαιρετικό εργαλείο για να ελέγχει ο εκπαιδευτικός την ποιότητα του μαθήματος γιατί μπορεί να εντοπίσει τα προβληματικά σημεία και να διορθώσει.

Για να συλλεχθούν αναλυτικές πληροφορίες χρειάζονται επιπλέον εργαλεία που να συνεργάζονται με H5P.

Στο Wordpress υπάρχουν δύο επιλογές. Η πρώτη είναι η διασύνδεση με εξωτερικό σύστημα καταγραφής των ενεργειών στην H5P. Λέγονται Αποθήκες Καταγραφής Μάθησης ή LRS (Learning Record Store) είναι επαγγελματικά και κοστίζουν αρκετά, υπάρχουν μερικά που διαθέτουν δωρεάν πρόσβαση αλλά με περιορισμένες δυνατότητες. Η δεύτερη επιλογή είναι πρόσθετο H5PxAPIkatchu που θα πρέπει να εγκατασταθεί. Διατίθεται δωρεάν και κάνει την καταγραφεί των πληροφοριών μέσα στο Wordpress. Το περιβάλλον με τις πληροφορίες βρίσκεται στο Πίνακας Ελέγχου / H5PxAPIkatchu. Τις πληροφορίες που καταγράφει μπορούμε να τις κατεβάσουμε τοπικά μόνο σε μορφή CSV και να το επεξεργαστούμε για να εξαχθούν συμπεράσματα για μαθήματα και μαθητές.

Στο Moodle μπορεί να χρησιμοποιηθεί μόνο εξωτερικό LRS.

Το OpenEclass δεν υποστηρίζει κανέναν τρόπο για καταγραφή ενεργειών στην H5P.

8

Επίλογος

Η διπλωματική δημιούργησε πλαίσιο ευαισθητοποίησης κυβερνοασφάλειας για μαθητικό πληθυσμό και πραγματοποίησε έρευνα. Ακολουθεί η σύνοψη, τα συμπεράσματα και οι μελλοντικές επεκτάσεις.

8.1 Σύνοψη και συμπεράσματα

Η διπλωματική δημιούργησε και αξιολόγησε ένα πλαίσιο επαγρύπνησης κυβερνοασφάλειας για μαθητικό πληθυσμό. Σκοπός του πλαισίου ήταν να βοηθηθούν οι μαθητές ενδυναμώνοντας την ευαισθητοποίησή τους σε θέματα κυβερνοασφάλειας ώστε να αποφεύγουν τους κινδύνους που ελλοχεύουν στα κοινωνικά δίκτυα. Χρησιμοποιήθηκε ανοιχτό λογισμικό στην υλοποίηση της πλατφόρμας και στα απαιτούμενα πρόσθετα. Με την χρήση H5P δημιούργησε διαδραστικό μάθημα, το οποίο εισήχθη σε εκπαιδευτική πλατφόρμα ανοιχτού και μετρήθηκε η αποδοτικότητά των μαθημάτων από ποσοτική έρευνα σε μαθητές.

Η έρευνα έδειξε βελτίωση κατά 12,14% της επαγρύπνησης στον εντοπισμό κινδύνων σε δημοσιεύσεις κοινωνικών δικτύων. Οι μαθητές που συμμετείχαν επιβεβαίωσαν την θετική συνεισφορά των μαθημάτων στην αύξηση του ενδιαφέροντος για το αντικείμενο των μαθημάτων. Σημαντικό εύρημα του ερωτηματολογίου της έρευνας ήταν το ποσοστό 60% των μαθητών που έχει κάνει ανάρτηση σε κοινωνικό δίκτυο με περιεχόμενο που θα μπορούσε να συμβάλει σημαντικά στην αποκάλυψη θέσης του.

Η υλοποίηση του συστήματος με ανοιχτό λογισμικό

8.2 Μελλοντικές επεκτάσεις

Σημαντική βελτίωση του συστήματος θα ήταν η δημιουργία και χρήση μαθημάτων ευαισθητοποίησης στην κυβερνοασφάλεια που να είναι σχετικά με τα ενδιαφέροντα του κάθε μαθητή. Η εξατομικευμένη μάθηση ενδεχομένως να χρειάζεται προσοχή καθώς θα είναι σοβαρό θέμα η πηγή πληροφόρησης για τα ενδιαφέροντα των μαθητών. Θα ήταν ίσως ευκολότερο να γίνεται σε λύκεια με ειδικότητες ή στην τριτοβάθμια εκπαίδευση, όπως κάνει το CAFA [5]. Σε τέτοια μαθήματα το υλικό θα περιέχει ορολογία και πλοκή που θα είναι οικία για τον μαθητή για να γίνει προσιτό το περιεχόμενο και ευχάριστη η ευαισθητοποίηση στην κυβερνοασφάλεια.

Η χρήση της Τεχνητής Νοημοσύνης στη δημιουργία μαθημάτων. Η δημιουργία κατάλληλου υλικού ανά ηλικία και αντικείμενο μαθήματος απαιτεί μεγάλο κόπο από τους εκπαιδευτικούς και η Τ.Ν. θα ελαχιστοποιούσε χρόνο και χρήματα που απαιτούνται. Παράλληλα θα μπορούσε να ετοιμάζει το μάθημα και με την επιθυμητό πρότυπο μάθησης, όπως SCORM, xAPI, cmi5, για να είναι εύκολη και γρήγορη η ενσωμάτωσή τους στις πλατφόρμες μάθησης.

Η χρήση Τεχνητής Νοημοσύνης για παιχνίδια σεναρίων με Κοινωνικής Μηχανικής. Θα μπορούσαν να δημιουργηθούν παιχνίδια στα οποία θα υπάρχει ο μαθητής και από την άλλη μεριά η Τ.Ν. να προσπαθεί με ερωτήσεις να εκμαιεύσει πληροφορίες που θα μπορούσαν να οδηγήσουν σε επικίνδυνες αποκαλύψεις αν γινόντουσαν στον πραγματικό κόσμο. Παρόμοια παιχνίδια θα μπορούσαν να γίνουν για όλες τις απειλές του διαδικτύου.

Η χρήση της Τεχνητής Νοημοσύνης στην ανάλυση των στατιστικών των μαθημάτων (learning analytics). Η ανάλυση των στατιστικών μαθημάτων θα βοηθούσε τη διαδικασία μάθησης καθώς θα ενημερωνόντουσαν οι υπεύθυνοι των μαθημάτων έγκαιρα για πιθανά προβλήματα σε κάποιο μάθημα. Θα μπορούσαν να ενημερώνονται και για την λίστα των μαθητών που αντιμετωπίζουν προβλήματα σε συγκεκριμένα θέματα κάθε μαθήματος. Η εφαρμογή πάνω στις πληροφορίες που συλλέγει το H5PxAPIkatchu θα είχε ενδιαφέρον για την εκπαιδευτική κοινότητα.

9

Βιβλιογραφία

[1] "Αποτελέσματα έρευνας 2019-2020 για διαδικτυακές συνήθειες παιδιών, επηρεασμό από κοινωνικά δίκτυα και online gaming.," SaferInternet4kids. Accessed: Jul. 18, 2024. [Online]. Available: https://saferinternet4kids.gr/nea/apotelesmata-ereynas-19-20/

[2] "The Digital Services Act (DSA) explained - Measures to protect children and young people online | Shaping Europe's digital future." Accessed: Aug. 18, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/digital-services-act-dsa-explained-measures-protect-children-and-young-people-online

[3] "The influence of social media on the development of children and young people".

[4] N. Kortjan and R. Solms, "A conceptual framework for cyber security awareness and education in SA," *South African Computer Journal*, vol. 52, Jun. 2014, doi: 10.18489/sacj.v52i0.201.

[5] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," *Information*, vol. 12, no. 10, Art. no. 10, Oct. 2021, doi: 10.3390/info12100417.

[6] M. Al-Tajer and I. Adeyemi, *Cyber Security Threat Awareness Framework for High School Students in Qatar*. 2022.

[7] L. Zhang-Kennedy and S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education," *ACM Comput. Surv.*, vol. 54, no. 1, p. 12:1-12:39, Jan. 2021, doi: 10.1145/3427920.

[8] G. Jiang, A. Ansari, M. Sivakumar, and T. McCarthy, "Evaluation of H5P interactive videos in enhanced elearning of an environmental engineering course during COVID-19 pandemic," in *9th Research in Engineering Education Symposium (REES 2021) and 32nd Australasian Association for Engineering Education Conference (REES AAEE 2021)*, Perth, WA, Australia: Research in Enineering Education Network (REEN), 2022, pp. 500–508. doi: 10.52202/066488-0055.

[9] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, Dec. 2021, doi: 10.1016/j.ijcci.2021.100343.

[10] S. Scholefield and L. A. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 191–203. doi: 10.1007/978-3-030-22351-9_13.

[11] T. Abrahams, O. Farayola, S. Kaggwa, P. Uwaoma, A. Hassan, and S. Dawodu, "Cybersecurity awareness and education programs: a review of employee engagement and accountability," *Computer Science & IT Research Journal*, vol. 5, pp. 100–119, Jan. 2024, doi: 10.51594/csitrj.v5i1.708.

[12]"Cyber Security Ontario: K-12." Accessed: Jun. 17, 2024. [Online]. Available: https://cybersecurityontario.ca/k-12#game-section
[13]"Cyber Curriculum - Minecraft Education," education.minecraft.net. Accessed: Mar. 17, 2024. [Online]. Available: https://education.minecraft.net/en-us/blog/cyber-curriculum
[14]"Παιχνίδι Κρυμμένου Θησαυρού | SaferInternet4kids." Accessed: Jan. 30, 2023. [Online]. Available: https://saferinternet4kids.gr/σχέδια-μαθημάτων/game
[15]"Βίντεο," SaferInternet4kids. Accessed: Jun. 18, 2024. [Online]. Available: https://saferinternet4kids.gr/%ce%b2%ce%af%ce%bd%cf%84%ce%b5%ce%bf/
[16]"Saferinternet.gr - Για ένα ασφαλέστερο Διαδίκτυο." Accessed: Jun. 18, 2024. [Online]. Available: https://www.saferinternet.gr/index.php?parentobjId=Page15&objId=Category17&p=0
[17]"Comic book introduces kids to key concepts and careers in cybersecurity | Institute for Advanced Learning Technologies." Accessed: Jun. 19, 2024. [Online]. Available: https://ialt.education.ufl.edu/2021/12/16/comic-book-introduces-kids-to-key-concepts-and-careers-in-cybersecurity/
[18]"cyber-threat-response-comic-final.pdf." Accessed: Jun. 18, 2024. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/cyber-threat-response-comic-final.pdf
[19]"Κόμικς," Internet Safety. Accessed: May 20, 2024. [Online]. Available: https://internetsafety.pi.ac.cy/kids/kids-comics/
[20]"Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές." Accessed: Jun. 19, 2024. [Online]. Available: https://www.consilium.europa.eu/el/policies/cybersecurity/
[21]"What is Cybersecurity? | IBM." Accessed: Mar. 20, 2024. [Online]. Available: https://www.ibm.com/topics/cybersecurity
[22]"Cybersecurity," ITU. Accessed: Mar. 20, 2024. [Online]. Available: https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[23]"Cyber Safety | CISA." Accessed: Mar. 20, 2024. [Online]. Available: https://www.cisa.gov/news-events/news/cyber-safety
[24]L. Kimpe, M. Walrave, K. Ponnet, and J. Van Ouytsel, "Internet Safety," pp. 1–11, May 2019, doi: 10.1002/9781118978238.ieml0093.
[25]C. C. Editor, "Awareness - Glossary | CSRC." Accessed: Sep. 16, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/awareness
[26]"CISA Cybersecurity Awareness Program | CISA." Accessed: Mar. 20, 2024. [Online]. Available: https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program
[27]"Awareness Raising," ENISA. Accessed: Apr. 20, 2024. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education
[28]"Cyber Vigilance | Deloitte CIS | Risk Advisory," Deloitte Kazakhstan. Accessed: Sep. 16, 2024. [Online]. Available: https://www2.deloitte.com/kz/en/pages/risk/solutions/cyber-vigilance.html
[29]"Κατηγορία: Hot topics," SaferInternet4kids. Accessed: Mar. 16, 2024. [Online]. Available: https://saferinternet4kids.gr/category/hot-topics/
[30]"SaferInternet4kids Ποιοι είμαστε," SaferInternet4kids. Accessed: Mar. 16, 2024. [Online]. Available: https://saferinternet4kids.gr/poioieimaste/
[31]"Αποτελέσματα έρευνας 2018-2019 σε 14.000 μαθητές για τις συνήθειες και τους κινδύνους που αντιμετωπίζουν στο διαδίκτυο," SaferInternet4kids. Accessed: Jul. 18, 2024. [Online]. Available: https://saferinternet4kids.gr/press-newsletter/researchresults/
[32]"Αποτελέσματα εθνικής έρευνας 2021-2022 για διαδικτυακές συνήθειες σε 5000 μαθητές," SaferInternet4kids. Accessed: Jul. 18, 2024. [Online]. Available: https://saferinternet4kids.gr/ereynes/ereuna21-22/
[33]"Αποτελέσματα πανελλήνιας έρευνας Ελληνικού Κέντρου Ασφαλούς Διαδικτύου ΙΤΕ σε 4.800 εφήβους," SaferInternet4kids. Accessed: Jul. 18, 2024. [Online]. Available: https://saferinternet4kids.gr/nea/surveyresults2024/
[34]"Safer Internet Centres - BIK Portal - BIK Community," BIK Portal. Accessed: Aug. 17, 2024. [Online]. Available: https://www.betterinternetforkids.eu/sic

[35]"What is OSINT (Open-Source Intelligence?) | SANS Institute." Accessed: Mar. 07, 2024. [Online]. Available: https://www.sans.org/blog/what-is-open-source-intelligence/
[36]"H5P." Accessed: Jun. 21, 2024. [Online]. Available: https://h5p.org/
[37]"H5P Licensing." Accessed: May 10, 2024. [Online]. Available: https://h5p.org/licensing
[38]"H5P Content Types." Accessed: Sep. 10, 2024. [Online]. Available: https://h5p.org/content-types-and-applications
[39]"Lumi Education," Lumi Education. Accessed: Jun. 21, 2024. [Online]. Available: https://lumi.education/en/
[40]Β. Β. Ζαχαριάδου, "Δημιουργία και αξιολόγηση διαδραστικού διδακτικού περιεχομένου για τη Δευτεροβάθμια Εκπαίδευση με χρήση του εργαλείου H5P," Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2020. doi: 10.26262/heal.auth.ir.321106.
[41]K. Mir, M. Iqbal, and J. Shams, "Investigation of Students' Satisfaction about H5P Interactive Video on MOODLE for Online Learning," *International Journal of Distance Education and E-Learning*, vol. 7, pp. 71–82, Jan. 2022, doi: 10.36261/ijdeel.v7i1.2228.
[42]"η-τάξη." Accessed: Jun. 23, 2024. [Online]. Available: https://eclass.sch.gr/
[43]"Ψηφιακή Εκπαιδευτική Πλατφόρμα e-me." Accessed: Jun. 23, 2024. [Online]. Available: https://e-me.edu.gr
[44]"Open eClass - e-learning platform," openeclass. Accessed: Jun. 21, 2024. [Online]. Available: https://www.openeclass.org/
[45]"Moodle." Accessed: Jun. 21, 2024. [Online]. Available: https://moodle.org/
[46]"Blog Tool, Publishing Platform, and CMS," WordPress.org. Accessed: Jun. 21, 2024. [Online]. Available: https://wordpress.org/
[47]"Analyzing results and answers." Accessed: Jun. 21, 2024. [Online]. Available: https://h5p.org/documentation/for-authors/analyzing-results-and-answers
[48]O. Tacke, "SNORDIAN's H5PxAPIkatchu," WordPress.org. Accessed: Jun. 23, 2024. [Online]. Available: https://wordpress.org/plugins/h5pxapikatchu/
[49]"SCORM vs xAPI," xAPI.com. Accessed: Jun. 24, 2024. [Online]. Available: https://xapi.com/scorm-vs-the-experience-api-xapi/
[50]"Can I sell images I create with DALL·E? | OpenAI Help Center." Accessed: Apr. 15, 2024. [Online]. Available: https://help.openai.com/en/articles/6425277-can-i-sell-images-i-create-with-dall-e
[51]"Εκπαιδευτικές Κοινότητες & Ιστολόγια ΠΣΔ." Accessed: Jun. 23, 2024. [Online]. Available: https://blogs.sch.gr/
[52]"e-learning – e-learning.sch.gr." Accessed: Jun. 23, 2024. [Online]. Available: https://e-learningnew.sch.gr/
[53]"Φιλοξενία ιστοτόπων Πανελλήνιο Σχολικό Δίκτυο." Accessed: Sep. 09, 2024. [Online]. Available: https://webhost.sch.gr/
[54]"H5P - Tutorials for authors." Accessed: Aug. 19, 2024. [Online]. Available: https://h5p.org/documentation/for-authors/tutorials

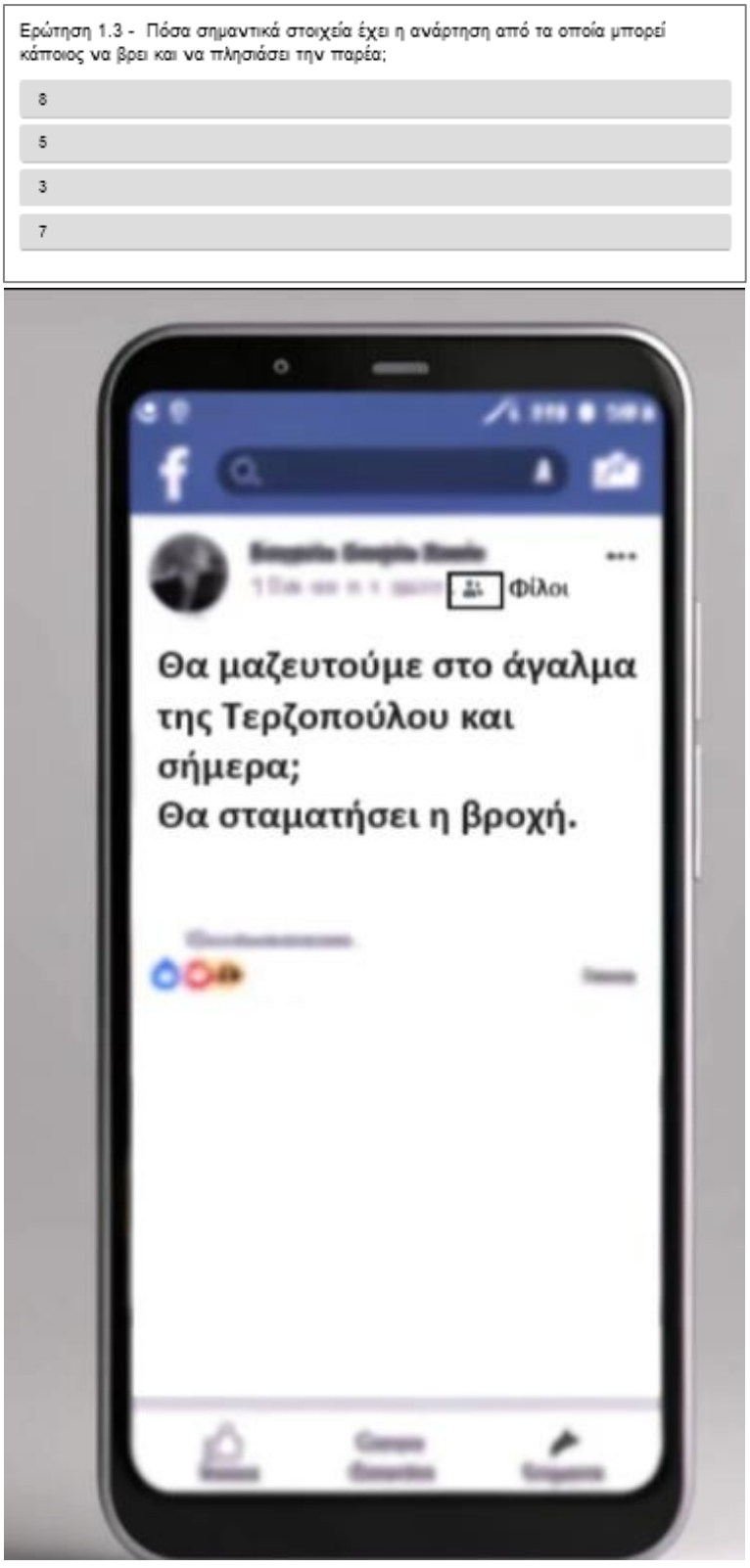
10

Παραρτήματα

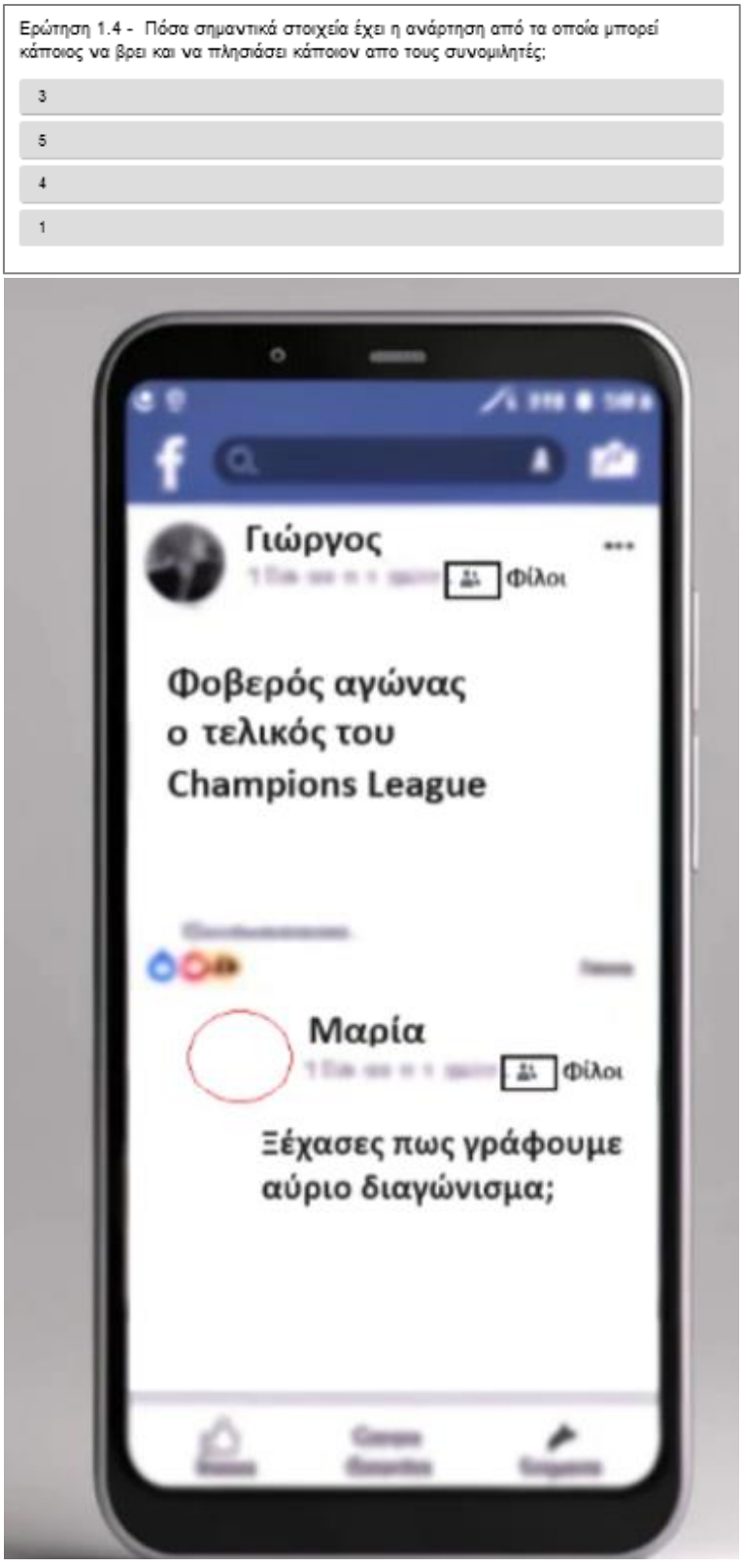
10.1Παράρτημα Α – Υλικό Α' Φάσης

Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα



Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα



Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

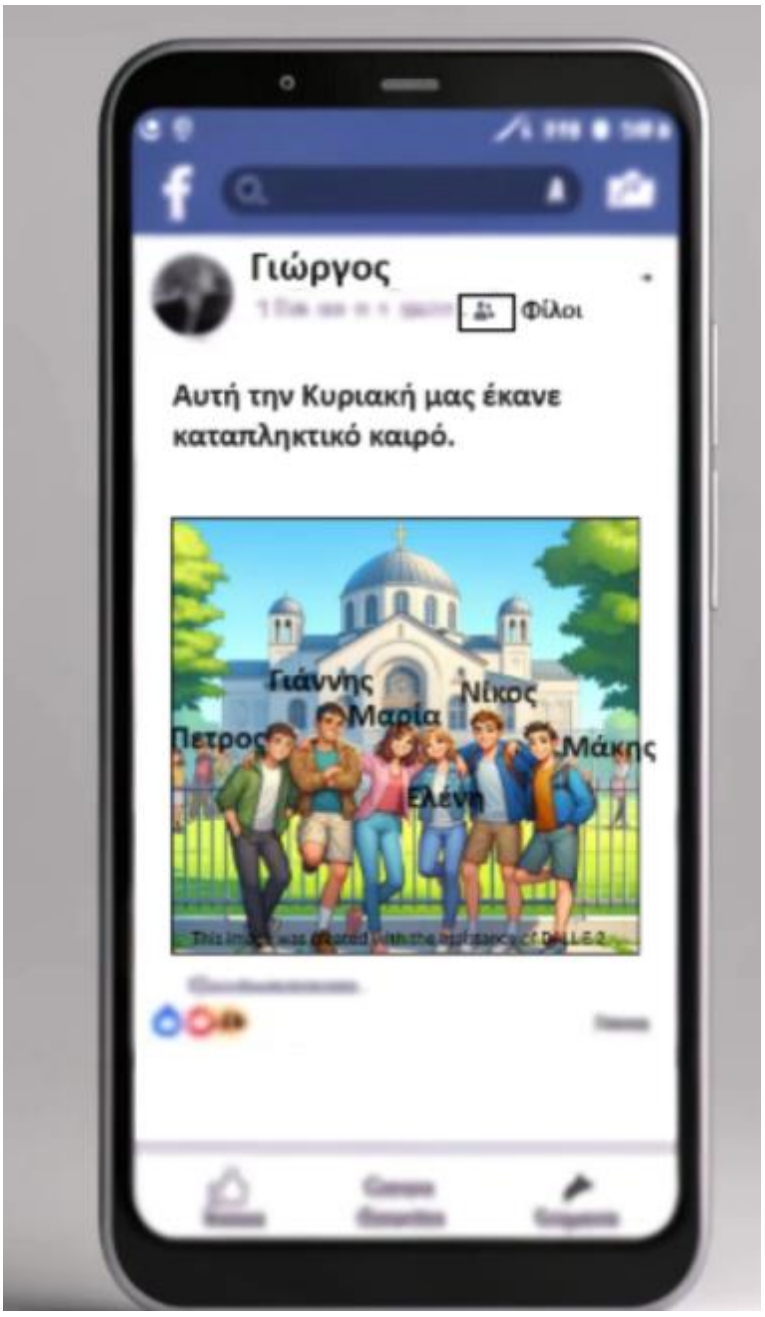
Ερώτηση 1.5 - Πόσα σημαντικά στοιχεία έχει η ανάρτηση από τα οποία μπορεί κάποιος να βρει και να πλησιάσει άτομο της παρέας;

5

8

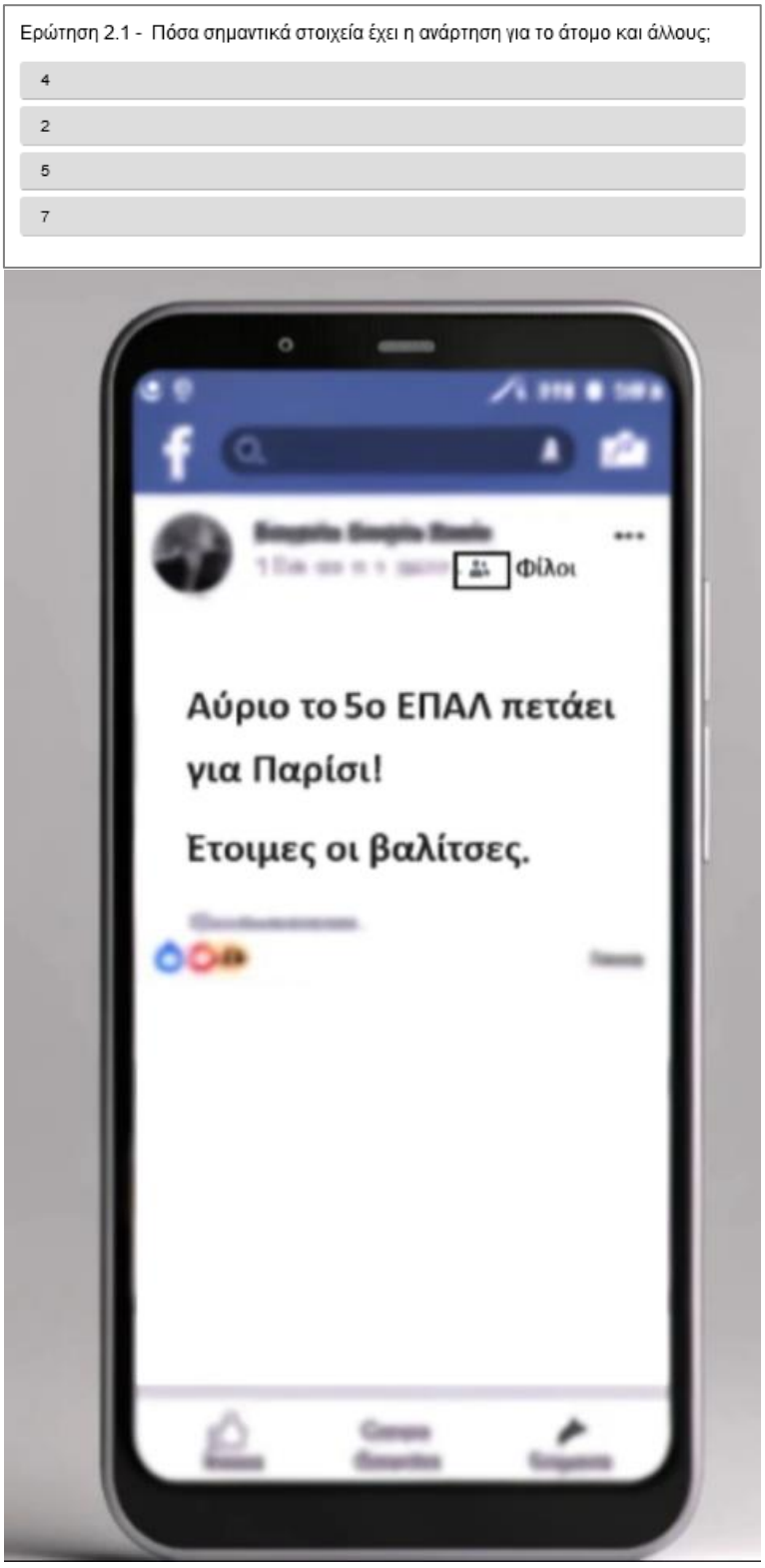
6

10



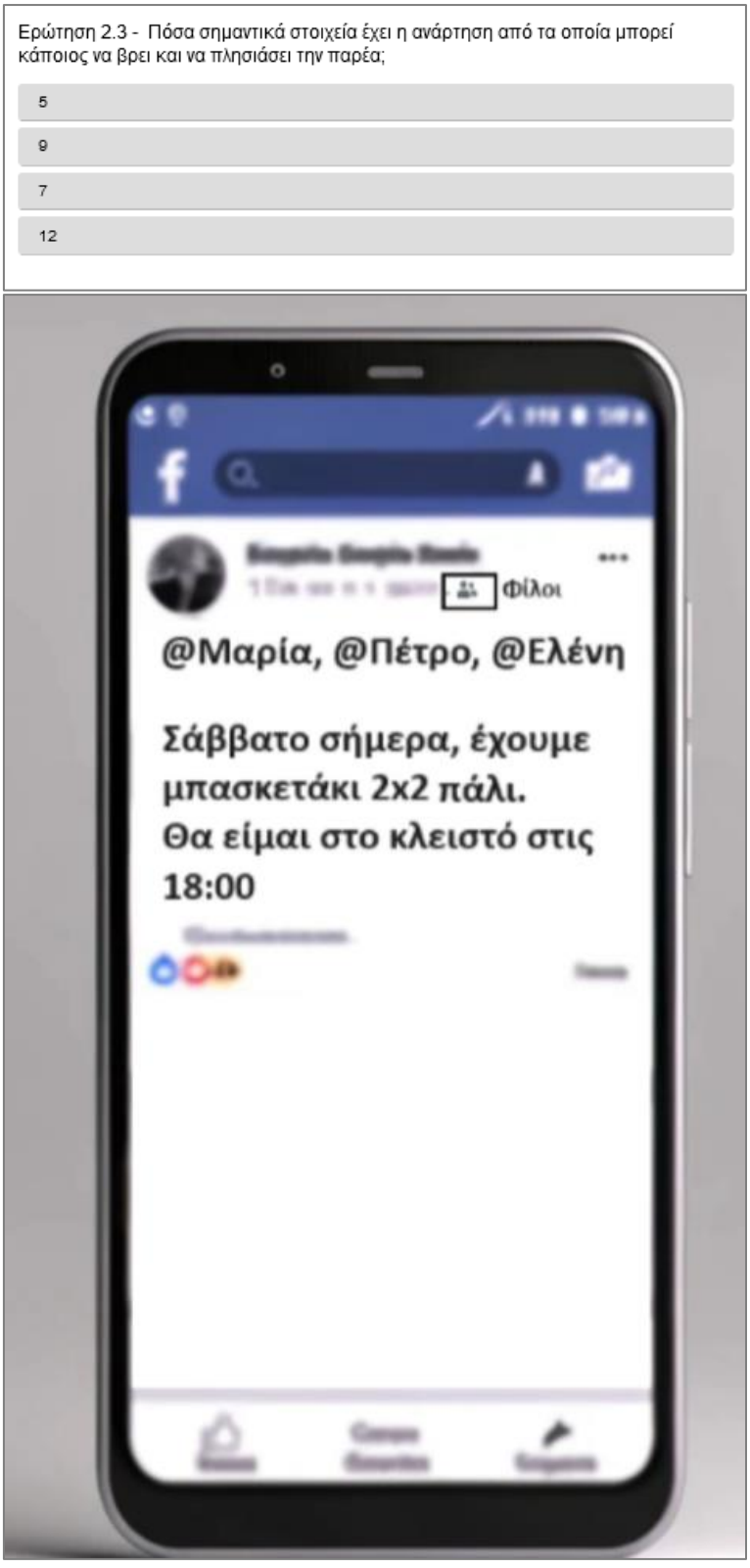
Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

10.2Παράρτημα Β – Υλικό Β' Φάσης

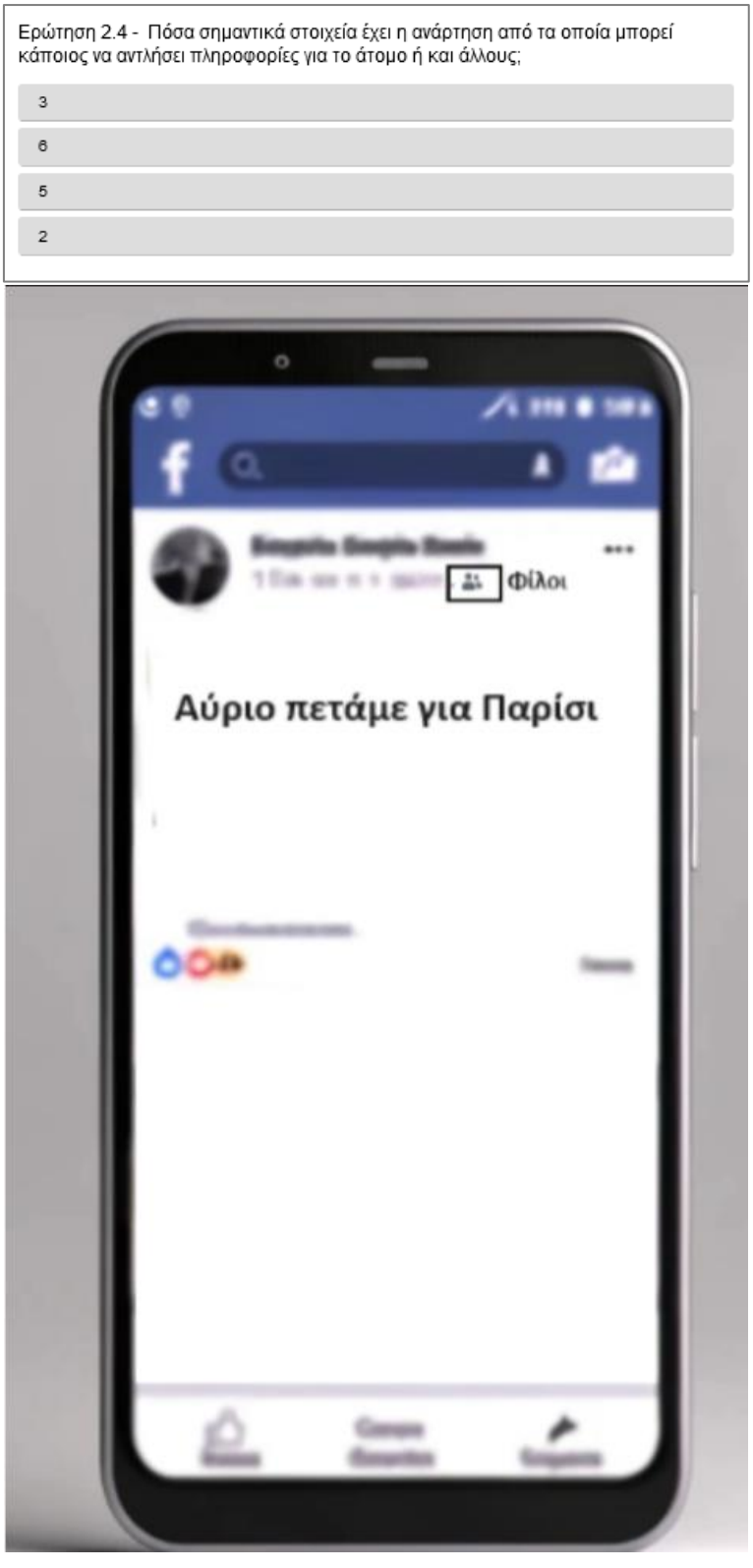


Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα



Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα



Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

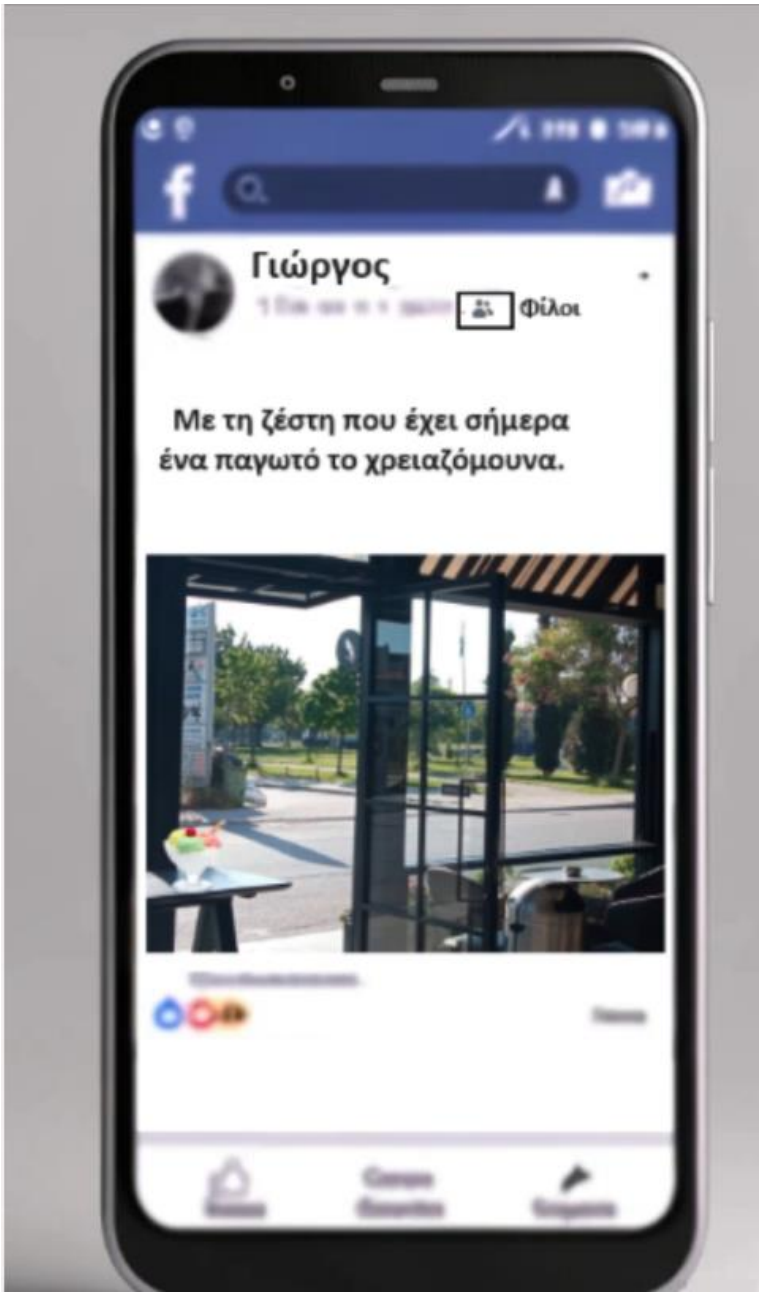
Ερώτηση 2.5 - Πόσα σημαντικά στοιχεία έχει η ανάρτηση από τα οποία μπορεί κάποιος να εντοπίσει το σημείο που βρίσκεται ο Γιώργος;

5

2

6

3



Αυτή η εικόνα δημιουργήθηκε με τη βοήθεια του DALL-E 2 και τροποποιήθηκε από τον συγγραφέα

10.3Παράρτημα Γ - Μάθημα ευαισθητοποίησης για την Αποκάλυψη Θέσης και Ταυτότητας

Μάθημα
προστασίας από την

Αποκάλυψη Θέσης και Ταυτότητας

Αυτές οι εικόνες δημιουργήθηκαν με τη βοήθεια του DALL-E 2

Τι είναι και πως σχηματίζεται η διαδικτυακή μας ταυτότητα;

- Η πραγματική μας ταυτότητα έχει πληροφορίες της γύρω από το άτομό μας στην πραγματική ζωή. Τέτοια είναι η φωτογραφία μας, όνομα και έχουμε όλοι μια διεύθυνση και τηλέφωνο.

- Η **διαδικτυακή μας ταυτότητα** σχηματίζεται από εμάς τους ίδιους.
  Από τα **ίχνη που αφήνουμε** στο διαδίκτυο.
  Είναι η εικόνα που σχηματίζουν οι άλλοι για εμάς στο διαδίκτυο.

Αφήνουμε ίχνη στο διαδίκτυο;

Ναι, **ίχνη** στο διαδίκτυο είναι όλα όσα κάνουμε εκεί:

- φωτογραφίες που αναρτούμε
- τα σχόλια που αναρτούμε
- τα Likes που κάνουμε
- τους online φίλους μας
- ομάδες (Groups) που ακολουθούμε

Τι είναι η αποκάλυψη της πραγματικής ταυτότητας και θέσης.

- Είναι η εύρεση στοιχείων από τα οποία μπορεί ένας κακόβουλος να εντοπίσει τη θέση μας και ίσως από αυτά να μπορεί να μάθει και την ταυτότητά μας.

- Στοιχεία που ίσως ψάξουν να βρουν σε δημοσιεύσεις δικές μας ή φίλων είναι:
  - που μπορούν να μας βρουν
  - που μένουμε
  - σχολείο, τάξη
  - ομάδα που αγωνιζόμαστε
  - φροντιστήριο και ώρες που πηγαίνουμε
  - μαγαζιά και πάρκα που σ υ χ ν ά ζ ο υ μ ε κλπ.

Πώς μπορεί να αποκαλυφθεί η ταυτότητα και η θέση σας (1)

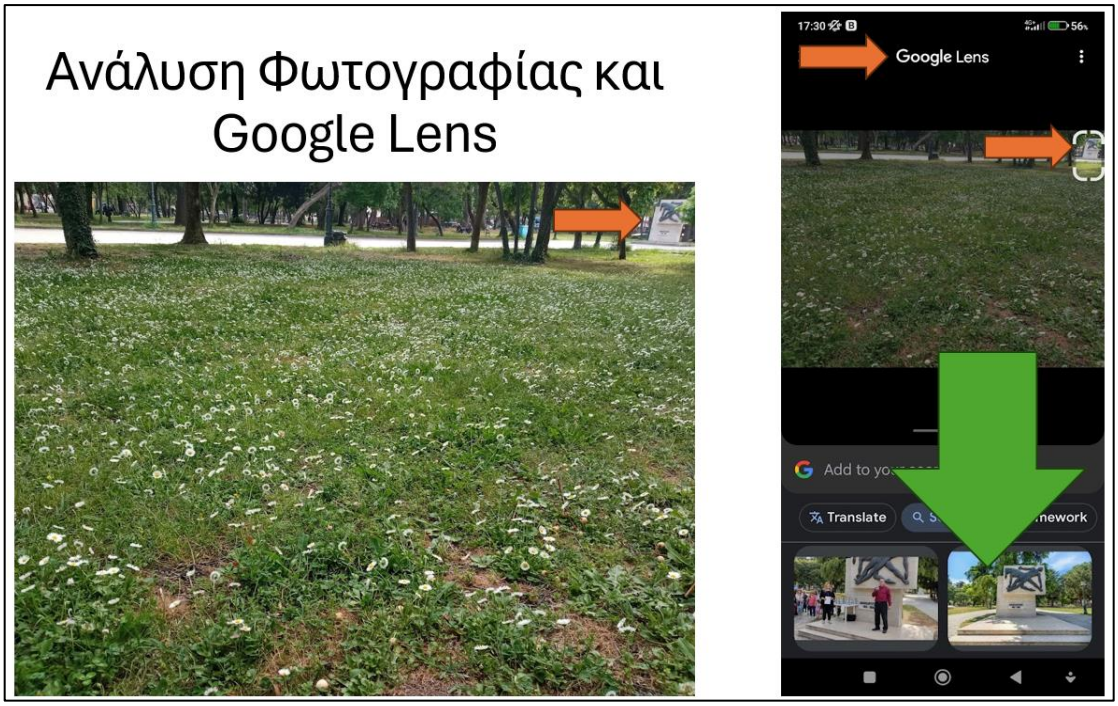
- **Από δημοσιεύσεις και σχόλια/απαντήσεις** αν αναφέρονται από σένα ή τους συνομιλητές σου κάποια από τα παρακάτω:
  - προσωπικές πληροφορίες (*πχ. Ονοματεπώνυμο, Σχολείο – Τάξη, Διεύθυνση κ.λπ*)
  - σημεία συνάντησης (πχ *Περιμένω απέναντι, στο άγαλμα του Καραϊσκάκη. Κατέβα.*)
  - συνήθειες που έχετε (*πχ. Στο κλειστό, 6-7 κάθε Σάββατο μεγαλουργώ στο βόλεϋ.*)
  - Ειδικά αν είναι προς "Φίλους/Ακολούθους" **που δεν γνωρίζουμε** ή Δημόσιες (Public)

  - **ΠΡΟΣΟΧΗ:** Οι παραπάνω πληροφορίες ίσως δοθούν από πραγματικούς φίλους μας **χωρίς να έχουν κακές προθέσεις**, το αποτέλεσμα όμως ίσως φανερώσει στοιχεία και για εσάς.
  - **Παράδειγμα**: Συμμαθητής σου έχει στείλει παλιότερα φωτογραφία σχολείου του, έχει γράψει σε ποιο σχολείο πάει/**έγραψε ή φαίνεται** πως είναι στην Ομάδα (Group) του Χ σχολείου **σε ρωτάει** σε σχόλιο «Θα έρθεις αύριο σχολείο;»)

Πώς μπορεί να αποκαλυφθεί η ταυτότητα και η θέση σας (2)

- **Φωτογραφίες και βίντεο,** αν φαίνονται χαρακτηριστικά σημεία της περιοχής σου όπως:
  - Πινακίδες διευθύνσεων οδών
  - Ταμπέλες καταστημάτων με πληροφορίες ή με σύμβολα
  - Εκκλησίες, Δημαρχεία, Γήπεδα, Σχολεία, πάρκα και άλλα **χαρακτηριστικά σημεία της περιοχής**
  - Checkins και Tagging-Mentioning
  - Φωτογραφίες με Geotagging
    (σημείο GPS που βάζει η κάμερα του κινητού αλλά πολλά Κοινωνικά Δίκτυα τις σβήνουν αυτόματα)
  - Συνδυασμός των παραπάνω με εξωτερικές συσκευές που βλέπουν προς συγκεκριμένη κατεύθυνση (κεραίες, ηλιακές συσκευές, κ.λπ)
  - **Και κυρίως** από το σπίτι μας, μέσα, έξω και γύρω από αυτό.
  - Συνδυασμός όλων των παραπάνω

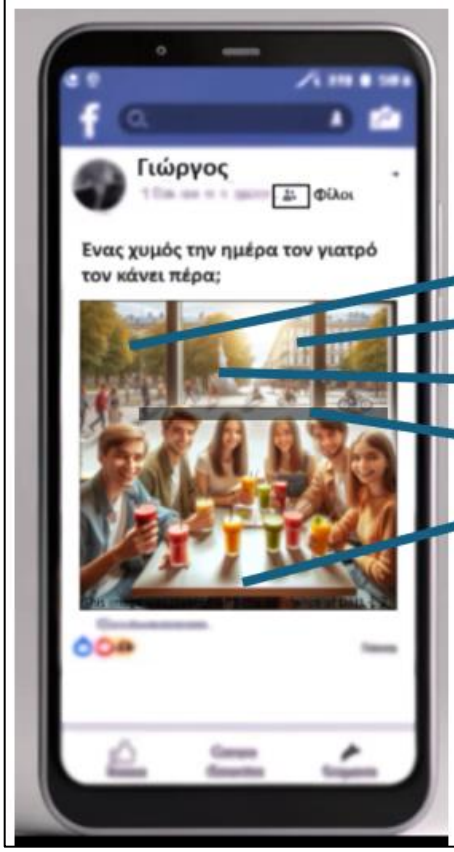
Παράδειγμα χρήσης δωρεάν της εφαρμογής Google Lens για εύρεση πληροφοριών από φωτογραφίες



Ποιες συνέπειες μπορεί να έχει η αποκάλυψη ταυτότητας και θέσης;

- Δημιουργία ψεύτικων λογαριασμών που με **φωτογραφίες** και **σχόλια** θα **βλάψουν τη φήμη** και ίσως και το εργασιακό **μέλλον** του.
- Παρενόχληση
- Ψυχολογική πίεση
- Απειλές
- Εκβιασμός

Λύσεις Α’ Φάσης



ΕΡΩΤΗΣΗ 1.1

Πάρκο

Νεοκλασικό κτίριο?

Άγαλμα

Πεζόδρομος

Μαγαζί

Εύρεση της θέσης με αναζήτηση σε **Google Maps** για :

- Πάρκα πόλης
- Αγάλματα πόλης
- Πεζόδρομοι

ΕΡΩΤΗΣΗ 1.2

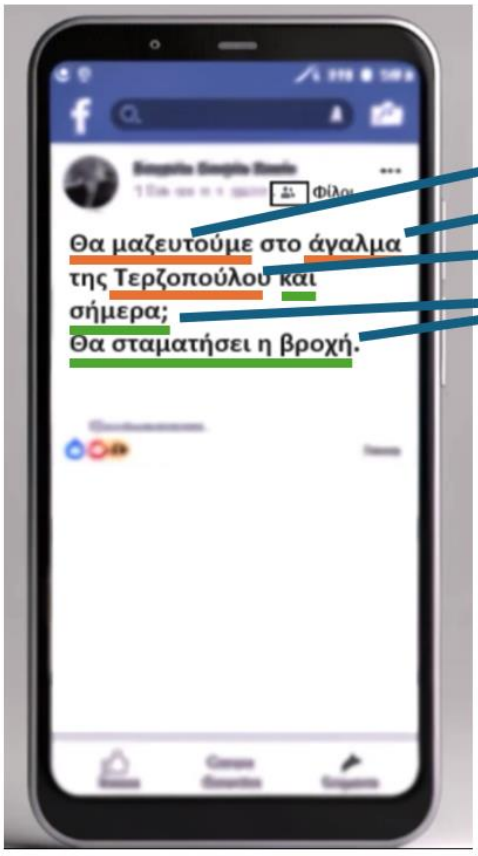
Πότε

Που (με αναζήτηση internet)

Ποιος

Παράδειγμα εύρεσης της θέσης – ταυτότητας με αναζήτηση σε μηχανή αναζήτησης για :

- Τελικός ποδοσφαίρου Κ16 στην Κατερίνη
- Αυριανή ημερομηνία
- Εύρεση του 22 στο γήπεδο



ΕΡΩΤΗΣΗ 1.3

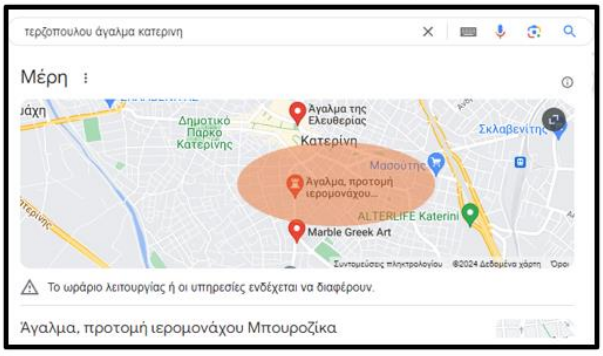
Ποιοι θα είναι

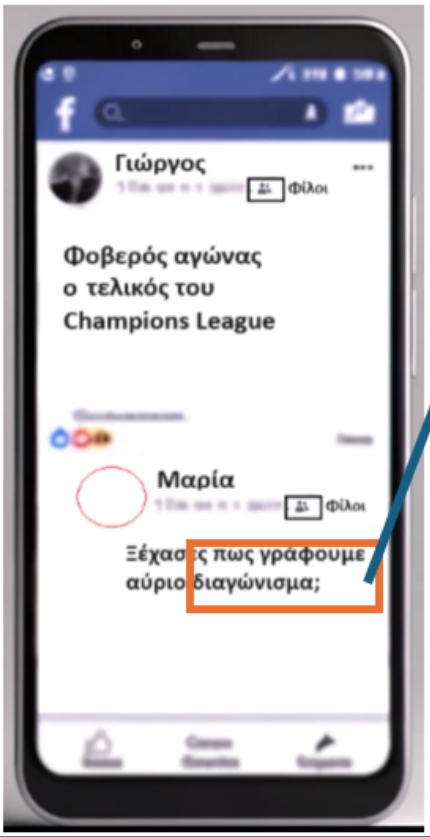
Που θα είναι - 1

Που θα είναι - 2

Πότε θα είναι

Παράδειγμα εύρεσης θέσης :
πχ. αναζήτηση στους Χάρτες της Google



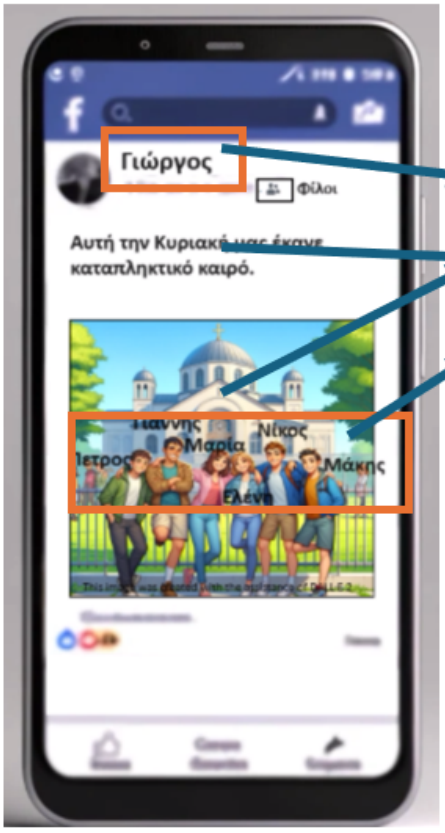


ΕΡΩΤΗΣΗ 1.4

Είναι συμμαθητές !

Παράδειγμα εύρεσης Σχολείου (θέσης – ταυτότητας) αν δεν το έχει στο προφίλ του ο Γιώργος επειδή προσέχει :

- σε φίλους της Μαρίας για το Σχολείο
- Για Group που ακολουθεί
- Για συμμαθητές της Μαρίας που να έγραψαν για το Σχολείο τους



ΕΡΩΤΗΣΗ 1.5

Ήταν και ο Γιώργος (έβγαλε φωτογραφία)

Που

Ποιοι

Παράδειγμα εύρεσης θέσης – ταυτότητας αν δεν έχει πληροφορίες στο προφίλ του ο Γιώργος επειδή προσέχει :

- Τις εκκλησίες τις βρίσκεις εύκολα από Google Maps
- Έγινε Tag σε 6 μέλη της παρέας
- Αναζήτηση στα προφιλ των φίλων για επιθυμητές πληροφορίες

Συμπεράσματα

1. Απλά μηνύματα και φωτογραφίες μας, μπορούν να δώσουν πολλές πληροφορίες Θέσης και Ταυτότητας σε κακόβουλους ανθρώπους.
2. Πληροφορίες για Θέση και Ταυτότητα μπορούν να αντληθούν και από «φίλους» μας στα Κοινωνικά Δίκτυα.
3. Προσέχουμε τι αναρτούμε και ποιοι «φίλοι» μπορούν να το δουν.
4. Υπάρχουν δωρεάν εφαρμογές που μπορούν να χρησιμοποιηθούν για κακόβουλη εύρεση πληροφοριών.
5. Το Διαδίκτυο δεν είναι καθόλου αθώο !

Ποιες συνέπειες μπορεί να έχει η αποκάλυψη ταυτότητας και θέσης;

- Δημιουργία ψεύτικων λογαριασμών που με **φωτογραφίες** και **σχόλια** θα **βλάψουν τη φήμη** και ίσως και το εργασιακό **μέλλον** του.
- Παρενόχληση
- Ψυχολογική πίεση
- Απειλές
- Εκβιασμός

10.4Παράρτημα Δ - Ερωτηματολόγιο εξόδου των μαθητών

Ερωτηματολόγιο διπλωματικής με θέμα «Ανάπτυξη πλαισίου επαγρύπνησης κυβερνοασφάλειας σε σχολικό πληθυσμό»

Το ερωτηματολόγιο αυτό είναι πλήρως ανώνυμο. Δεν θα σας ζητηθούν και δεν θα κρατηθούν με κανένα τρόπο, άμεσο ή έμμεσο, πληροφορίες που μπορούν να οδηγήσουν σε συσχέτιση απαντήσεων με το άτομο που το συμπλήρωσε.

ΠΑΝΑΓΙΩΤΙΔΗΣ ΣΩΤΗΡΙΟΣ
Απρίλιος-Μάιος 2024

---

1. Φύλο

- ◯ Κορίτσι
- ◯ Αγόρι

2. Έχετε Εφαρμογή Μηνυμάτων όπως *WhatsApp, Viber, Discord, κ.λπ.*;

- ◯ Έχω, είμαι σε ομάδα που έχει και αγνώστους.
- ◯ Έχω, δεν είμαι σε ομάδα που έχει και αγνώστους.
- ◯ Όχι, δεν έχω τέτοια εφαρμογή

2.1 Στέλνετε μηνύματα στις ομάδες με αγνώστους του *WhatsApp, Viber, Discord, κ.λπ.*;

- ◯ Δεν στέλνω, μόνο βλέπω τα μηνύματα της ομάδας
- ◯ Ναι, κάνω 1 ως 5 αποστολές τη βδομάδα
- ◯ Ναι, κάνω 6 ως 10 αποστολές τη βδομάδα
- ◯ Ναι, κάνω πάνω από 10 αποστολές τη βδομάδα

2.2 Έχετε κάνει αποστολή μηνυμάτων με πληροφορίες σαν των παραδειγμάτων που είδατε σήμερα σε ομάδες με αγνώστους του *WhatsApp, Viber, Discord, κ.λπ.*;

- ◯ Όχι
- ◯ Ναι, ελάχιστες φορές
- ◯ Ναι, συχνά

3. Έχετε λογαριασμό σε Κοινωνικό Δίκτυο με Φίλους/Ακόλουθους;

- ◯ Ναι
- ◯ Είχα παλιότερα, δεν έχω τώρα
- ◯ Δεν είχα και δεν έχω

3.1 Πόσες αναρτήσεις κάνετε σε Κοινωνικά Δίκτυα;

- ◯ Δεν αναρτώ, μόνο βλέπω αναρτήσεις και μιλάω με στενούς φίλους αντί με SMS
- ◯ Ναι, κάνω 1 ως 5 αναρτήσεις τη βδομάδα
- ◯ Ναι, κάνω 6 ως 10 αναρτήσεις τη βδομάδα
- ◯ Ναι, κάνω πάνω από 10 αναρτήσεις τη βδομάδα

3.2 Έχετε κάνει αναρτήσεις με πληροφορίες σαν των παραδειγμάτων που είδατε σε Κοινωνικά Δίκτυα;

- ◯ Οχι
- ◯ Ναι, ελάχιστες φορές
- ◯ Ναι, συχνά

4. Βελτιώσατε σήμερα τις γνώσεις σας στον εντοπισμό κινδύνων σε αναρτήσεις που μπορούν να αποκαλύψουν την ταυτότητα και τη θέση σας;

- ◯ Καθόλου
- ◯ Λίγο
- ◯ Αρκετά
- ◯ Πολύ
- ◯ Πάρα πολύ

5. Πόσο πιθανό είναι να εφαρμόσετε τις γνώσεις αυτές στην καθημερινή σας ζωή στο διαδίκτυο;

- ◯ Δεν θα τις εφαρμόσω
- ◯ Μάλλον θα τις εφαρμόσω
- ◯ Σίγουρα θα τις εφαρμόσω

6. Έχει συμβεί ποτέ κάποιο περιστατικό στο διαδίκτυο που σας αναστάτωσε;

- ◯ Ναι, έχει συμβεί σε εμένα
- ◯ Ναι, έχει συμβεί σε άτομο που γνωρίζω
- ◯ Ναι, έχει συμβεί και σε εμένα και σε άτομο που γνωρίζω
- ◯ Όχι