

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



Διπλωματική Εργασία

Αξιολόγηση προγραμμάτων επιμόρφωσης και επίγνωσης σχετικά με την ασφάλεια και το ηλεκτρονικό ψάρεμα (Phishing) στην δευτεροβάθμια εκπαίδευση. Ανάλυση της αποτελεσματικότητας των προγραμμάτων επιμόρφωσης με χρήση ερωτηματολογίου. Εξαγωγή αποτελεσμάτων και ανάλυση τους.

Σωτηρία Σαρδέλη

ΠΚΜ202011

Επιβλέπων καθηγητής: Χριστόφορος Νταντογιάν

Κέρκυρα, Μάρτιος, 2022



Αξιολόγηση προγραμμάτων επιμόρφωσης και επίγνωσης σχετικά με την ασφάλεια και το ηλεκτρονικό ψάρεμα (Phishing) στην δευτεροβάθμια εκπαίδευση. Ανάλυση της αποτελεσματικότητας των προγραμμάτων επιμόρφωσης με χρήση ερωτηματολογίου. Εξαγωγή αποτελεσμάτων και ανάλυση τους.

Σωτηρία Σαρδέλη

ΠΚΜ202011

Τριμελής επιτροπή

Χριστόφορος Νταντογιάν

Αγγελική Τσώχου

Ελένη Χριστοπούλου

Επίκουρος Καθηγητής

Επίκουρη Καθηγήτρια

ΕΔΙΠ

Τμήμα Πληροφορικής

Τμήμα Πληροφορικής

Τμήμα Πληροφορικής

Ιόνιο Πανεπιστήμιο

Ιόνιο Πανεπιστήμιο

Ιόνιο Πανεπιστήμιο

Κέρκυρα, Μάρτιος, 2022

Περίληψη

Η εποχή της πληροφορίας έρχεται με τους ανάλογους κινδύνους. Η ολοένα και αυξανόμενη χρήση του διαδικτύου ενέχει έναν αριθμό κινδύνων, ειδικά για τα παιδιά και τους εφήβους που δεν είναι σε θέση να διακρίνουν ακόμα τις ηλεκτρονικές επιθέσεις, συμπεριλαμβανομένων και των επιθέσεων ηλεκτρονικού ψαρέματος. Η ανάγκη ένταξης προγραμμάτων επιμόρφωσης και επίγνωσης στη δευτεροβάθμια εκπαίδευση κρίνεται απαραίτητη ούτως ώστε οι έφηβοι, συχνοί στόχοι και θύματα ηλεκτρονικών επιθέσεων, να μπορούν να αυτοπροστατευτούν από ενδεχόμενες, μελλοντικές απειλές. Αυτό άλλωστε δείχνουν και οι συνεχόμενες μελέτες σε διεθνές επίπεδο, όπως και τα διαφορετικά πιλοτικά προγράμματα επιμόρφωσης των μαθητών πάνω στο θέμα της ηλεκτρονικής ασφάλειας, όπως αυτά παρουσιάζονται παρακάτω.

Μέσα από έρευνα που διεξήχθη, στα πλαίσια της παρούσας εργασίας, καταδείχθηκαν κάποια σημαντικά ζητήματα σχετικά με την ηλεκτρονική ασφάλεια των μαθητών, από ένα ενδεικτικό δείγμα 100 εκπαιδευτικών και 107 μαθητών της δευτεροβάθμιας εκπαίδευσης. Οι απόψεις των εκπαιδευτικών, ειδικά των καθηγητών πληροφορικής, όπως και οι απαντήσεις των μαθητών, αντιπαραβαλλόμενες μεταξύ τους, έδειξαν είτε την ανάγκη ένταξης τέτοιων προγραμμάτων είτε ακόμα και την ανάγκη επαναδιαμόρφωσης του μαθήματος της πληροφορικής.

Λέξεις – Κλειδιά

Ηλεκτρονικό ψάρεμα, ηλεκτρονική ασφάλεια, δευτεροβάθμια εκπαίδευση

Abstract

The Information age is riddled with danger. The ongoing and growing use of the internet is imbedded with a number of risks, especially for children and teenagers, who are not yet in the position of identifying cyber-attacks, including those of phishing. The need to integrate training and awareness programs into the secondary education is essential, in order for teenagers, frequent targets and victims of cyber-attacks, to be able to protect themselves from potential and future attacks. This is shown by the ongoing studies, as well as the variant pilot training programs for students, on the subject of cyber security, as presented below.

The research, conducted for the need of the current paper, has shown some important issues, concerning the cyber security of the students, as illustrated by an indicative sample of 100 teachers and 107 students of secondary education. The views of teachers, especially those teaching computer science courses, as well as the students' responses, contrasting with each other, showed either the need to integrate such programs or even the need to reshape the current IT course.

Keywords

Phishing, internet security, secondary education

Περιεχόμενα

Περίληψη	ii
Abstract	iii
1. Θεωρητικό Πλαίσιο	1
1.1 Οι Προκλήσεις της Ηλεκτρονικής Ασφάλειας.....	1
1.2 Τι είναι το phishing. Όρος και ιστορία.....	3
1.3 Phishing – Τρόποι αναγνώρισης	6
1.4 Έφηβοι και η Σύγχρονη Πρόκληση του Phishing.....	8
1.5 Έφηβοι και Ηλεκτρονική Συμπεριφορά: Πόσο ενημερωμένοι είναι τελικά οι έφηβοι στους κινδύνους του διαδικτύου και τις μεθόδους αυτοπροστασίας;.....	11
1.6 Στρατηγικές επιμόρφωσης και επίγνωσης και ο ρόλος των καθηγητών της δευτεροβάθμιας εκπαίδευσης.....	15
2. Ερευνητικό Κομμάτι.....	20
2.1 Σκοπός και Στόχοι της Έρευνας.....	20
2.2 Μέθοδος	21
2.2.1 Δείγμα και Ερευνητικά Εργαλεία.....	21
2.2.2 Ερωτηματολόγιο Εκπαιδευτικών	26
2.2.3 Ερωτηματολόγιο Μαθητών	31
3. Ανάλυση Δεδομένων και Παρουσίαση Αποτελεσμάτων	36
3.1 Στάσεις και απόψεις εκπαιδευτικών.....	36
3.2 Στάσεις και απόψεις μαθητών	49
4. Συμπεράσματα	60
Βιβλιογραφία	62

1. Θεωρητικό Πλαίσιο

1.1 Οι Προκλήσεις της Ηλεκτρονικής Ασφάλειας

Η σημερινή εποχή, χαρακτηρίζεται ως η εποχή της πληροφορίας. Η χρήση του διαδικτύου, έχει επεκταθεί με γεωμετρικό ρυθμό σε όλη την υφήλιο. Σύμφωνα με έρευνα από το 2000 μέχρι το 2016 η χρήση του διαδικτύου σε παγκόσμιο επίπεδο είχε αυξηθεί κατά 900,4%, έκτοτε, λογικό είναι κάποιος να υποθέσει, ότι η χρήση έχει πολλαπλασιαστεί. Η μαζική χρήση του διαδικτύου όμως έρχεται μαζί με ανάλογους κινδύνους. Μερικοί από τους κινδύνους και τις προκλήσεις που έχουν αναδειχθεί είναι η ασφάλεια, το cyberbullying, το sexting, η λογοκλοπή και το phishing, που αποτελεί και το ζητούμενο στην παρούσα εργασία. Από τη στιγμή που η χρήση έχει γίνει τόσο μαζική και σε καθημερινή βάση η ενσωμάτωση των νέων τεχνολογιών στην εκπαιδευτική διαδικασία έχει αυξηθεί και επομένως το σχολείο θα μπορούσε να συμβάλλει σε μεγάλο βαθμό στην αντιμετώπιση των κινδύνων του διαδικτύου. Η διαδικασία αυτή έρχεται όμως με προκλήσεις (Tirumala, Sarrafzadeh, & Pang, 2016, σ. 223).

Η κυβερνο-προστασία αποτελεί, όπως καταδεικνύουν τα παραπάνω, έναν τομέα με ανάγκη επέκτασης και γρήγορης επιτάχυνσης. Σύμφωνα με έρευνες όμως, η έλλειψη ικανοποιητικώς καταρτισμένων ατόμων που μπορούν να βοηθήσουν απέναντι σε αυτή τη νέα απειλή δημιουργεί κενό και ένα μεγάλο πρόβλημα, που έρχεται μαζί με αυτό. Σύμφωνα με την ίδια έρευνα ένας από τους λόγους της έλλειψης κατάρτισης είναι και η έλλειψη εκπαίδευσης. Αυτό συμβαίνει καθώς οι σπουδές που απαιτούνται από ανώτατα εκπαιδευτικά ιδρύματα είναι χρονοβόρες, απαιτητικές και εξειδικευμένες. Ως αποτέλεσμα ένα μεγάλο μέρος των μαθητών και σπουδαστών που έχουν ολοκληρώσει τις δευτεροβάθμιες ή προπτυχιακές τους σπουδές, αντίστοιχα, δε συνεχίζουν σε επίπεδο μεταπτυχιακών και διδακτορικών εξειδικεύσεων, ίσως λόγω του επικείμενου φόρτου, δημιουργώντας έτσι αυτό το κενό κατάρτισης (Cyber Innovation Center, 2020, σ. 2). Η μειωμένη εκπροσώπηση και γυναικών, ή και μειονοτήτων, επιπλέον στο χώρο των επιστημών της πληροφορικής, παρά την ολοένα και μεγαλύτερη ένταξή τους σε προγράμματα σπουδών STEM, δε βοηθάει στην αναβάθμιση του τομέα της ασφάλειας

με επιπλέον εξειδικευμένο ανθρώπινο δυναμικό σε αυτήν, που θα μπορούσε να γεμίσει τα ολοένα και αυξανόμενα κενά (Mountrouidou, και συν., 2019, σ. 157)

Τίθεται λοιπόν το θέμα της σωστής εκπαίδευσης, ευαισθητοποίησης και πιθανής επαγγελματικής προσέγγισης, ήδη από το επίπεδο της δευτεροβάθμιας εκπαίδευσης. Ο τομέας της κυβερνο-προστασίας αποτελεί μέρος των επιστημών πληροφορικής και δυστυχώς τομέα με ανεπαρκές προσωπικό. Η ανάγκη επομένως σωστής εκπαίδευσης και εξειδίκευσης οφείλει να ξεκινήσει από τις πρώτες τάξεις της δευτεροβάθμιας εκπαίδευσης, αν όχι ήδη από την πρωτοβάθμια. Με αυτόν τον τρόπο μπορούν να τεθούν οι βάσεις δημιουργίας μιας μελλοντικής γενιάς, ευαισθητοποιημένης σε θέματα προστασίας του διαδικτύου, η οποία όμως πρέπει να έχει και στέρεες θεωρητικές βάσεις. Σε θεωρητικό επίπεδο αυτή είναι μια σωστή και εύκολη στρατηγική. Σε πρακτικό επίπεδο όμως, έρχεται αντιμέτωπη με άλλες σημαντικές δυσκολίες. Η σωστή εκπαίδευση των μαθητών έρχεται χέρι με χέρι με άρτια εξειδικευμένους καθηγητές, και ένα άρτια οργανωμένο πρόγραμμα σπουδών (Javidi & Sheybani, 2018, σσ. 1-2). Φυσικά για να μπορέσουν αυτά να επιτευχθούν οι καθηγητές της δευτεροβάθμιας εκπαίδευσης θα πρέπει να είναι σε θέση να παρεμβαίνουν με θετικό τρόπο. Αυτό όμως είναι κάτι που απαιτεί γνώσεις ή περαιτέρω εκπαίδευση.

Στην παρούσα εργασία θα καταδειχθούν, λοιπόν, η ιστορία και ο κίνδυνος του ηλεκτρονικού ψαρέματος, πώς μπορεί να επηρεάσει παιδιά και εφήβους, το κατά πόσο παιδιά και έφηβοι είναι σε θέση να αντιληφθούν τους κινδύνους του ηλεκτρονικού ψαρέματος, μέθοδοι επίγνωσης αυτού του κινδύνου, όπως και ο ρόλος της δευτεροβάθμιας εκπαίδευσης στην απόκτηση δεξιοτήτων από τους μαθητές για την αντιμετώπιση των κινδύνων της ηλεκτρονικής ασφάλειας.

1.2 Τι είναι το phishing. Όρος και ιστορία

Η ασφάλεια στο διαδίκτυο αποτελεί μια συνεχόμενη πρόκληση. Οι επιθέσεις από hackers και οι περιπτώσεις εξαπάτησης συνεχώς εξελίσσονται με τη χρήση νέων μεθόδων και εργαλείων. Ένα από αυτά τα εργαλεία, με στόχο την απόσπαση ευαίσθητων πληροφοριών ή κωδικών είναι το ηλεκτρονικό ψάρεμα (phishing), ή η μαζική αποστολή email από φαινομενικά αξιόλογες εταιρείες με στόχο την απόσπαση αυτών των ευαίσθητων δεδομένων. Σαν όρος υπάρχει καταγεγραμμένος από την 2^η Ιανουαρίου 1996, στην Αμερική, από μία ομάδα hackers πίσω από την εφαρμογή AOHell, οι οποίοι με αλγόριθμο που δημιούργησαν, ήταν σε θέση να υποδυθούν υπαλλήλους της America Online (AOL), και μέσω μηνυμάτων να αποσπάσουν προσωπικές πληροφορίες των χρηστών της (History of Information). Σε αυτήν την αρχική φάση οι πελάτες της AOL που είχαν πέσει θύματα παραχωρούσαν τις ζητούμενες πληροφορίες, κάτι φυσικά και για την εποχή αναμενόμενο από την στιγμή που δεν υπήρχε προηγούμενο. Ο κίνδυνος έγινε ακόμα εντονότερος με τη δημιουργία λογαριασμών AIM (AOL Instant Messenger), με την AOL να μην είναι σε θέση να προβεί σε κυρώσεις, και τελικώς να περιλαμβάνει προειδοποιήσεις προς τους χρήστες της για τους κινδύνους παροχής ευαίσθητων προσωπικών δεδομένων μέσω ηλεκτρονικών μηνυμάτων (Online Education).

Σύμφωνα με την ιστοσελίδα phishing.org, «το phishing αποτελεί μια μορφή κυβερνοεγκλήματος, του οποίου το θύμα ή τα θύματα έρχονται σε επαφή μέσω email, τηλεφώνου ή ακόμα και μέσω γραπτού μηνύματος με κάποιον που παριστάνει εκπρόσωπο ή υπάλληλο μιας νόμιμης επιχείρησης ή ενός θεσμού, με στόχο να παρασύρει τα άτομα να παραχωρήσουν ευαίσθητα δεδομένα όπως ατομικές πληροφορίες, τραπεζικές λεπτομέρειες και λεπτομέρειες τραπεζικών καρτών, όπως και κωδικούς ασφαλείας. Αυτές οι πληροφορίες χρησιμοποιούνται αργότερα με στόχο την πρόσβαση σε λογαριασμούς και μπορούν να οδηγήσουν τελικώς σε κλοπή ταυτότητας ή ακόμα και σοβαρές οικονομικές απώλειες (phishing.org).

Δεν είναι λοιπόν απορίας άξια η προέλευση και η ετυμολογία του όρου για το συγκεκριμένο τύπο ηλεκτρονικών εγκλημάτων, phishing (=ψάρεμα). Αν και αντί για f-, γράφεται με ph-, καθώς, σύμφωνα με την ίδια ιστοσελίδα μία από τις αρχικές ορολογίες για να περιγράψει τους hackers ήταν phreaks, με το phreaking να περιγράφει

τις δραστηριότητες που σχετίζονται με τον πειραματισμό και την εξερεύνηση των τηλεπικοινωνιακών συστημάτων (phishing.org).

Έκτοτε η λογική πίσω από το ηλεκτρονικό ψάρεμα δεν έχει αλλάξει σε μεγάλο βαθμό. Ακόμα και σήμερα αποτελεί έναν υπαρκτό κίνδυνο στο διαδίκτυο, αν και η εστίαση του έχει αλλάξει. Από το 2001 κύριος στόχος είναι τα τραπεζικά δεδομένα και οι online μέθοδοι πληρωμής. Με τη δημιουργία domains που να προσομοιάζουν σε αυτά των eBay και PayPal, ζητούσαν μέσω email την επιβεβαίωση και ενημέρωση των στοιχείων τραπεζικών καρτών. Με αντίστοιχο τρόπο, έχουν πέσει θύματα επίθεσης και τραπεζικές ιστοσελίδες και οι πελάτες τους, και με τη χρήση popur παραθύρων έχουν υποστεί υπεξαίρεσης ευαίσθητων πληροφοριών εκατομμύρια άνθρωποι. Σύμφωνα με έρευνα εταιρείες χάνουν περίπου δύο δισεκατομμύρια δολάρια το χρόνο μέσω του ηλεκτρονικού ψαρέματος (phishing.org).

Το ηλεκτρονικό ψάρεμα και οι κίνδυνοι που έρχονται με αυτό εξακολουθούν να υφίστανται ακόμα και σήμερα και σε ακόμα μεγαλύτερη έκταση σε σχέση με το παρελθόν. Η χρήση https από το 2017 και έπειτα σε ιστοσελίδες ηλεκτρονικού ψαρέματος δημιουργεί μια ψεύτικη αίσθηση ασφάλειας από τους χρήστες, δίνοντας χωρίς δεύτερη σκέψη τις πληροφορίες τους. Επιπλέον με τη χρήση kit, διαθέσιμων στο Dark Web, επιτρέπει σε όποιον τα χρησιμοποιεί να δημιουργήσει πειστικά και αληθοφανή email και sites, τα οποία παραπέμπουν σε επωνυμίες μεγάλων εταιριών, συλλέγοντας και με αυτόν τον τρόπο πληροφορίες. Η χρήση gift-cards αποτελεί επιπλέον άλλη μια στρατηγική, ιδιαίτερα διαδεδομένη από το 2019, δίνοντας ψεύτικα οικονομικά κίνητρα σε όποιον απευθύνονται (phishing.org).

Σύμφωνα με τη Microsoft μερικές από τις πιο πρόσφατες μεθόδους ηλεκτρονικού ψαρέματος περιλαμβάνουν email με ψεύτικους συνδέσμους google, που οδηγούν σε sites με κακόβουλο λογισμικό, μη υπαρκτές ιστοσελίδες, συνήθως με το μήνυμα '404', όπως και ρεαλιστικές σελίδες σύνδεσης στο Office 365, που κι εδώ φυσικά ζητούνται προσωπικές πληροφορίες (Microsoft, 2019).

Τέλος από τις αρχές του 2020 και της πανδημίας του Covid-19 τα email ηλεκτρονικού ψαρέματος έχουν πολλαπλασιαστεί με γεωμετρικό ρυθμό. Η πιο συνήθης θεματολογία σε αυτά περιλαμβάνει ψεύτικες προειδοποιήσεις, εργασία από το σπίτι, απάτες σχετικές με το Netflix, και άλλα θέματα αναλόγως τη χώρα στην οποία βρίσκεται το επίδοξο

θύμα. Αυτό το φαινόμενο έχει καταδείξει όσο ποτέ την ανάγκη προστασίας από μεριάς των εταιριών και συνεχούς ενημέρωσης των χρηστών του διαδικτύου, ούτως ώστε να μην πέφτουν θύματα τέτοιων πρακτικών (phishing.org).

1.3 Phishing – Τρόποι αναγνώρισης

Αν και οι επιθέσεις ηλεκτρονικού ψαρέματος έχουν εξελιχθεί σε μεγάλο βαθμό, και πλέον θα μπορούσε να πει κανείς ότι έχει αναδειχθεί σε τέχνη, με τη δημιουργία εξαιρετικά αληθοφανών λογότυπων και url, υπάρχουν αρκετά σημεία, τα οποία, αν ο χρήστης είναι παρατηρητικός και προσεχτικός, θα μπορέσει να αυτοπροστατευθεί.

Οι ανακολουθίες και οι ανακρίβειες στο url είναι ένας πρώτος τρόπος αναγνώρισης. Οι υπερσύνδεσμοι συνήθως κρύβουν τον κίνδυνο, που ο χρήστης πρέπει να αποφεύγει. Με το να μετακινεί το δείκτη του ποντικιού πάνω από το link, χωρίς όμως να το πατάει, ο χρήστης μπορεί να δει ότι η σελίδα δεν είναι η αυθεντική, αλλά συνήθως redirect στην πραγματικά κακόβουλη ιστοσελίδα.

Η μη σωστή χρήση γραμματικής και ορθογραφίας είναι άλλος ένας τρόπος αναγνώρισης. Οι διακεκριμένες εταιρίες και εκπαιδευτικοί θεσμοί προσλαμβάνουν υψηλά εκπαιδευμένο προσωπικό, και πάντα προβαίνουν σε έλεγχο, γραμματικό και συντακτικό, πριν την αποστολή email. Αυτού του είδους τα λάθη επομένως είναι μια σαφής ένδειξη προσπάθειας απάτης.

Το αίτημα παροχής προσωπικών στοιχείων επίσης πρέπει να κρούει τον κώδωνα του κινδύνου. Οι μεγάλες, αξιόπιστες εταιρίες, οι τράπεζες και τα εκπαιδευτικά ιδρύματα δεν αποστέλλουν email για την ενημέρωση στοιχείων, όπως προσωπικών κωδικών, ονόματος χρήστη ή άλλες ευαίσθητες προσωπικές πληροφορίες. Ο χρήστης επομένως θα πρέπει αμέσως να υποψιαστεί ότι δεν πρόκειται για email από υπάρχουσα εταιρεία.

Ο τόνος του email είναι άλλη μία ένδειξη. Χρήση χαιρετισμού, όπως ‘Αγαπητέ Πελάτη’ πέφτει σε αυτήν την κατηγορία, καθώς τα πραγματικά μηνύματα περιέχουν προσωπικό και όχι γενικό χαιρετισμό προς τους πελάτες ή τους χρήστες τους. Επιπλέον, ο επιθετικός, ο απειλητικός ή ο τόνος του κατεπείγοντος αποτελεί μέρος παραπλανητικών μηνυμάτων, που προσπαθούν με αυτή την τακτική να δημιουργήσουν συναισθήματα πανικού στα επίδοξα θύματά τους, με στόχο την όσο πιο γρήγορη και χωρίς σκέψη παροχή των πληροφοριών που ζητούνται.

Μία από τις παλαιότερες απάτες, που αγγίζει τα όρια του αστείου στη σημερινή εποχή είναι η απάτη του Νιγηριανού Πρίγκιπα. Αποτελεί μία απάτη από τη δεκαετία ήδη του

1990, κατά την οποία ζητείται από το επίδοξο θύμα μια μικρή οικονομική διευκόλυνση μέχρι ο ‘πρίγκιπας’ να μπορέσει να αποκτήσει πρόσβαση στην προσωρινά δεσμευμένη αμύθητη περιουσία του, με αντάλλαγμα ένα μέρος αυτής. Φυσικά, έκτοτε, αυτού του είδους οι απάτες έχουν εξελιχθεί, για να γίνουν πιο πιστευτές, πάντα όμως με το πρόσχημα μιας οικονομικής υπόσχεσης, ειδικά αν ο χρήστης δεν είναι ενημερωμένος για αυτές (Online Education).

Εκ πρώτης όψεως, για κάποιον ο οποίος έχει λάβει σωστή ενημέρωση, αυτού του είδους οι ενδείξεις φαίνονται ξεκάθαρες. Η πραγματικότητα όμως είναι ότι χιλιάδες έως εκατομμύρια άνθρωποι κάθε μέρα πέφτουν θύματα ηλεκτρονικού ψαρέματος παγκοσμίως. Η ανάγκη ενημέρωσης είναι πιο επιτακτική από ποτέ. Ειδικά για τους μαθητές και τα παιδιά μικρής και νεαρής ηλικίας, η σωστή εκπαίδευση από το σχολείο κρίνεται παραπάνω από αναγκαία. Στα επόμενα μέρη της παρούσας εργασίας, θα αναλυθούν πιο συγκεκριμένα οι κίνδυνοι τους οποίους οι μαθητές διατρέχουν κατά τη χρήση του internet και πώς και εάν αυτοί μπορούν να αποφευχθούν μέσα από το σχολείο και προγράμματα επιμόρφωσης σε αυτό, με στόχο την ασφαλή χρήση του διαδικτύου και την αποφυγή φαινομένων ηλεκτρονικού ψαρέματος.

1.4 Έφηβοι και η Σύγχρονη Πρόκληση του Phishing

Όπως αναφέρθηκε, μέσω του ηλεκτρονικού ψαρέματος, επιτήδριοι προσπαθούν να αποσπάσουν από τα θύματά τους προσωπικές πληροφορίες, συνήθως χρησιμοποιώντας πλαστά διαπιστευτήρια. Ο στόχος, στην πληθώρα των περιπτώσεων, είναι η απόσπαση χρηματικών ποσών και για αυτό το λόγο εταιρείες και τράπεζες προσπαθούν, μέσω αντιμέτρων, να αντιμετωπίσουν τις επιθέσεις ηλεκτρονικού ψαρέματος προς τις ίδιες και τους πελάτες τους. Παρόλα αυτά τα αντίμετρα και τα προγράμματα επιμόρφωσης συνήθως αφορούν ενήλικες (Lastdrager, Carvajal Gallardo, Hartel, & Junger, 2017, σ. 229).

Σύμφωνα με έρευνα που διεξήχθη στο πανεπιστήμιο Carnegie στην Πενσυλβάνια, ανάμεσα σε μέλη του προσωπικού, εκπαιδευτικούς και φοιτητές, διαπιστώθηκε ότι οι φοιτητές είναι η πιο ευάλωτη ομάδα σε επιθέσεις ηλεκτρονικού ψαρέματος. Σε σχέση με το προσωπικό και τους εκπαιδευτικούς μεγαλύτερης ηλικίας, οι φοιτητές ηλικιών 18-25 απεδείχθησαν οι πιο επιρρεπείς στο να ανοίξουν, ή και να απαντήσουν σε ύποπτα email ή να πατήσουν τους συνδέσμους που βρίσκονται σε αυτά (Kumaraguru, και συν., 2009, σ. 8). Το πρόβλημα όμως έλλειψης γνώσεων και επιμόρφωσης ξεκινάει σε μικρότερη ηλικία.

Τα παιδιά και οι έφηβοι, ακριβώς λόγω της αυξανόμενης χρήσης του διαδικτύου αποτελούν έναν καινούργιο και εύκολο στόχο. Τα σημερινά παιδιά και οι έφηβοι αποτελούν τη λεγόμενη γενιά του διαδικτύου. Είναι παιδιά τα οποία μεγάλωσαν με το διαδίκτυο ήδη βαθιά ενταγμένο στην καθημερινότητά τους, και με τα μέσα κοινωνικής δικτύωσης να αποτελούν ένα αναπόσπαστο κομμάτι της ζωής τους. Σύμφωνα με έρευνα περίπου το 25% των παιδιών ηλικίας 9 ετών και το 73% των εφήβων από την ηλικία των 13 ετών έχουν δημιουργήσει τουλάχιστον έναν λογαριασμό στα μέσα κοινωνικής δικτύωσης. Συνολικά, το 92% των παιδιών και εφήβων στην Αμερική και το 60% των παιδιών και εφήβων στην Ευρώπη έχουν μια μεγάλη παρουσία στο διαδίκτυο. Αυτό, όμως, δε σημαίνει ότι κατέχουν και τις απαραίτητες ψηφιακές δεξιότητες (Lastdrager, Carvajal Gallardo, Hartel, & Junger, 2017, σ. 229).

Δεν πρέπει να ξεχνάει κανείς ότι πρόκειται και για μια ευαίσθητη και ειδική ηλικιακή ομάδα. Οι έφηβοι ειδικά αποτελούν μια ιδιαίτερα ευάλωτη ηλικιακή ομάδα. Πρόκειται για μια ιδιαίτερη αναπτυξιακή περίοδο στη ζωή ενός ανθρώπου, όπου ο εγκέφαλος

ακόμα αναπτύσσεται. Οι έφηβοι επομένως συνήθως λειτουργούν βάσει άμεσων επιβραβεύσεων, οι οποίες συνήθως έρχονται μέσω της ανάληψης κινδύνου. Η δημιουργία λογαριασμών, συνδεδεμένων με μεθόδους ηλεκτρονικών πληρωμών εντάσσεται σε αυτήν την κατηγορία, καθιστώντας τους ευάλωτους σε επίθεση που έχει στόχο την απόσπαση χρημάτων. Ένα χαρακτηριστικό των εφήβων άλλωστε είναι ο αντιδραστικός τρόπος σκέψης, και όχι η ανάλυση μέσω λογικών συλλογισμών, κάνοντάς τους να αντιδρούν και να παίρνουν αποφάσεις άμεσα και γρήγορα. Αυτός ο τρόπος σκέψης, όπου εδώ πρέπει να επισημανθεί ότι αποτελεί ένα φυσιολογικό αναπτυξιακό χαρακτηριστικό, τους καθιστά ευάλωτους και σε email ηλεκτρονικού ψαρέματος, καθώς δεν είναι σε θέση να αναρωτηθούν αν πρόκειται για γνήσιο ή όχι, λόγω του αισθήματος πανικού που βιώνουν εκείνη τη στιγμή. Αυτό που τους κάνει ακόμα πιο ευάλωτους σε επιθέσεις είναι και το ηλεκτρονικό τους αποτύπωμα, δεδομένου ότι συνήθως ανταλλάσσουν πληροφορίες σε μεταξύ τους συνομιλίες, χωρίς δεύτερη σκέψη. Δε βοηθάει τέλος, η τάση των ενηλίκων να βασίζονται σε εφήβους για τη δημιουργία των δικών τους προσωπικών λογαριασμών, ή τη διεξαγωγή συναλλαγών, αφήνοντάς τους και αυτούς διάτρητους σε απειλές, υπερεκτιμώντας τις ψηφιακές δεξιότητες των εφήβων (Nicholson, και συν., 2020, σσ. 140-141).

Επιπλέον, ένα ακόμα πρόβλημα είναι η έλλειψη, ή και η απουσία σε αρκετές περιπτώσεις, γονικής επίβλεψης. Τα παιδιά και οι έφηβοι διαθέτουν όλο και περισσότερο δικές τους προσωπικές συσκευές. Η πρακτική αυτή οδηγεί τα παιδιά στο να αποθηκεύουν τους κωδικούς, χωρίς τακτικές αλλαγές, κωδικούς τραπεζικών καρτών των γονιών, ή ακόμα και προσωπικές πληροφορίες, τακτική η οποία έχει οδηγήσει στην αύξηση της κλοπής ταυτοτήτων ακόμα και παιδιών κάτω των 17 ετών. Αλλά ακόμα και υπό γονική επίβλεψη δε φαίνεται να βελτιώνεται η κατάσταση, καθώς εδώ γίνεται λόγος για μια γενιά, η πλειοψηφία των μελών της οποίας, δεν έχει εντάξει ακόμα τη σημασία και τις πρακτικές της ασφάλειας στο διαδίκτυο στην καθημερινότητά της (Nicholson, και συν., 2020, σ. 140).

Αυτοί είναι και οι λόγοι που τα παιδιά και οι έφηβοι αποτελούν ένα συνήθη στόχο επιθέσεων ηλεκτρονικού ψαρέματος. Η σχεδόν καθημερινή τους παρουσία στο διαδίκτυο, με τις ανεπαρκείς ψηφιακές δεξιότητες τα καθιστούν ένα εύκολο στόχο, με έναν τρόπο που είναι και το ίδιο ευάλωτα στις στρατηγικές μάρκετινγκ. Ο απώτερος στόχος δεν είναι τα ίδια, αλλά συνήθως οι πληροφορίες των γονιών τους. Με την απόσπαση ακόμα και μιας φαινομενικά μικρής και αμελητέας πληροφορίας, όπως ο

αριθμός τηλεφώνου, η διεύθυνση ή η διεύθυνση ηλεκτρονικού ταχυδρομείου, με τη χρήση ενός φαινομενικά αθώου και προσωποποιημένου μηνύματος, η απόσπαση προσωπικών, ευαίσθητων πληροφοριών γίνεται μια ακόμα πιο εύκολη υπόθεση (Lastdrager, Carvajal Gallardo, Hartel, & Junger, 2017, σ. 229).

Γίνεται λοιπόν επιτακτικό τα παιδιά και οι έφηβοι, όπως και οι γονείς τους, να γνωρίζουν και να αναγνωρίζουν τους πιθανούς κινδύνους του διαδικτύου. Οι τελευταίες εξελίξεις έρχονται να το επιβεβαιώσουν με τον χειρότερο τρόπο. Η πανδημία του Covid-19 κατέδειξε την ανάγκη για τη μετακίνηση στην εξ αποστάσεως εκπαίδευση, ως τρόπου μη εξάπλωσής της. Σε αρκετές χώρες η χρήση του Zoom και του WebEx για την εκπαιδευτική διαδικασία αποτέλεσε τον ενδεδειγμένο τρόπο δράσης. Αυτό όμως οδήγησε και σε άλλους κινδύνους, με περιπτώσεις, του λεγόμενου, ‘Zoombombing’ να λαμβάνουν χώρα, όπου ‘trolls’ κατάφεραν να μπαίνουν στις πλατφόρμες κατά τη διάρκεια του μαθήματος, χρησιμοποιώντας από αγενή έως βαθιά προσβλητική γλώσσα, ή ακόμα και διαμοιράζοντας προσβλητικό περιεχόμενο, όπως εικόνες πορνογραφίας. Επιπλέον, σε αρκετές περιπτώσεις και σχολεία έπεσαν θύματα επιθέσεων, λόγω της έλλειψης προσωπικού ηλεκτρονικής ασφάλειας ή της έλλειψης κατάλληλης εκπαίδευσής τους. Ως αποτέλεσμα γονείς και μαθητές διέτρεχαν ή πατούσαν σε συνδέσμους για την ηλεκτρονική τάξη, οι οποίοι, αν και εκ πρώτης όψεως φαίνονταν οι σωστοί, όταν άνοιγαν ζητούσαν προσωπικές πληροφορίες. Η χρήση προσωπικών συσκευών από τους μαθητές και τους εκπαιδευτικούς δε βοήθησε κατά των κινδύνων, λόγω των μειωμένων, έως και ανύπαρκτων, ρυθμίσεων ασφαλείας που απαιτούνται για αυτού του είδους τη χρήση (Samsel, 2020).

Στο επόμενο κομμάτι της εργασίας είναι ιδιαιτέρως χρήσιμο να αναδειχθούν και άλλα προβλήματα σχετικά με την επίγνωση των παιδιών και των εφήβων σε θέματα προσωπικής ηλεκτρονικής ασφάλειας, αλλά και πώς αντιδρούν σε επιθέσεις ηλεκτρονικού ψαρέματος.

1.5 Έφηβοι και Ηλεκτρονική Συμπεριφορά: Πόσο ενημερωμένοι είναι τελικά οι έφηβοι στους κινδύνους του διαδικτύου και τις μεθόδους αυτοπροστασίας;

Όπως τονίστηκε στο προηγούμενο κομμάτι της εργασίας τα παιδιά, και κυρίως οι έφηβοι, είναι ιδιαίτερα ευάλωτα σε επιθέσεις ηλεκτρονικού ψαρέματος. Ένα από τα στοιχεία που τα καθιστά ευάλωτα είναι η μαζική εξάπλωση του διαδικτύου, αλλά και η ίδια η ηλικία τους, η οποία και αποτελεί μια ιδιαίτερη περίοδο στη ζωή ενός ανθρώπου. Αλλά ποια άλλα επιπλέον χαρακτηριστικά παρουσιάζει η γενικότερη συμπεριφορά των εφήβων στο διαδίκτυο;

Σύμφωνα με έρευνα των Tirumala, Sarrafzadeh και Pang σε μαθητές και φοιτητές ηλικιών μεταξύ 8 και 21 ετών, καταδείχθηκε ότι παρά την συνεχώς εκτεταμένη χρήση του διαδικτύου, δεν υπήρχε ανάλογη αύξηση της επίγνωσης σε θέματα προστασίας και ασφαλείας. Οι συμμετέχοντες μαθητές δείχνουν να είναι εξοικειωμένοι με έννοιες όπως τείχος προστασίας, απόρρητο και antivirus, αλλά όχι με έννοιες όπως trackers και phishing. Συγκεκριμένα για το ηλεκτρονικό ψάρεμα, η έρευνα έδειξε ότι από τη μικρότερη ηλικιακή ομάδα στην επόμενη (8-12, 13-17, 18-21) η επίγνωση για αυτό μπορεί να αυξάνεται, αλλά όχι σε ικανοποιητικά ποσοστά, δημιουργώντας έτσι την ανάγκη για την παροχή ενημέρωσης για το συγκεκριμένο θέμα από μικρή ηλικία. Επιπλέον, όσον αφορά τα λογισμικά ασφαλείας, η έρευνα κατέδειξε ότι οι μαθητές γνωρίζουν για αυτά, αλλά δεν έχουν επίγνωση για την ανάγκη εγκατάστασής τους σε smartphones και tablets, στα οποία και η χρήση είναι μεγαλύτερη. Άλλο ένα προβληματικό αποτέλεσμα της εν λόγω έρευνας είναι ότι η πλειονότητα των συμμετεχόντων δεν έχει διαβάσει ποτέ τους όρους και τις προϋποθέσεις κατά την εγκατάσταση εφαρμογών, ή στην αποδοχή σύνδεσης με άλλες συσκευές, ειδικά στις νεαρότερες ηλικίες. Τέλος, ένα πολύ μικρό ποσοστό είχε επίγνωση ότι κατά την εγκατάσταση εφαρμογών ή την παρακολούθηση υπάρχει η πιθανότητα το λογισμικό να αποκτήσει πρόσβαση, χωρίς την άδεια του χρήστη, σε πληροφορίες, που δεν είναι απαραίτητες για την εγκατάστασή του, αλλά που μπορεί να χρησιμοποιηθούν για άλλους σκοπούς (Tirumala, Sarrafzadeh, & Pang, 2016, σσ. 224-227).

Σε έρευνα των Nicholson, Javed, Dixon, Coventry, Ajayi και Anderson για την ικανότητα των εφήβων να διακρίνουν περιπτώσεις ηλεκτρονικού ψαρέματος τα

αποτελέσματα ήταν ακόμα πιο ανησυχητικά. Σε γενικές γραμμές, και παρά το γεγονός ότι οι συμμετέχοντες μαθητές ήξεραν για το στόχο της μελέτης οι απαντήσεις τους κατέδειξαν ότι δεν είναι σε θέση να διακρίνουν πότε έχουν πέσει θύματα ηλεκτρονικού ψαρέματος και πώς να προστατευτούν μετά από μια τέτοια επίθεση. Αν και ένα σημαντικό ποσοστό ήταν σε θέση να διακρίνει την επίθεση κατά τη διάρκεια της προσομοίωσης, οι ερευνητές δεν είναι πεπεισμένοι ότι θα μπορούσαν να διακρίνουν μία πραγματική επίθεση, καθώς τα αποτελέσματά τους κατέδειξαν ελάχιστα ποσοστά επιτυχίας όταν επρόκειτο για email αλλαγής κωδικού. Αυτό που έκανε εντύπωση στους ερευνητές είναι ότι δεν υπήρχε σημαντική διαφορά ανάμεσα στις δύο διαφορετικές ηλικιακές ομάδες, 12-14 και 15-17, δείχνοντας ότι η ανάγκη κατάλληλης εκπαίδευσης κρίνεται επιτακτική σε όλες τις τάξεις της δευτεροβάθμιας εκπαίδευσης. Το μόνο θετικό σημείο στην έρευνα είναι ότι οι μαθητές, με βάση τις απαντήσεις τους, τείνουν να αγνοούν μηνύματα για τα οποία δεν ήταν σίγουροι. Η υπερβολική όμως αυτοπεποίθηση που κατέδειξαν για τις ικανότητές τους δείχνει ότι σε πραγματικές καταστάσεις θα ήταν ανίκανοι να προστατεύσουν τους εαυτούς τους (Nicholson, και συν., 2020, σσ. 144-147).

Με την έρευνα τους οι Lastdrager, Carvajal Gallardo, Hartel, και Junger κατέλειξαν και αυτοί στο συμπέρασμα ότι η ανάγκη των μαθητών να κατονοήσουν τους κινδύνους που έρχονται με τη χρήση του διαδικτύου είναι μεγάλη. Επιπλέον, έδειξαν ότι σε αρκετές περιπτώσεις τα παιδιά προσπαθούν να ενημερωθούν μόνο τους, κάτι το οποίο όμως οδηγεί σε ανεπαρκή έως μηδαμινά αποτελέσματα, χωρίς τη συστηματική εκπαίδευση που παρέχει το σχολείο. Στο πείραμά τους, οι μισοί μαθητές είχαν ήδη λάβει ενημέρωση, ενώ οι μισοί όχι. Οι μαθητές που είχαν περάσει από εκπαίδευση, κατά τη διάρκειά της διατύπωναν απορίες και περιέγραφαν περιστατικά, όπου κάποιος από το οικείο περιβάλλον τους είχε πέσει θύμα μιας τέτοιας επίθεσης, συνήθως οικονομικής φύσης, δείχνοντας και τη θέλησή τους να μάθουν περισσότερα. Ως αποτέλεσμα κατά τη διάρκεια του πειράματος τα παιδιά που είχαν λάβει ενημέρωση έδειξαν καλά αποτελέσματα. Δεν ισχύει όμως τα ίδιο και για τα άλλα μισά, καθώς μόνο ένα μικρό ποσοστό ήταν σε θέση να αναγνωρίσει ένα email ηλεκτρονικού ψαρέματος, με τη συντριπτική πλειοψηφία να απαντάει αρνητικά ή ότι δεν είναι σίγουροι, παρά το γεγονός ότι περίπου το 80% κατείχε προσωπικό email και περίπου το 26% προσωπικό λογαριασμό κοινωνικής δικτύωσης (Lastdrager, Carvajal Gallardo, Hartel, & Junger, 2017, σσ. 233-236, 237-238).

Η έρευνα του Alwanain επικεντρώθηκε στη χρήση της εφαρμογής WhatsApp και κατά πόσο μικρότεροι μαθητές μπορούν να αναγνωρίσουν μηνύματα ηλεκτρονικού ψαρέματος, και πώς αντιδρούν σε αυτά, με τη συμμετοχή των γονιών τους σε ρόλο παρατηρητή. Το πρώτο πείραμα περιελάμβανε την αποστολή ενός συνδέσμου που οδηγούσε σε ψεύτικη ιστοσελίδα στους μισούς 15 μαθητές, ενώ στους άλλους μισούς 15 στάλθηκε ο γνήσιος σύνδεσμος. Στο σύνολο μόνο 4 παιδιά από τα 15 πάτησαν τον ψεύτικο σύνδεσμο. Τα αγόρια απέρριψαν κατευθείαν τον αποστολέα, ενώ η τάση στα κορίτσια ήταν να ενημερώσουν τους γονείς τους. Στο δεύτερο πείραμα σε όλα τα παιδιά στάλθηκε ψεύτικος σύνδεσμος σε φαινομενικά αξιόπιστη ιστοσελίδα, η οποία περιείχε πληροφορίες σχετικά με το πρόγραμμα μαθημάτων. Μόνο 3 μαθητές, όλα αγόρια, πάτησαν το σύνδεσμο, δείχνοντας μείωση σε σχέση με το πρώτο πείραμα. Με το συγκεκριμένο φάνηκε η αξία και η ανάγκη ενημέρωσης σε σχέση με τους κινδύνους του διαδικτύου. Τα χαμηλά ποσοστά ‘θυμάτων’, κατόπιν μετέπειτα συνεντεύξεων με τους συμμετέχοντες μαθητές, ήταν αποτέλεσμα ύπαρξης κατάλληλης και αποτελεσματικής ενημέρωσης και εκπαίδευσης πάνω σε θέματα ασφάλειας και προστασίας, τα οποία ίσως δεν είχαν επιτευχθεί χωρίς αυτή. Με αυτόν τον τρόπο καταδεικνύονται τα αποτελέσματα της επίγνωσης, σε όσο το δυνατόν μικρότερη ηλικία (Alwanain, 2021, σσ. 131-132).

Η έρευνα του Frauenstein καταδεικνύει και αυτή με τη σειρά της την ανάγκη επαρκούς, τουλάχιστον, ενημέρωσης σχετικά με τις επιθέσεις ηλεκτρονικού ψαρέματος στα μέσα κοινωνικής δικτύωσης. Η αυξανόμενη χρήση τους έχει κάνει τους χρήστες τους ιδιαίτερα ευάλωτους καθώς οι phishers βρίσκουν ολοένα και περισσότερες ευκαιρίες αξιοποίησής τους για επιθέσεις. Τα αποτελέσματα της έρευνας, σε φοιτητές αυτή τη φορά, έδειξαν ότι οι συμμετέχοντες δεν κατέχουν επίγνωση των κινδύνων. Οι απαντήσεις τους κατέδειξαν ότι παρά τον κίνδυνο θα πατούσαν σε εικόνες ή βίντεο clickbait, ειδικά αν αφορούσε ένα θέμα που τους εξέπτατε το ενδιαφέρον. Επιπλέον, δεν ήταν σε θέση να διακρίνουν ποια ιστοσελίδα ήταν ασφαλής και ποια ενείχε κινδύνους, ενώ μια συντηρητική πλειοψηφία θα άνοιγε το επικίνδυνο επισυναπτόμενο έγγραφο, σε email που φαινομενικά στάλθηκε από το facebook. Ένα θετικό αποτέλεσμα ήταν ότι μία σημαντική πλειοψηφία δεν θα άνοιγε ή θα αγνοούσε ύποπτα email τραπεζών, δείχνοντας επίγνωση για επιθέσεις οικονομικής εξαπάτησης. Αλλά σχετικά με προειδοποιήσεις ασφαλείας, οι περισσότεροι φάνηκε να τις αγνοούν, προτιμώντας να επισκεφθούν την ιστοσελίδα, από την οποία το πρόγραμμα περιήγησής

τους ήθελε να τους προστατεύσει. Καταλήγοντας, οι επιθέσεις ηλεκτρονικού ψαρέματος έχουν γίνει πιο εκλεπτυσμένες και η ανάγκη ικανοποιητικής παρέμβασης, όσο πιο γρήγορα και σε νεαρότερες ηλικίες, τίθεται στο επίκεντρο (Frauenstein, 2018, σσ. 49-50, 62-63).

Από τις συγκεκριμένες έρευνες γίνεται ολοφάνερη η ανάγκη προγραμμάτων επιμόρφωσης και επίγνωσης για την ασφάλεια στο διαδίκτυο και το ηλεκτρονικό ψάρεμα. Τα παιδιά και οι έφηβοι βρίσκονται σε μια δύσκολη θέση, όσον αφορά την ασφάλειά τους. Ιδιαίτερα ενδιαφέρον είναι το γεγονός ότι καθηγητές και γονείς των μαθητών που συμμετείχαν σε αυτές τις έρευνες έδειξαν και αυτοί αυτήν την ανάγκη, όπως και την πρόθεση και θέλησή τους για συμμετοχή τους σε αυτά. Συγκεκριμένα η πλειοψηφία των καθηγητών ανέφερε τη σημασία εξειδικευμένης προσέγγισης από τα σχολεία, όπως και τις προθέσεις για ενσωμάτωση κατάλληλου υλικού στη διδασκαλία με στόχο μια πιο εκ βαθέων ανάλυση του θέματος. Αρκετοί μάλιστα, ήδη ενσωμάτωσαν πρακτικές, που είχαν υποδειχθεί κατά τη διάρκεια της έρευνας, στη διδασκαλία τους, βελτιώνοντας τόσο το μάθημα της πληροφορικής, όσο και τις στάσεις των μαθητών (Nicholson, και συν., 2020, σ. 147). Αυτό φάνηκε και στην έρευνα των Lastdrager, Carvajal Gallardo, Hartel, και Junger. Τόσο οι καθηγητές, όσο και οι γονείς αγκάλιασαν την συγκεκριμένη προσέγγιση και ανέφεραν πως το σχολείο θα πρέπει να περιλαμβάνει μαθήματα σχετικά με την ηλεκτρονική ασφάλεια στο πρόγραμμα σπουδών. Ακόμα πιο θετικό ήταν το γεγονός ότι και οι καθηγητές ήταν πρόθυμοι να λάβουν την κατάλληλη εκπαίδευση και οι ίδιοι, ούτως ώστε να είναι και αυτοί σε θέση να αντιλαμβάνονται και να αντιμετωπίζουν τις απειλές του διαδικτύου, αλλά και να μπορούν να μεταδώσουν αυτές τις γνώσεις στους μαθητές τους (Lastdrager, Carvajal Gallardo, Hartel, & Junger, 2017, σ. 238).

Στο επόμενο κομμάτι θα παρουσιαστούν κάποιες από τις στρατηγικές που έχουν ακολουθηθεί, το ρόλο των καθηγητών δευτεροβάθμιας εκπαίδευσης, όπως και κατά πόσο κρίνονται αποτελεσματικές στη μάχη απέναντι στις ηλεκτρονικές απειλές και το ηλεκτρονικό ψάρεμα.

1.6 Στρατηγικές επιμόρφωσης και επίγνωσης και ο ρόλος των καθηγητών της δευτεροβάθμιας εκπαίδευσης

Η εκπαίδευση σχετικά με την ηλεκτρονική ασφάλεια αποτελεί ένα ολοένα φλέγον θέμα και περιλαμβάνει δύο κρίσιμα και καίρια συστατικά, την αναγνώριση της ανάγκης λήψης σωστών προφυλάξεων και τη σωστή εκπαίδευση των μαθητών. Πλέον τα μαθήματα πληροφορικής έχουν ενταχθεί, αν όχι πλήρως τουλάχιστον σε ικανοποιητικό επίπεδο, στο πρόγραμμα σπουδών των σχολείων. Η σωστή εκπαίδευση, επομένως, σε θέματα ασφάλειας του διαδικτύου κρίνεται επιβεβλημένη μέσω αυτών. Η καλύτερη πρόληψη, άλλωστε, βρίσκεται στη σωστή και ολοκληρωμένη εκπαίδευση, σε όλες τις ηλικίες, και ακόμα περισσότερο στις μικρότερες (Venter, Blignaut, Renaud, & Venter, 2019, σ. 1). Δεν αρκεί όμως ένα απλό παραδοσιακό μάθημα για να μπορέσουν οι μαθητές να είναι σε θέση να αναγνωρίζουν και να αντιμετωπίζουν καταστάσεις, που μπορούν να βλάψουν τους εαυτούς τους και το άμεσο περιβάλλον τους. Ο τρόπος προσέγγισης των μαθητών θα πρέπει να λαμβάνει βιωματικά χαρακτηριστικά, έτσι ώστε, σε περίπτωση που βρεθούν σε ανάλογες καταστάσεις να μπορούν να αναγνωρίζουν τον κίνδυνο μπροστά τους.

Μια τέτοια στρατηγική, όπως περιγράφηκε προηγουμένως, είναι μέσω βιωματικών παιχνιδιών. Σύμφωνα με τους Weanquoi, Johnson, και Zhang, παραθέτοντας έρευνα των Patel και Luo (2017), οι περισσότεροι χρήστες που πέφτουν θύματα επιθέσεων ηλεκτρονικού ψαρέματος, δεν είχαν επίγνωση των κινδύνων αυτού, αλλά και πώς να το αναγνωρίζουν. Οι ερευνητές πιστεύουν ότι η χρήση παιχνιδιών σε όλα τα μαθήματα προτρέπουν τους μαθητές να συμμετέχουν ενεργά μέσα στο μάθημα, με αποτέλεσμα την καλύτερη απορρόφηση γνώσεων. Προτείνουν, λοιπόν, τη χρήση 2D παιχνιδιού, ονόματι Bird's Life, με τρία επίπεδα, με στόχο την ενημέρωση, μέσα από ένα οικείο και διασκεδαστικό περιβάλλον, των μαθητών για τους κινδύνους του ηλεκτρονικού ψαρέματος. Το πρώτο επίπεδο εισάγει τον μαθητή στην ιστορία του παιχνιδιού, μέσα από το δεύτερο επίπεδο δίνονται συμβουλές στους μαθητές για την αποφυγή του ηλεκτρονικού ψαρέματος και στο τρίτο και τελευταίο επίπεδο οι μαθητές καλούνται να αναγνωρίζουν μηνύματα ηλεκτρονικού ψαρέματος. Σημαντική κρίνεται η συλλογή δεδομένων πριν και μετά τη χρήση του παιχνιδιού, με στόχο να κριθεί η αποτελεσματικότητά του παιχνιδιού (Weanquoi, Johnson, & Zhang, 2018, pp. 1-2).

Τα αποτελέσματα που έλαβαν ήταν παραπάνω από ικανοποιητικά. Η συντριπτική πλειοψηφία των μαθητών έδειξε σημαντική βελτίωση στην αναγνώριση των κινδύνων, σύμφωνα με τα ερωτηματολόγια που τους διαμοιράστηκαν πριν και μετά το πέρας του παιχνιδιού. Ιδιαίτερα σημαντικό ήταν το γεγονός ότι πολλοί από τους μαθητές που δεν έδειξαν από την αρχή σημαντική βελτίωση, επανέλαβαν τις προσπάθειές τους, μέχρι να δουν καλά αποτελέσματα. Επιπλέον, η συμμετοχή των μαθητών στο παιχνίδι και την αξιολόγηση του παιχνιδιού, βοήθησε τους ερευνητές σε αισθητά καλύτερη αναδιαμόρφωση του παιχνιδιού, για μελλοντική πιο μαζική χρήση από μαθητές και εκπαιδευτικούς θεσμούς. Άλλο ένα θετικό στοιχείο είναι ότι δεν απαιτούνταν πρότερες δεξιότητες και εμπειρία στα ηλεκτρονικά παιχνίδια από τους μαθητές, με την απορρόφηση γνώσεων για την ηλεκτρονική ασφάλεια να είναι το ίδιο εύκολη για αυτούς που είχαν εμπειρία σε ηλεκτρονικά παιχνίδια και για αυτούς που δεν είχαν. Η ανάπτυξη, επομένως παιχνιδιών, στοχευμένων στην αναγνώριση ηλεκτρονικών απειλών και επιθέσεων ηλεκτρονικού ψαρέματος φαίνεται να αποτελεί μια βιώσιμη στρατηγική. Τα παιδιά μπορούν να μάθουν σε ένα ευχάριστο περιβάλλον, αποκτώντας τις απαραίτητες δεξιότητες για την ασφάλειά τους, αλλά και ηλεκτρονικές δεξιότητες γενικά (Weanquoi, Johnson, & Zhang, 2018).

Με έναν αντίστοιχο τρόπο οι Hanafi, Hanafia, Rokmana, Ibrahim, Zawawi και Rahimb πρότειναν τη χρήση του παιχνιδιού «Πάρε τη Σημαία!» (Capture the Flag), με στόχο να εισάγουν τους μαθητές στις έννοιες σχετικές με την ηλεκτρονική ασφάλεια και να κεντρίσουν το ενδιαφέρον τους σε αυτόν τον τομέα, μέσα από μια σειρά ερωτήσεων, οι ικανοποιητικές απαντήσεις των οποίων θα οδηγούσαν στην ανάδειξη του νικητή. Από τα δεδομένα που άντλησαν, η αποτελεσματικότητα μιας τέτοιας προσέγγισης είναι ικανοποιητικά υψηλή, και οι μαθητές έδειξαν να είναι σε θέση να κατανοούν τις έννοιες γύρω από το θέμα της ηλεκτρονικής ασφάλειας. Επιπλέον, βάσει των αποτελεσμάτων προτείνουν ότι να υπάρχουν απλώς μαθήματα STEM στο σχολείο, δεν επαρκεί για να κεντρίσει το ενδιαφέρον των παιδιών για μελλοντική ενασχόλησή τους με τον τομέα των επιστημών της πληροφορικής. Μεγαλύτερης σημασίας είναι η αύξηση της επίγνωσης των μαθητών, των εκπαιδευτικών και των γονιών τους για την ηλεκτρονική ασφάλεια, όπως και των επαγγελματικών διεξόδων που αυτός ο τομέας παρέχει. Η δευτεροβάθμια εκπαίδευση, επομένως, αποτελεί ένα ιδανικό περιβάλλον, λόγω του χρόνου διάρκειάς της αποτελεί ένα πλαίσιο στο οποίο, οι μαθητές θα μπορούσαν να ενημερωθούν πάνω στην ηλεκτρονική ασφάλεια, και ίσως να ενδιαφερθούν για την

ακαδημαϊκή και επαγγελματική ανάμειξή τους σε αυτό, αρκεί να υπάρχουν οι κατάλληλες εκπαιδευτικές δράσεις (Hanafi, και συν., 2021).

Η ένταξη εργαστηρίων δείχνει να έχει και αυτή θετικά για τους μαθητές αποτελέσματα, και μάλιστα σε πολλαπλά επίπεδα. Η μέθοδος που παρουσίασαν οι Pencheva, Hallett και Rashid βασίζεται στη δημιουργία τριών τέτοιων εργαστηρίων, διάρκειας μίας μέρας. Το πρώτο εργαστήριο (Cyber Teens or Are They?) εστιάζει στη σχέση των εφήβων με την τεχνολογία. Η πεποίθηση των εφήβων ότι δεν μπορούν να πάθουν κάτι κακό αποτελεί το στοιχείο που τους καθιστά και ευάλωτους σε ηλεκτρονικές επιθέσεις, ο στόχος επομένως ήταν να δείξουν στους μαθητές ότι δεν είναι τόσο προστατευμένοι, με τις γνώσεις που κατέχουν, όσο πιστεύουν. Η έλλειψη κατανόησης και από τους γονείς και τους εκπαιδευτικούς για τις καταστάσεις, στις οποίες μπορεί να βρεθεί ένας έφηβος έδειξε και την έλλειψη ενημέρωσης αυτών. Το δεύτερο εργαστήριο (Mind the Gap!) εστιασθηκε σε ερωτήσεις σχετικά με τα προβλήματα που μπορεί να δημιουργηθούν με τον υπερβολικό ενθουσιασμό ένταξης μαθημάτων για την ηλεκτρονική ασφάλεια. Η ανάγκη και προφανώς υπάρχει, αλλά για να εισαχθεί αυτό το μάθημα, πρέπει να ληφθεί υπόψη το υπάρχον πρόγραμμα σπουδών, όπως και οι αμφιβολίες όσων αναρωτούνται για τη χρησιμότητά του, και πώς αυτές θα απαντηθούν. Στο τρίτο εργαστήριο (What Should We Be Teaching and How Should We Be Teaching It?) ερωτήθηκαν οι ίδιοι οι συμμετέχοντες για το περιεχόμενο του μαθήματος. Οι απαντήσεις κινήθηκαν γύρω από τομείς της ηλεκτρονικής ασφάλειας, όπως οι ψηφιακές δεξιότητες, η προστασία συσκευών όπως και οι ευκαιρίες καριέρας, αλλά και αν θα πρέπει να ενταχθεί και στην πρωτοβάθμια εκπαίδευση. Μεγάλη σημασία δώθηκε στον τρόπο που το μάθημα θα πρέπει να διδάσκεται, όπως και του τρόπου ένταξής του στο πρόγραμμα σπουδών. Η χρήση σεναρίων και προσωμιώσεων έδειξε να είναι ο προτιμότερος τρόπος διδασκαλίας, ενώ η ένταξή τους στο πρόγραμμα σπουδών θα πρέπει να γίνει με ένα μεθοδικό και αποτελεσματικό τρόπο, λαμβάνοντας υπόψη και τη θέληση των καθηγητών, καθώς η έλλειψή της οδηγεί σε ανεπαρκή και αναποτελεσματική τελικώς διδασκαλία. Τα τελικά συμπεράσματα είναι ότι η ανάγκη ένταξης του μαθήματος υπάρχει, οι καθηγητές πρέπει να υποβοηθηθούν σε αυτό το έργο και το υλικό διδασκαλίας θα πρέπει να είναι κατανοητό και αποτελεσματικό (Pencheva, Hallett, & Rashid, 2020).

Παρατηρείται λοιπόν, ότι η χρήση παιχνιδιών, εργαστηρίων και προσομοιώσεων αποτελεί μια ενδεδειγμένη στρατηγική για την απόκτηση δεξιοτήτων σχετικές με την

ηλεκτρονική ασφάλεια και την αναγνώριση του ηλεκτρονικού ψαρέματος. Στον πυρήνα όμως της εκπαιδευτικής διαδικασίας είναι οι ίδιοι οι εκπαιδευτικοί, ούτως ώστε να είναι σε θέση να εφαρμόσουν αυτές τις στρατηγικές. Δυστυχώς όμως, στην πλειονότητα των περιπτώσεων, οι εκπαιδευτικοί βρίθουν ανάγκης επιμόρφωσης για το συγκεκριμένο ζήτημα. Σύμφωνα με έρευνα μόνο ένα μικρό ποσοστό των εκπαιδευτικών της δευτεροβάθμιας εκπαίδευσης, ερωτώμενοι για τις γνώσεις τους πάνω σε θέματα ηλεκτρονικής ασφάλειας απαντάει με αυτοπεποίθηση ότι γνωρίζει, ενώ η συντριπτική πλειοψηφία παραδέχεται ότι γνωρίζει ελάχιστα για το συγκεκριμένο θέμα. Σύμφωνα με την ίδια έρευνα οι καθηγητές, στην ερώτηση για τις υποθεματικές της ηλεκτρονικής ασφάλειας, που απασχολούν τους μαθητές και γίνεται λόγος κατά τη διάρκεια του μαθήματος, είναι το cyberbullying, η ρομποτική και η τεχνητή νοημοσύνη. Η ίδια η εκπαίδευση επομένως δημιουργεί ανάγκη για περαιτέρω εκπαίδευση και εμβάθυνση σε θέματα, τα οποία μπορεί να επηρεάσουν τη ζωή των μαθητών, όπως και θέματα που μπορεί να αφορούν το μέλλον τους. Αυτό καταδεικνύει ότι η δευτεροβάθμια εκπαίδευση έχει περιθώρια ανάπτυξης στον τομέα της πληροφορικής γενικότερα και της ηλεκτρονικής ασφάλειας ειδικότερα. Όμως οι μαθητές έχουν ελάχιστες γνώσεις και πληροφορίες για μια πιθανή ακαδημαϊκή και επαγγελματική εξέλιξη σε αυτόν τον τομέα, δημιουργώντας άλλη μια ανάγκη που πρέπει να καλυφθεί από τη δευτεροβάθμια εκπαίδευση. Για να μπορέσει άλλωστε να στελεχωθεί μελλοντικά ένας συνεχώς αυξανόμενος τομέας, οι βάσεις πρέπει να τεθούν από τη δευτεροβάθμια εκπαίδευση, χωρίς όμως την κατάρτιση των εκπαιδευτικών και τις ελλείψεις στα σχολεία οι μαθητές είναι δύσκολο να εκτεθούν (Cyber Innovation Center, 2020).

Τέλος, κρίνεται απαραίτητη και η ένταξη γυναικών και μειονοτήτων στο επαγγελματικό δυναμικό, απασχολημένο στον τομέα της ηλεκτρονικής ασφάλειας. Γενικώς αποτελεί έναν κλάδο που δεν έχει στελεχωθεί επαρκώς, παρά τις συνεχώς αυξανόμενες ανάγκες σε αυτό. Κατά αυτόν τον τρόπο η έλλειψη προσέγγισης σε κορίτσια, και άλλες κοινωνικές ομάδες, που θα μπορούσαν να έχουν τις κατάλληλες κλίσεις για την ανάπτυξη ψηφιακών δεξιοτήτων αποτελεί τροχοπέδη για τη βελτίωση της υπάρχουσας κατάστασης. Η δευτεροβάθμια εκπαίδευση είναι αυτή που μπορεί να λειτουργήσει με πολύ θετικό τρόπο στην αντιμετώπιση αυτού του προβλήματος. Η έλλειψη όμως μαθημάτων, έστω και επιλογής, που μπορεί να δημιουργήσουν το γνωστικό υπόβαθρο και την έξαψη της περιέργειας και του ενδιαφέροντος των

μαθητών λειτουργεί με κατασταλτικό τρόπο. Η πρόσληψη εκπαιδευτικών από ανάλογο κοινωνικό περιβάλλον, με υψηλές δεξιότητες ίσως μπορεί να είναι μία από τις λύσεις του προβλήματος, πέρα από την ένταξη και εισαγωγικών μαθημάτων, στην πληροφορική επιστήμη γενικώς. Αυτό πάντως που γίνεται αντιληπτό είναι ότι, όλοι οι μαθητές, ανεξαρτήτως, βρίθουν ενημέρωσης, επίγνωσης και σωστών κινήτρων (Mountrouidou, και συν., 2019).

2. Ερευνητικό Κομμάτι

2.1 Σκοπός και Στόχοι της Έρευνας

Μέσα από την επισκόπηση της βιβλιογραφίας παρατηρείται ότι η ασφάλεια στο διαδίκτυο είναι και παραμένει μία συνεχής πρόκληση. Η αυξανόμενη χρήση του διαδικτύου, η μαζική χρήση συσκευών όπως smartphones, tablets και ηλεκτρονικοί υπολογιστές, ειδικά από τα παιδιά και τους εφήβους, καθιστούν αυτήν την πρόκληση ένα μέρος της καθημερινότητας πολλών ανθρώπων. Οι επιθέσεις ηλεκτρονικού ψαρέματος, ως μέρος των κινδύνων ασφαλείας, συνεχώς αυξάνονται και εξελίσσονται μαζί με την εποχή τους. Αυτό καθιστά, ειδικά τα παιδιά και τους εφήβους, ένα ευάλωτο κοινό, στόχο αυτών των επιθέσεων, με αποτέλεσμα τα ίδια και οι γονείς τους να πέφτουν θύματα υπεξαίρεσης προσωπικών πληροφοριών, ταυτοτήτων και χρηματικών ποσών. Η ανάγκη επομένως επιμόρφωσης και προγραμμάτων επίγνωσης είναι πιο επιτακτική από ποτέ. Η δευτεροβάθμια εκπαίδευση θα μπορούσε να καλύψει αυτό το κενό επίγνωσης, με στοχευόμενα και εξειδικευμένα προγράμματα, όπως κατέδειξε και η βιβλιογραφία. Παιχνίδια, προσομοιώσεις με τη χρήση ηλεκτρονικών παιχνιδιών, εργαστήρια δεξιοτήτων μπορούν να αποτελέσουν χρήσιμα εργαλεία στα χέρια των εκπαιδευτικών. Δύο βασικά προβλήματα, όμως, παραμένουν, η έλλειψη κατάρτισης των εκπαιδευτικών και η έλλειψη παροχής ισχυρών κινήτρων στους μαθητές για μελλοντική επαγγελματική ενασχόληση με τον τομέα της ηλεκτρονικής ασφαλείας, τομέας ο οποίος, παρά τους αυξανόμενους κινδύνους, παραμένει υποστελεχωμένος. Αν αυτά τα δύο προβλήματα καταφέρουν να ξεπεραστούν, ο κίνδυνος δε θα εξαλειφθεί, αλλά τα παιδιά και οι έφηβοι θα είναι σε θέση να προστατεύουν τους εαυτούς τους.

Με βάση αυτά, στο επόμενο κομμάτι της εργασίας θα γίνει προσπάθεια να αναδειχθεί η επίγνωση των Ελλήνων καθηγητών και μαθητών της δευτεροβάθμιας εκπαίδευσης πάνω στα θέματα της ηλεκτρονικής ασφαλείας και των κινδύνων του ηλεκτρονικού ψαρέματος, όπως και οι απόψεις τους σχετικά με την αποτελεσματικότητα του μαθήματος της πληροφορικής ή την ένταξη νέων μαθημάτων στο πρόγραμμα σπουδών.

2.2 Μέθοδος

2.2.1 Δείγμα και Ερευνητικά Εργαλεία

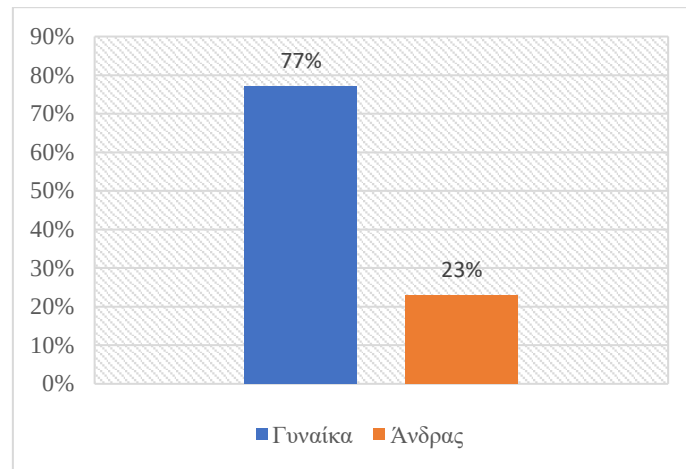
Για τις ανάγκες της παρούσας εργασίας προετοιμάστηκαν από την ερευνήτρια δύο ερωτηματολόγια, με σκοπό τη μέτρηση του επιπέδου επίγνωσης για το ηλεκτρονικό ψάρεμα. Ένας αριθμός ερωτήσεων προσαρμόστηκε από το quiz «Ξέρεις πώς να προστατευτείς από τις απάτες στο διαδίκτυο;», της ιστοσελίδας <https://saferinternet4kids.gr/>. Η συγκεκριμένη ιστοσελίδα δημιουργήθηκε από το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, υπό την αιγίδα του Ιδρύματος Τεχνολογίας και Έρευνας και πιο συγκεκριμένα του Ινστιτούτου Πληροφορικής. Παρέχει επίσης πολυμεσικό ενημερωτικό υλικό για γονείς, μαθητές και εκπαιδευτικούς για την ασφαλή χρήση του διαδικτύου, το οποίο είναι εγκεκριμένο από το Υπουργείο Παιδείας και Θρησκευμάτων.

Οι ερωτήσεις, λοιπόν, πέραν από τις ερωτήσεις δημογραφικών στοιχείων, και επαγγελματικών για τους εκπαιδευτικούς, εστιάζουν στην καταγραφή των υπάρχουσών γνώσεων των καθηγητών και των μαθητών πάνω στα θέματα ηλεκτρονικής ασφάλειας, στις τυχούσες προσωπικές εμπειρίες και στις προσωπικές απόψεις για την αποτελεσματικότητα του μαθήματος της πληροφορικής, στο υπάρχον πρόγραμμα σπουδών απέναντι σε αυτό το θέμα. Μέσα από αυτές, θα προσπαθήσει να διευκρινιστεί το κατά πόσο οι εκπαιδευτικοί και οι μαθητές είναι σε θέση να αναγνωρίζουν και να μην πέφτουν θύματα καθημερινών ηλεκτρονικών απειλών. Το ένα ερωτηματολόγιο διαμοιράστηκε σε εκπαιδευτικούς της δευτεροβάθμιας εκπαίδευσης και το δεύτερο σε μαθητές γυμνασίου και λυκείου.

Ο διαμοιρασμός των ερωτηματολογίων έγινε μέσω της πλατφόρμας Google Forms και η ανάλυση των δεδομένων έγινε με τη χρήση του προγράμματος Microsoft Excel. Τα ερωτηματολόγια διαμοιράστηκαν εκτός της σχολικής μονάδας, μέσω απευθείας email στους καθηγητές, ή με email σε γονείς και κηδεμόνες των μαθητών.

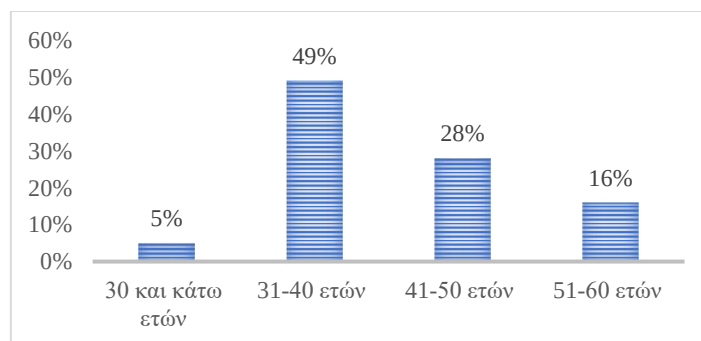
Το τελικό δείγμα αποτελείται από 100 εκπαιδευτικούς και 107 μαθητές. Οι απαντήσεις που ελήφθησαν έδειξαν την τάση έλλειψης επίγνωσης από τους μαθητές για το συγκεκριμένο θέμα, όπως και την ανάγκη ένταξης ξεχωριστού μαθήματος για θέματα ηλεκτρονικής προστασίας στα σχολεία της δευτεροβάθμιας εκπαίδευσης.

Όσον αφορά τα δημογραφικά στοιχεία του δείγματος των εκπαιδευτικών, το 77% των ερωτηθέντων εκπαιδευτικών ήταν γυναίκες και το 23% άνδρες (βλ. εικόνα 1).



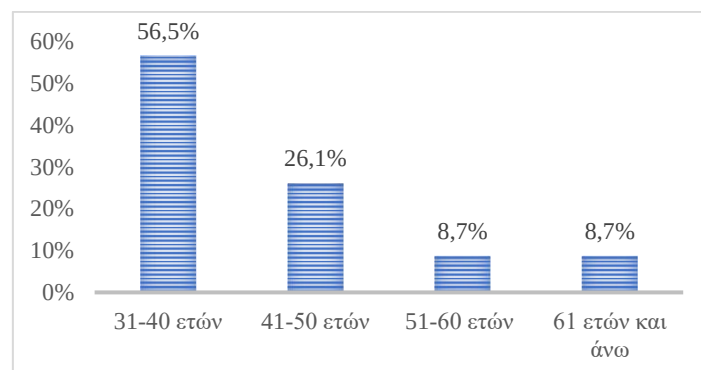
Εικόνα 1: Φύλο

Οι ηλικίες των γυναικών κυμαίνονταν από κάτω των 30 ετών μέχρι 60, με το 5,19% να είναι μικρότερες των 30, το 49,35% ηλικιών 31-40, το 28,57% ηλικιών 41-50 και 16,88% ηλικιών 51-60 (βλ. εικόνα 2).



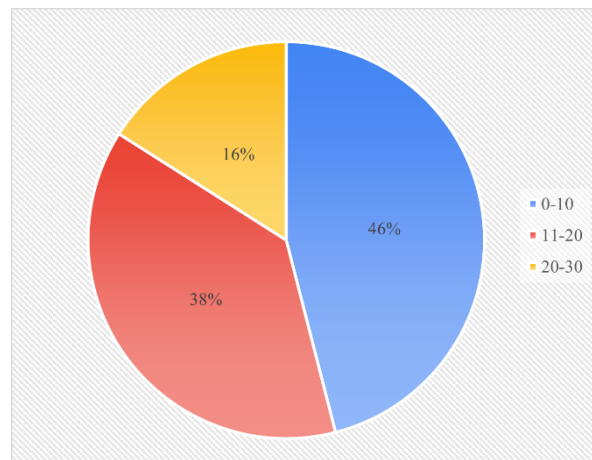
Εικόνα 2: Ηλικίες Γυναικών

Οι ηλικίες των ανδρών κυμάνθηκαν από τα 31 έως πάνω από τα 61 έτη, με το 56,52% να είναι 31-40 ετών, το 26,09% 41-50 ετών, το 8,7% 51-60 ετών και το 8,7% 61 ετών και άνω (βλ. εικόνα 3).



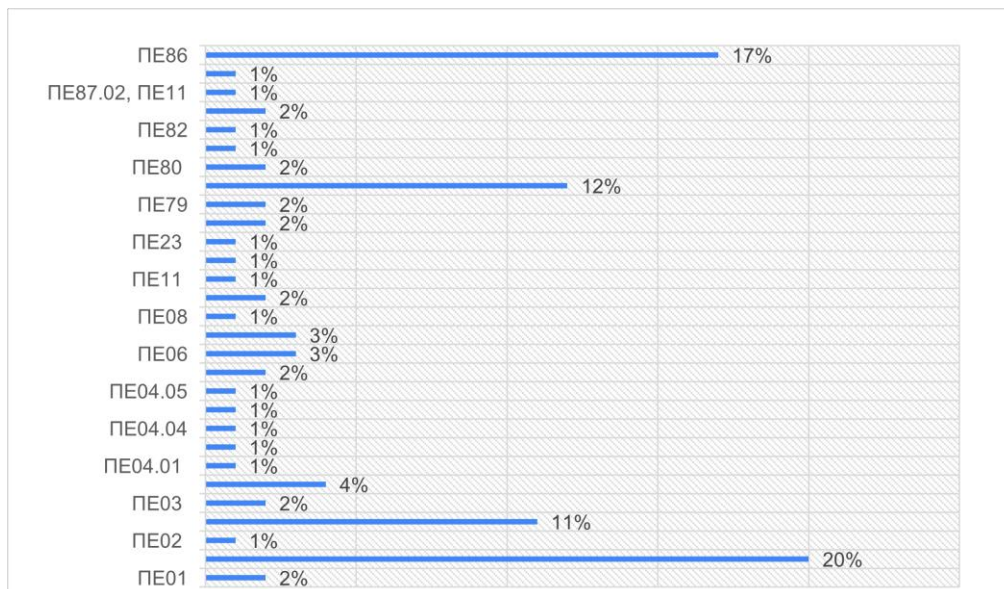
Εικόνα 3: Ηλικίες Ανδρών

Η πλειοψηφία των εκπαιδευτικών είχαν μικρή εκπαιδευτική εμπειρία, με ποσοστό 46%, ενώ το 38% είχε διδακτική εμπειρία 11-20 έτη και το 16% 20-30 έτη (βλ. εικόνα 4).



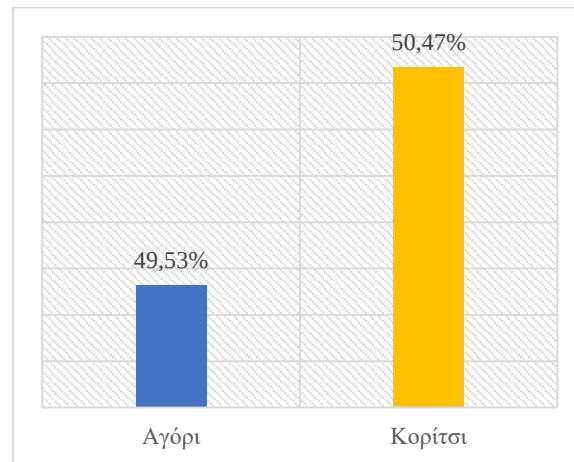
Εικόνα 4: Διδακτική Εμπειρία

Οι καθηγητές που απάντησαν στο ερωτηματολόγιο ήταν διαφορετικών ειδικοτήτων, με την πλειοψηφία των απαντήσεων να προέρχεται από φιλόλογους (ΠΕ02) με ποσοστό 20%, καθηγητές πληροφορικής (ΠΕ86) με ποσοστό 17%, οικονομολόγους (ΠΕ80) με ποσοστό 12% και μαθηματικούς (ΠΕ03) με ποσοστό 11%, ενώ οι υπόλοιπες ειδικότητες κυμαίνονταν σε ποσοστά από 1% έως 4% (βλ. εικόνα 5).



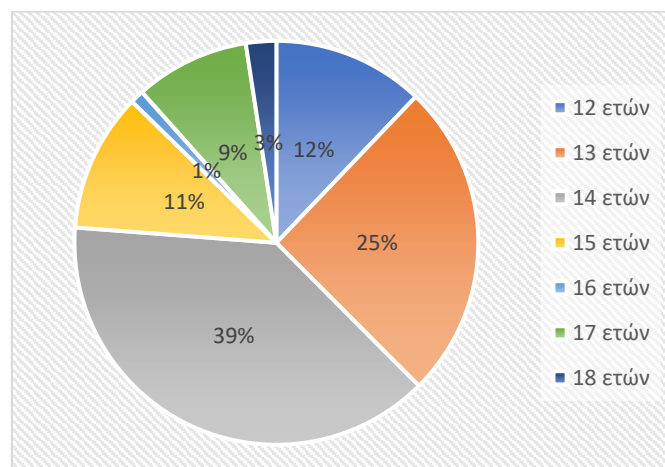
Εικόνα 5: Ειδικότητες

Αναφορικά με τους μαθητές, το 50,47% των ερωτηθέντων ήταν κορίτσια και το 49,53% αγόρια (βλ. εικόνα 6).



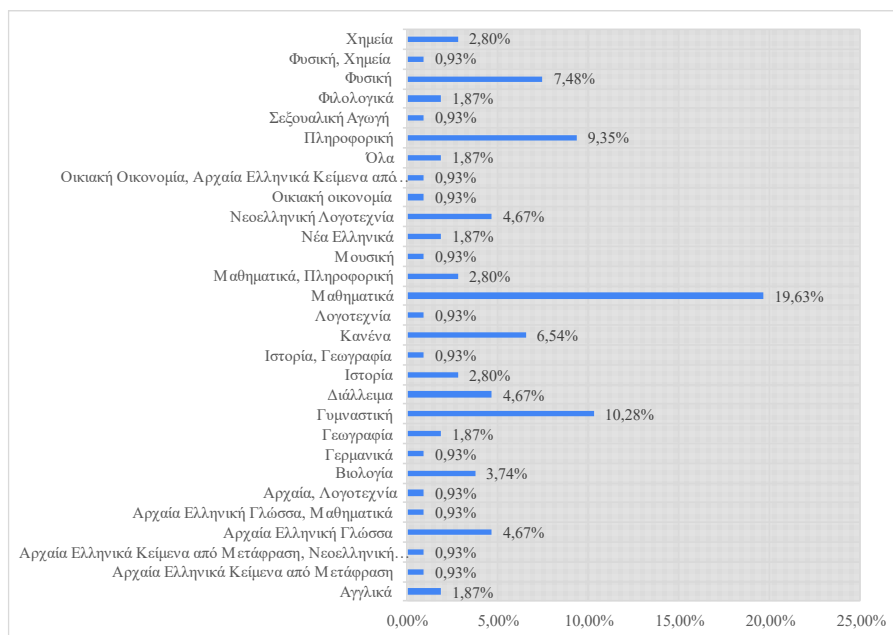
Εικόνα 6: Φύλο Μαθητών

Οι ηλικίες τους κυμαίνονται από 12 έως 18 ετών. Συγκεκριμένα το 12,13% ήταν μαθητές ηλικίας 12 ετών, το 25,4% ηλικίας 13 ετών, το 38,68% ηλικίας 14 ετών, το 11,12% ηλικίας 15 ετών, το 1,08% ηλικίας 16 ετών, το 9,16% ηλικίας 17 ετών και το 2,43% ηλικίας 18 ετών (βλ. εικόνα 7).



Εικόνα 7: Ηλικίες Μαθητών

Ανάμεσα στα αγαπημένα μαθήματα των μαθητών συγκαταλέγονται τα μαθηματικά, η πληροφορική, η γυμναστική και η φυσική με ποσοστά 19,63%, 9,35%, 10,28% και 7,48% (βλ. εικόνα 8).



Εικόνα 8: Ποιο είναι το αγαπημένο σου μάθημα;

Στο επόμενο κομμάτι της συγκεκριμένης ενότητας κρίνεται χρήσιμο να παρουσιαστούν τα ερωτηματολόγια που έχουν δοθεί σε καθηγητές και μαθητές της δευτεροβάθμιας εκπαίδευσης, πριν γίνει η παρουσίαση και η ανάλυση των αποτελεσμάτων τους.

2.2.2 Ερωτηματολόγιο Εκπαιδευτικών

1. Φύλο

- ☐ Άνδρας
- ☐ Γυναίκα

2. Ηλικία

- ☐ 30 και κάτω
- ☐ 31-40
- ☐ 41-50
- ☐ 51-60
- ☐ 61 και άνω

3. Διδακτική Εμπειρία (σε χρόνια)

- ☐ 0-10
- ☐ 11-20
- ☐ 20-30

4. Ειδικότητα: _____

5. Ποια είναι η εξοικείωση σου με την Πληροφορική;

- ☐ Επαγγελματική χρήση.
- ☐ Βασική χρήση.
- ☐ Προσωπική χρήση.
- ☐ Καμία χρήση.

6. Πόσες ώρες την ημέρα χρησιμοποιείτε το διαδίκτυο;

- ☐ 0-1
- ☐ 1-2
- ☐ 2-3
- ☐ Πάνω από 3

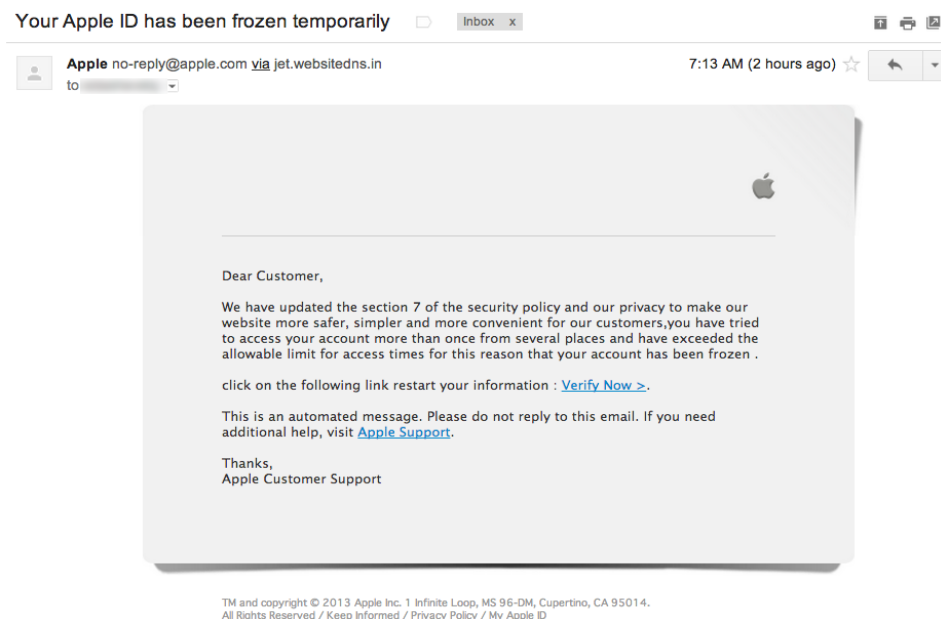
7. Σου έχει σταλεί, ή έχει πέσει ποτέ στην αντίληψή σου, email που να σου ζητάει προσωπικά δεδομένα;

- ☐ Ναι
- ☐ Όχι

8. Γνωρίζεις τι είναι το τι είναι το Phising;

- ☐ Παιδικό παιχνίδι για tablet;
- ☐ Εφαρμογή για κινητά;
- ☐ Ηλεκτρονική επίθεση με σκοπό ανάκτησης προσωπικών πληροφοριών;
- ☐ Εταιρία ανάπτυξης λογισμικού;
- ☐ Δεν γνωρίζω.

9. Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;



<https://news.softpedia.com/news/Your-App i>

- ☐ Θα ακολουθούσα τον σύνδεσμο (Verify Now>>)
- ☐ Θα απαντούσα στο μήνυμα
- ☐ Θα επέλεγα το «Φιλτράρισμα τέτοιων μηνυμάτων»
- ☐ Θα διέγραφα το μήνυμα
- ☐ Θα επέλεγα την «Αναφορά ως ανεπιθύμητου μηνύματος»

- ☐ Θα επέλεγα την «Αναφορά ηλεκτρονικού ‘ψαρέματος’»
- ☐ Θα αγνοούσα το μήνυμα

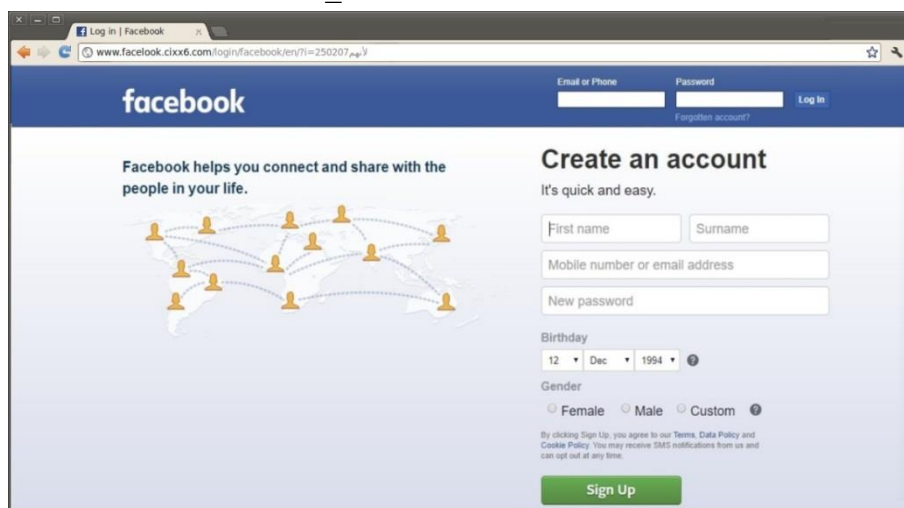
10. Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;

☐ 1. 

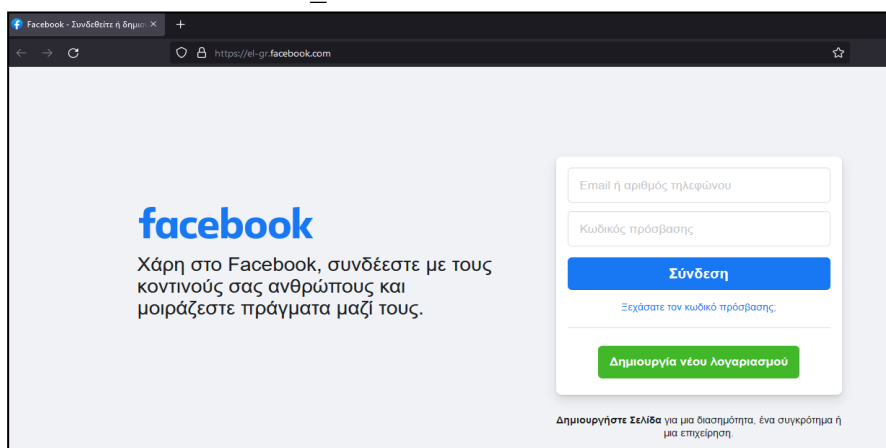
☐ 2. 

11. Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;

☐ Εικόνα_1



☐ Εικόνα_2



<https://el-gr.facebook.com/i>

12. Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;

- ☐ Γράμματα μικρά και κεφαλαία, σύμβολα και αριθμούς
- ☐ Όσο το δυνατόν πιο πολλούς χαρακτήρες
- ☐ Το όνομά μας ή/και την ημερομηνία γέννησής μας
- ☐ Ακολουθία από τουλάχιστον 8 τυχαίους χαρακτήρες

13. Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;

- ☐ 123456
- ☐ Helen
- ☐ F001_@14p
- ☐ Nikos2003

14. Κατά τη διάρκεια του μαθήματος έχεις μιλήσει ποτέ με τους μαθητές για τους κινδύνους του διαδικτύου;

- ☐ Ναι
- ☐ Όχι

15. Οι μαθητές σου έχουν διατυπώσει απορίες για την ασφάλεια στο διαδίκτυο κατά τη διάρκεια του μαθήματος;

- ☐ Ναι
- ☐ Όχι

16. Αν ναι, με αφορμή γεγονότα από την επικαιρότητα ή δικούς τους προβληματισμούς/εμπειρίες;

- ☐ με αφορμή γεγονότα από την επικαιρότητα
- ☐ με αφορμή δικούς τους προβληματισμούς/εμπειρίες
- ☐ και τα δύο

17. Έχουν υπάρξει περιπτώσεις στο σχολείο που υπηρετείς, όπου μαθητής έχει πέσει θύμα κάποιας μορφής ηλεκτρονικής απειλής;

- ☐ Ναι
- ☐ Όχι
- ☐ Δεν γνωρίζω

18. Για την αντιμετώπιση ηλεκτρονικών κινδύνων πιστεύεις ότι επαρκεί το μάθημα της πληροφορικής;

☐ Ναι

☐ Όχι

19. Αν όχι, τι πιστεύεις ότι θα ήταν αποτελεσματικότερο;

☐ Σεμινάριο

☐ Ξεχωριστό μάθημα στο πρόγραμμα σπουδών

☐ Ως ενότητα στα πλαίσια των εργαστηρίων δεξιοτήτων

☐ Άλλο: _____

2.2.3 Ερωτηματολόγιο Μαθητών

1. Φύλο

- ☐ Αγόρι
- ☐ Κορίτσι

2. Ηλικία

- ☐ 12
- ☐ 13
- ☐ 14
- ☐ 15
- ☐ 16
- ☐ 17
- ☐ 18

3. Ποιο είναι το αγαπημένο σου μάθημα; _____

4. Διαθέτεις e-mail;

- ☐ Ναι
- ☐ Όχι

5. Έχεις δημιουργήσει λογαριασμό κοινωνικής δικτύωσης (facebook, Instagram κλπ.);

- ☐ Ναι
- ☐ Όχι

6. Πόσες ώρες την ημέρα χρησιμοποιείς το διαδίκτυο;

- ☐ 0-1
- ☐ 1-2
- ☐ 2-3
- ☐ Πάνω από 3

7. Σου έχει σταλεί, ή έχει πέσει ποτέ στην αντίληψή σου, email που να σου ζητάει προσωπικά δεδομένα, δικά σου ή των γονιών σου;
- ☐ Ναι
 - ☐ Όχι
8. Αν, ναι, πώς αντέδρασες;
- ☐ Άνοιξα το email, χωρίς να απαντήσω
 - ☐ Άνοιξα το email και απάντησα
 - ☐ Διέγραψα κατευθείαν το email
 - ☐ Ενημέρωσα τους γονείς μου
9. Γνωρίζεις τι είναι το τι είναι το Phising;
- ☐ Παιδικό παιχνίδι για tablet;
 - ☐ Εφαρμογή για κινητά;
 - ☐ Ηλεκτρονική επίθεση με σκοπό ανάκτησης προσωπικών πληροφοριών;
 - ☐ Εταιρία ανάπτυξης λογισμικού;
 - ☐ Δεν γνωρίζω.
10. Λαμβάνεις email από το αγαπημένο σου site ζητώντας να τους προωθήσεις τον κωδικό σου για να κάνουν κάποιες τροποποιήσεις στο λογαριασμό σου. Τι κάνεις;
- ☐ Τους στέλνεις τον κωδικό σου
 - ☐ Αγνοείς το email και το διαγράφεις
 - ☐ Τους στέλνεις το τηλέφωνό σου για να επικοινωνήσετε και να τους δώσεις τον κωδικό σου
 - ☐ Απαντάς το email ζητώντας περισσότερες πληροφορίες
11. Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;

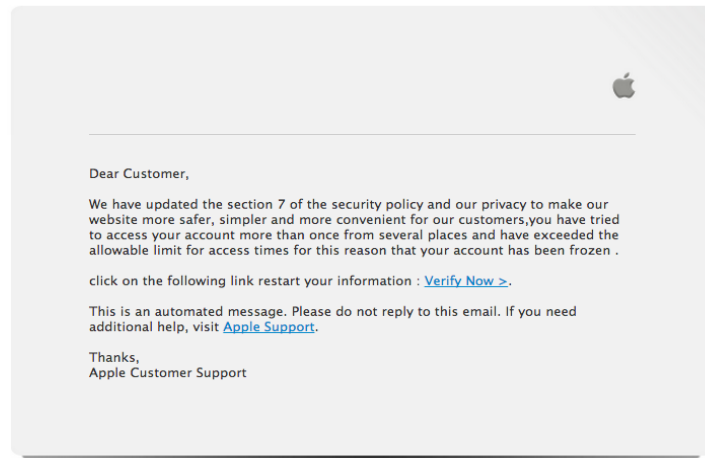
Your Apple ID has been frozen temporarily

Inbox x



Apple no-reply@apple.com via jet.websitedns.in
to [redacted]

7:13 AM (2 hours ago) ☆ ↩



TM and copyright © 2013 Apple Inc. 1 Infinite Loop, MS 96-DM, Cupertino, CA 95014.
All Rights Reserved / Keep Informed / Privacy Policy / My Apple ID

[https://news.softpedia.com/news/Your-App ii](https://news.softpedia.com/news/Your-App-ii)

- ☐ Θα ακολουθούσα τον σύνδεσμο (Verify Now>>)
- ☐ Θα απαντούσα στο μήνυμα
- ☐ Θα επέλεγα το «Φιλτράρισμα τέτοιων μηνυμάτων»
- ☐ Θα διέγραφα το μήνυμα
- ☐ Θα επέλεγα την «Αναφορά ως ανεπιθύμητου μηνύματος»
- ☐ Θα επέλεγα την «Αναφορά ηλεκτρονικού 'ψαρέματος'»
- ☐ Θα αγνοούσα το μήνυμα

12. Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;

- ☐ 1. 
- ☐ 2. 

13. Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;
(Σύντομη απάντηση) _____

□ Εικόνα_1

The screenshot shows the Facebook homepage with the login and sign-up options. The login section at the top right has fields for 'Email or Phone' and 'Password', with a 'Log In' button and a link for 'Forgotten account?'. Below this, the 'Create an account' section is titled 'It's quick and easy.' and includes fields for 'First name', 'Surname', 'Mobile number or email address', and 'New password'. It also has a 'Birthday' selector (month and year) and a 'Gender' selector (Female, Male, Custom). A 'Sign Up' button is at the bottom right. On the left, there is a graphic with the text 'Facebook helps you connect and share with the people in your life.' and a network diagram of people icons.

□ Εικόνα_2

The screenshot shows the Facebook homepage in Greek. The login section on the right has fields for 'Email ή αριθμός τηλεφώνου' and 'Κωδικός πρόσβασης', with a blue 'Σύνδεση' button and a link 'Ξεχάσατε τον κωδικό πρόσβασης;'. Below this is a green 'Δημιουργία νέου λογαριασμού' button. At the bottom, there is a note: 'Δημιουργήστε Σελίδα για μια διασημότητα, ένα συγκρότημα ή μια επιχείρηση.' On the left, the Facebook logo is followed by the text 'Χάρη στο Facebook, συνδέεστε με τους κοντινούς σας ανθρώπους και μοιράζεστε πράγματα μαζί τους.'

<https://el-gr.facebook.com/> ii

14. Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;

- ☐ Γράμματα μικρά και κεφαλαία, σύμβολα και αριθμούς
- ☐ Όσο το δυνατόν πιο πολλούς χαρακτήρες
- ☐ Το όνομά μας ή/και την ημερομηνία γέννησής μας
- ☐ Ακολουθία από τουλάχιστον 8 τυχαίους χαρακτήρες

15. Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;

- ☐ 123456
- ☐ Helen
- ☐ F001_@14p
- ☐ Nikos2003

16. Πιστεύεις, με όσα έχεις μάθει στο σχολείο, ότι μπορείς να αναγνωρίσεις ηλεκτρονικές απειλές;

- ☐ Ναι
- ☐ Όχι

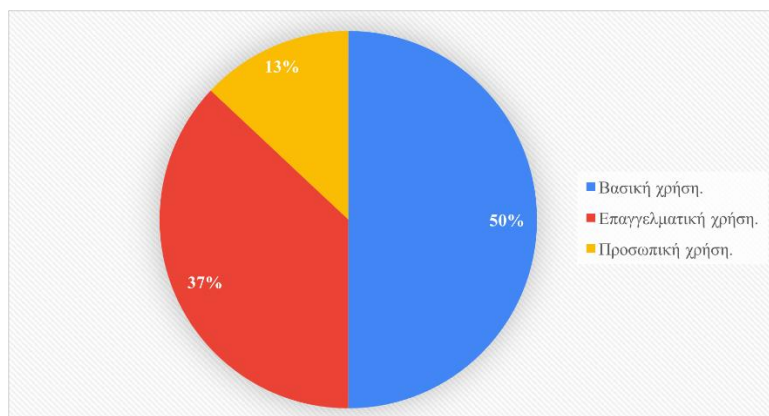
17. Θα ήθελες να γίνονται περισσότερα μαθήματα στο σχολείο για την ασφάλεια στο Διαδίκτυο;

- ☐ Ναι
- ☐ Όχι

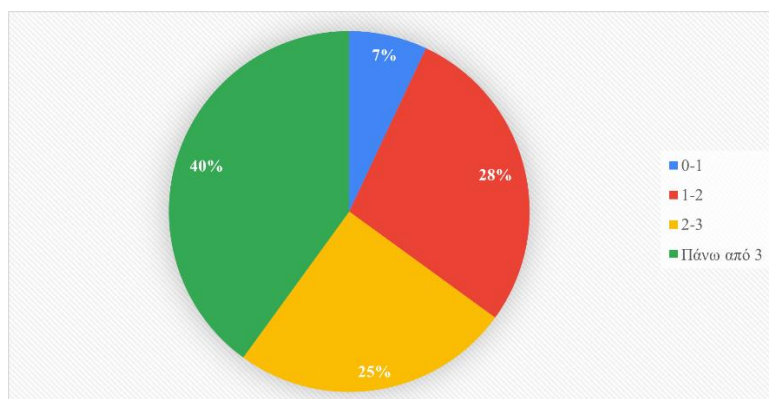
3. Ανάλυση Δεδομένων και Παρουσίαση Αποτελεσμάτων

3.1 Στάσεις και απόψεις εκπαιδευτικών

Το 50% των εκπαιδευτικών απάντησε ότι η εξοικείωσή τους με την πληροφορική ήταν βασική (βλ. εικόνα 9), με το 40% να χρησιμοποιεί το διαδίκτυο πάνω από τρεις ώρες την ημέρα (βλ. εικόνα 10). Αυτό δείχνει ότι οι υπολογιστές και το διαδίκτυο αποτελούν μια βασική συνιστώσα στην καθημερινότητα ενός εκπαιδευτικού. Η εξ αποστάσεως διδασκαλία, άλλωστε, των τελευταίων ετών είναι κάτι που κατέδειξε την ανάγκη εξοικείωσης των εκπαιδευτικών με αυτά, οπότε και η μέτρηση της επίγνωσης των κινδύνων και στους εκπαιδευτικούς κρίθηκε αναγκαία.



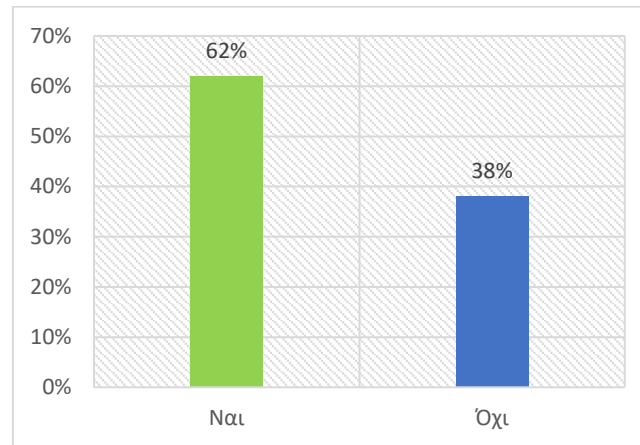
Εικόνα 9: Ποια είναι η εξοικείωσή σου με την Πληροφορική;



Εικόνα 10: Πόσες ώρες την ημέρα χρησιμοποιείς το διαδίκτυο;

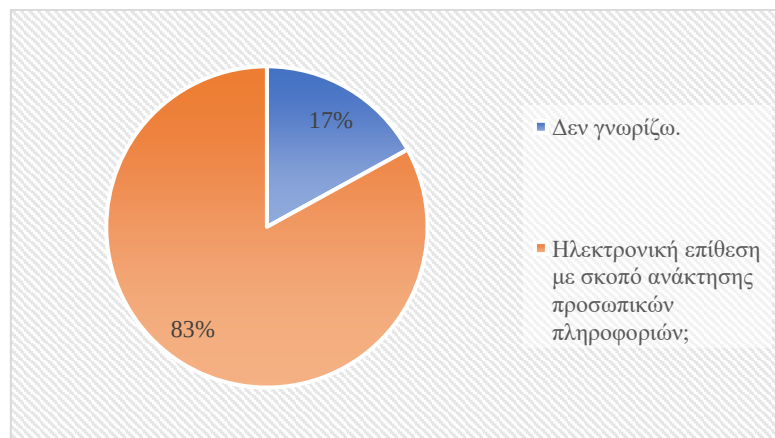
Περνώντας λοιπόν, στις επόμενες ερωτήσεις που μετρούν το βαθμό επίγνωσης των καθηγητών σχετικά με τους κινδύνους της ηλεκτρονικής ασφάλειας, όπως και τις απόψεις του σχετικά με την αποτελεσματικότητα του υπάρχοντος προγράμματος σπουδών για την αντιμετώπισή τους, παρατηρούμε τα εξής.

Πρώτα από όλα, στην ερώτηση 7, «Σου έχει σταλεί, ή έχει πέσει ποτέ στην αντίληψή σου, email που να σου ζητάει προσωπικά δεδομένα», βλέπουμε ότι 62% έχει απαντήσει θετικά (βλ. εικόνα 11), δείχνοντας κατά αυτόν τον τρόπο τον συνεχόμενο και καθημερινό κίνδυνο του ηλεκτρονικού ψαρέματος.



Εικόνα 11: Σου έχει σταλεί, ή έχει πέσει ποτέ στην αντίληψή σου, email που να σου ζητάει προσωπικά δεδομένα;

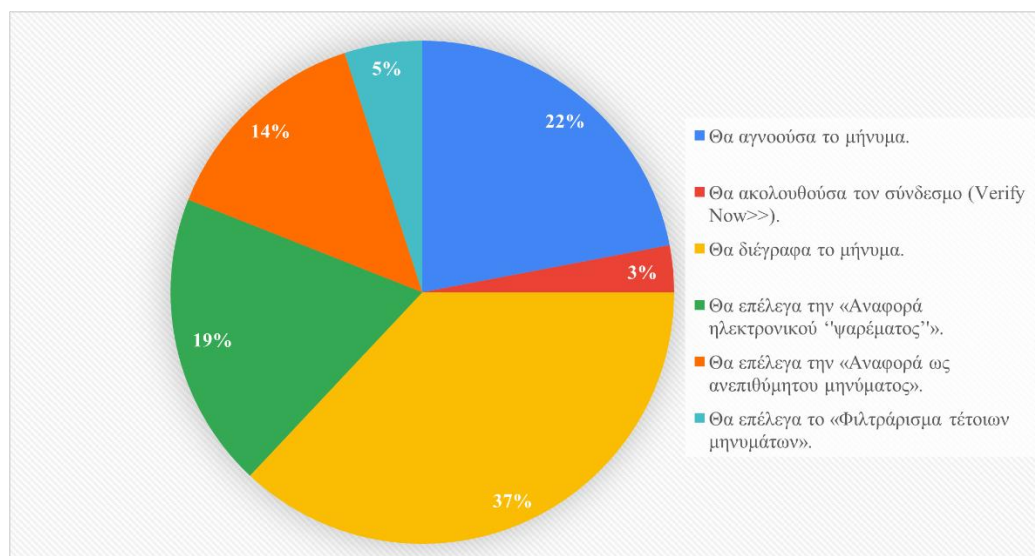
Ένα από τα θετικά αποτελέσματα είναι ότι μόλις το 17% απάντησε αρνητικά στην ερώτηση 8, «Γνωρίζεις τι είναι το Phishing» (βλ. εικόνα 12).



Εικόνα 12: Γνωρίζεις τι είναι το Phishing;

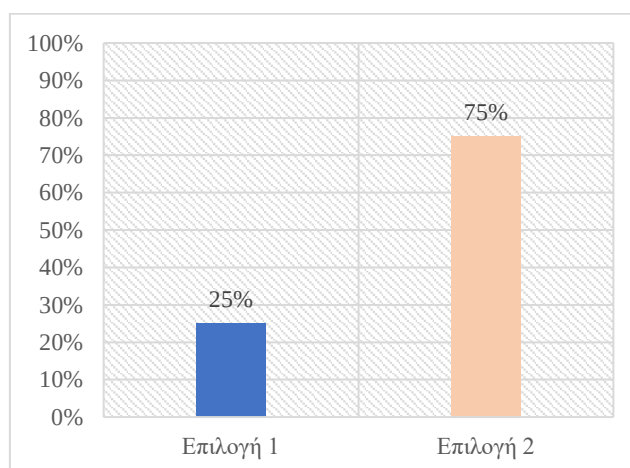
Επιπλέον το 3% επέλεξε την απάντηση «Θα ακολουθούσα τον σύνδεσμο (Verify Now>>)» στην ερώτηση 9 «Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;», με το 22% να επιλέγει την απάντηση «Θα αγνοούσα το μήνυμα», το 37% την απάντηση «Θα διέγραφα το μήνυμα», το 19% την απάντηση «Θα επέλεγα την «Αναφορά ηλεκτρονικού ψαρέματος», το 14% την

απάντηση «Θα επέλεγα την Αναφορά ως ανεπιθύμητου μηνύματος» και το 5% την απάντηση «Θα επέλεγα το Φιλτράρισμα τέτοιων μηνυμάτων» (βλ. εικόνα 13).



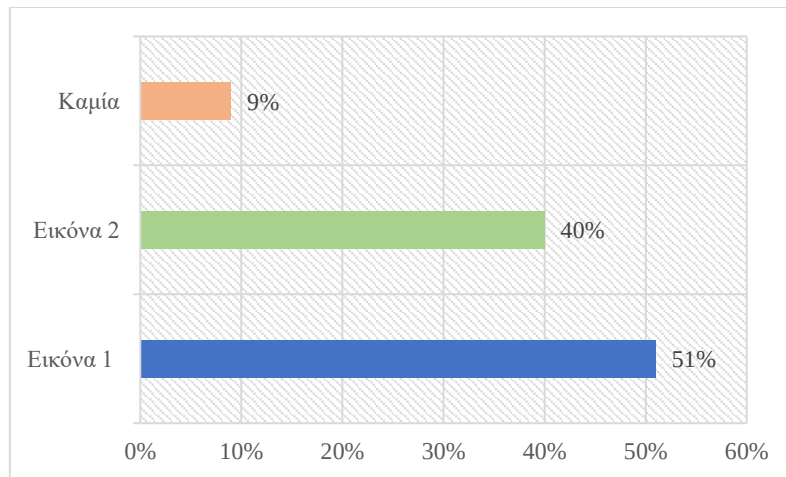
Εικόνα 13: Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;

Όσον αφορά την αναγνώριση ύποπτων ιστοσελίδων οι απαντήσεις έδειξαν ότι το 75% απάντησε σωστά στην ερώτηση 10, «Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;» (βλ. εικόνα 14).



Εικόνα 14: Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;

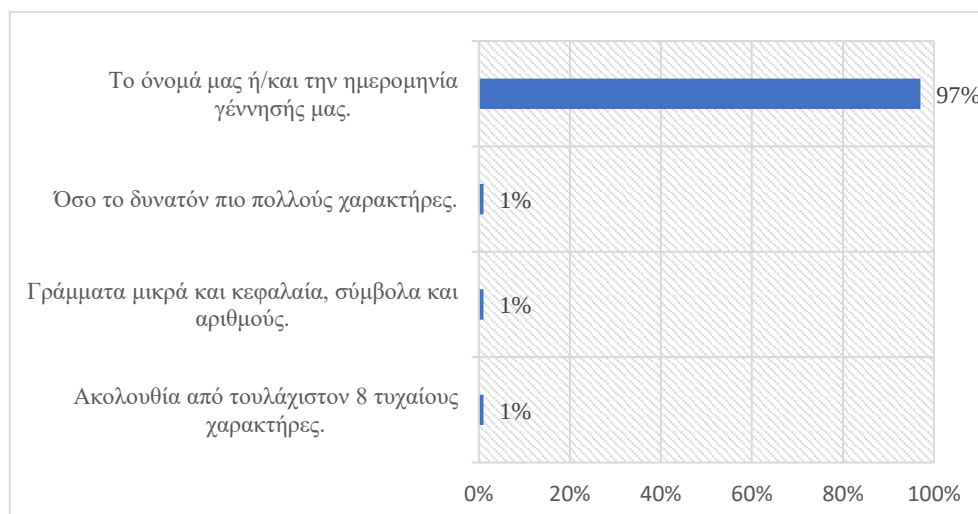
Αν και μόλις το 51% μπόρεσε να αναγνωρίσει την ύποπτη ιστοσελίδα στην ερώτηση 11, «Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;», με το 40% να επιλέγει την εικόνα 2 ως την ύποπτη και το 9% να μη βρίσκει καμία ως ύποπτη (βλ. εικόνα 15).



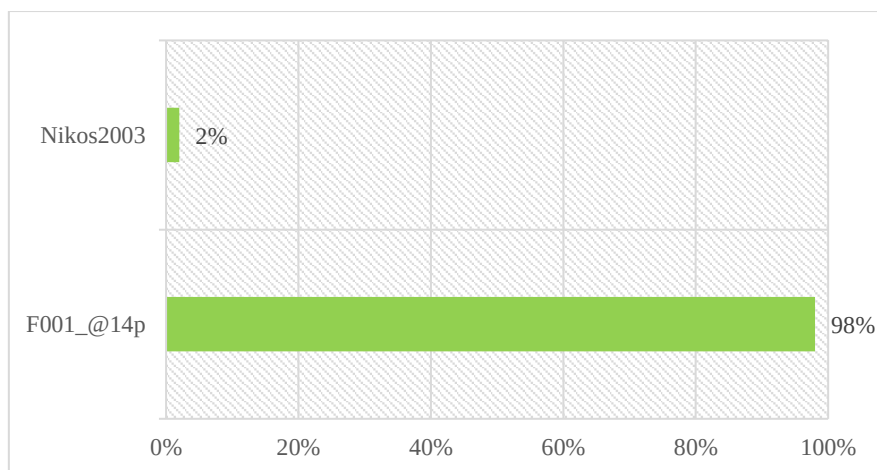
Εικόνα 15: Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;

Ο τρόπος αναγνώρισης της ύποπτης ιστοσελίδας, μέσω των σχολίων που λήφθηκαν, για αυτούς που έδωσαν ως απάντηση την εικόνα 1, ήταν η ύπαρξη ανακρίβειών στο url, ένας τρόπος, όπως εξηγήθηκε σε παραπάνω ενότητα, αναγνώρισης ιστοσελίδων ηλεκτρονικού ψαρέματος. Το γεγονός όμως ότι περίπου οι μισοί από το δείγμα δεν ήταν σε θέση να το αναγνωρίσουν είναι ένα ανησυχητικό αποτέλεσμα.

Οι επόμενες ερωτήσεις, αντίθετα, κατέδειξαν την ύπαρξη επίγνωσης των εκπαιδευτικών, που απάντησαν, για την ασφάλεια των ηλεκτρονικών τους κωδικών. Το 97% έδωσε την απάντηση «Το όνομά μας ή/και την ημερομηνία γέννησής μας» στην ερώτηση 12 (βλ. εικόνα 16), «Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;» και στην ερώτηση 13, «Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;» το 98% απάντησε «F001_@14p» (βλ. εικόνα 17).

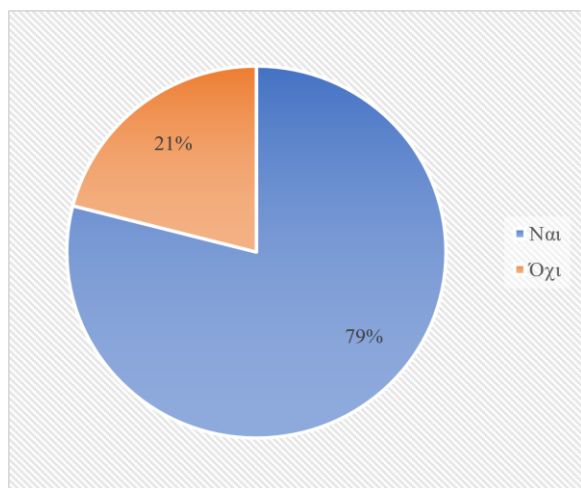


Εικόνα 16: Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;

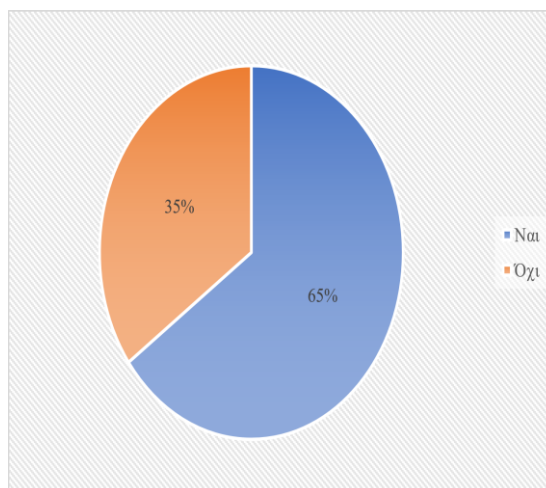


Εικόνα 17: Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;

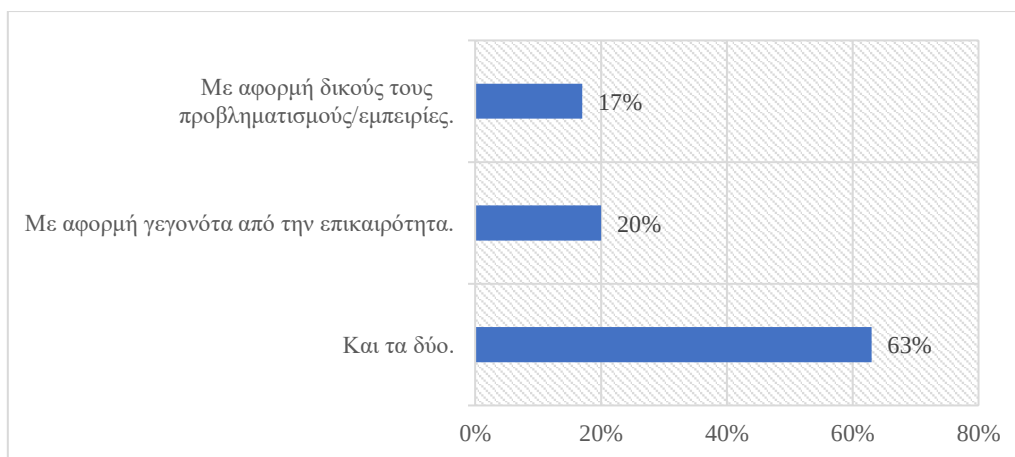
Το γεγονός ότι οι κίνδυνοι που συνδέονται με το διαδίκτυο είναι πλέον καθημερινοί και ένα συνεχές ζήτημα στο μυαλό των μαθητών φαίνονται και στις απαντήσεις των επόμενων ερωτήσεων. Συγκεκριμένα, στην ερώτηση 14, «Κατά τη διάρκεια του μαθήματος έχεις μιλήσει ποτέ με τους μαθητές για τους κινδύνους του διαδικτύου;» το 79% απάντησε θετικά (βλ. εικόνα 18). Επιπροσθέτως, το 65% των εκπαιδευτικών στην ερώτηση 15, «Οι μαθητές σου έχουν διατυπώσει απορίες για την ασφάλεια στο διαδίκτυο κατά τη διάρκεια του μαθήματος;» απάντησε ναι (βλ. εικόνα 19), με αφορμή τόσο τις εμπειρίες των ίδιων των μαθητών, όσο και τα γεγονότα της επικαιρότητας (βλ. εικόνα 20).



Εικόνα 18: Κατά τη διάρκεια του μαθήματος έχεις μιλήσει ποτέ με τους μαθητές για τους κινδύνους του διαδικτύου;

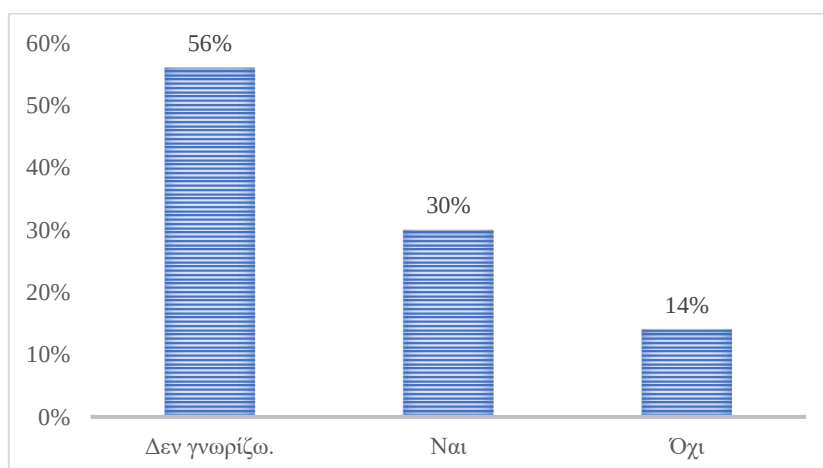


Εικόνα 19: Οι μαθητές σου έχουν διατυπώσει απορίες για την ασφάλεια στο διαδίκτυο κατά τη διάρκεια του μαθήματος;



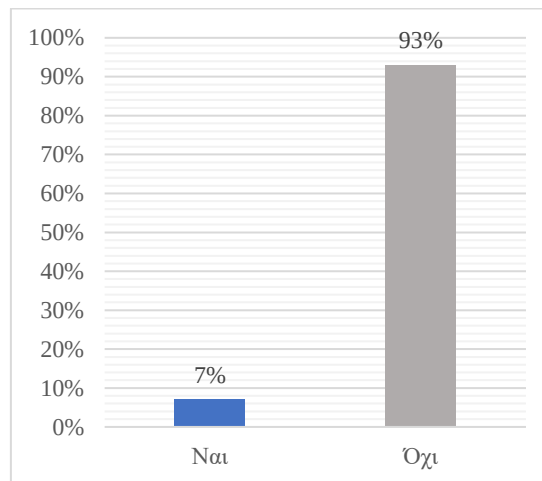
Εικόνα 20: Αν ναι, με αφορμή γεγονότα από την επικαιρότητα ή δικούς τους προβληματισμούς/εμπειρίες;

Παρόλα αυτά πάνω από τους μισούς ερωτηθέντες δεν είχαν επίγνωση περιπτώσεων όπου μαθητής του σχολείου που υπηρετούν, έχει πέσει θύμα κάποιας μορφής ηλεκτρονικής απειλής (βλ. εικόνα 21).

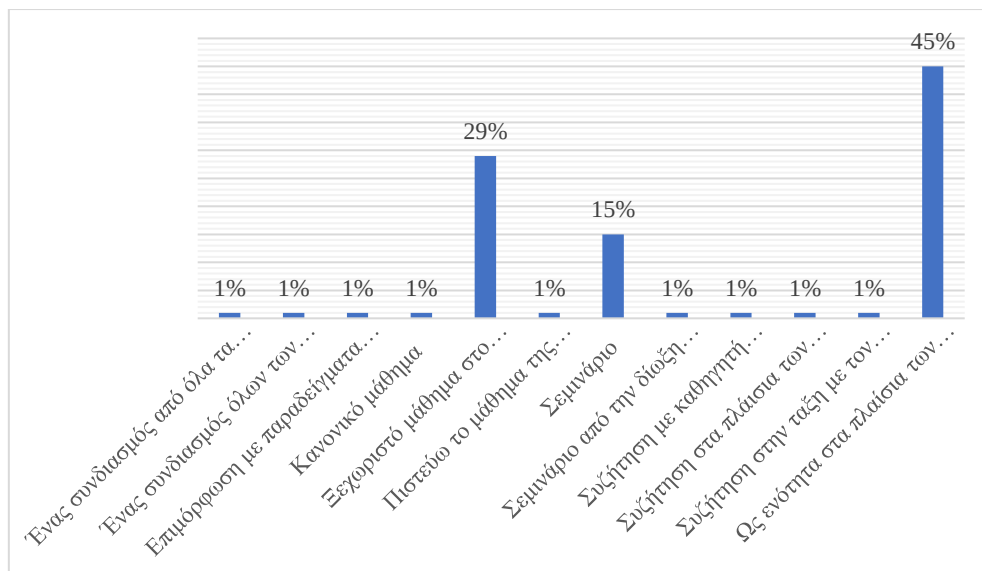


Εικόνα 21: Έχουν υπάρξει περιπτώσεις στο σχολείο που υπηρετείς, όπου μαθητής έχει πέσει θύμα κάποιας μορφής ηλεκτρονικής απειλής;

Τέλος, είναι ιδιαίτερα ενδιαφέρον, και ανησυχητικό, το γεγονός ότι στην ερώτηση 18, «Για την αντιμετώπιση ηλεκτρονικών κινδύνων πιστεύεις ότι επαρκεί το μάθημα της πληροφορικής;» το 93% απάντησε όχι (βλ. εικόνα 22). Από αυτούς που έδωσαν την απάντηση όχι, το 45,83%, ως αποτελεσματικότερο μέσο, πρότεινε την ηλεκτρονική ασφάλεια ως ενότητα στα πλαίσια των εργαστηρίων δεξιοτήτων, το 29,17% να εισαχθεί ως ξεχωριστό μάθημα στο πρόγραμμα σπουδών και το 15,63% θεώρησε την ένταξη ειδικού σεμιναρίου ως αποτελεσματικότερη μέθοδο (βλ. εικόνα 23).



Εικόνα 22: Για την αντιμετώπιση ηλεκτρονικών κινδύνων πιστεύεις ότι επαρκεί το μάθημα της πληροφορικής;



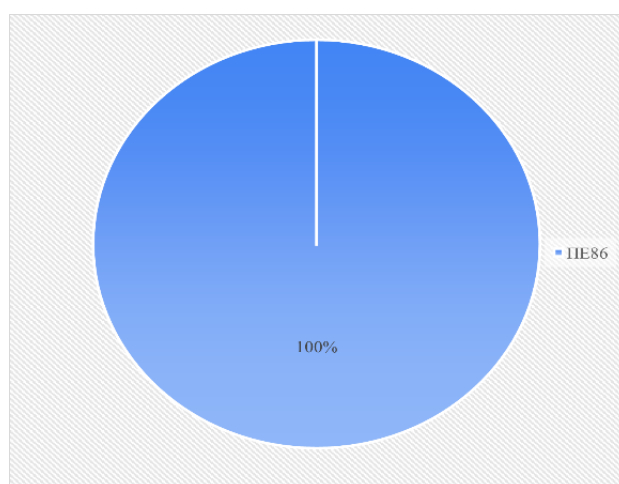
Εικόνα 23: Αν όχι, τι πιστεύεις ότι θα ήταν αποτελεσματικότερο;

Κάποιες από τις άλλες απαντήσεις που δόθηκαν ήταν ο συνδυασμός από όλα τα παραπάνω, ή και με επιμόρφωση των εκπαιδευτικών, η επιμόρφωση με παραδείγματα από ειδικούς, σεμινάριο από την δίωξη ηλεκτρονικού εγκλήματος και η συζήτηση με από κοινού τον καθηγητή πληροφορικής και τον ψυχολόγο. Αυτό που πρέπει να μας μένει είναι ότι η άποψη των καθηγητών για την αποτελεσματικότητα του μαθήματος της πληροφορικής, με τη δομή και το περιεχόμενο που έχει αυτή τη στιγμή στο αναλυτικό πρόγραμμα σπουδών, δεν επαρκεί για την αύξηση της επίγνωσης των μαθητών πάνω σε θέματα ηλεκτρονικής ασφάλειας.

Συγκεκριμένα για τους καθηγητές της πληροφορικής βλέπουμε τα εξής. Οι απαντήσεις, τις οποίες έδωσαν, καταδεικνύουν ότι η συντριπτική πλειοψηφία των καθηγητών

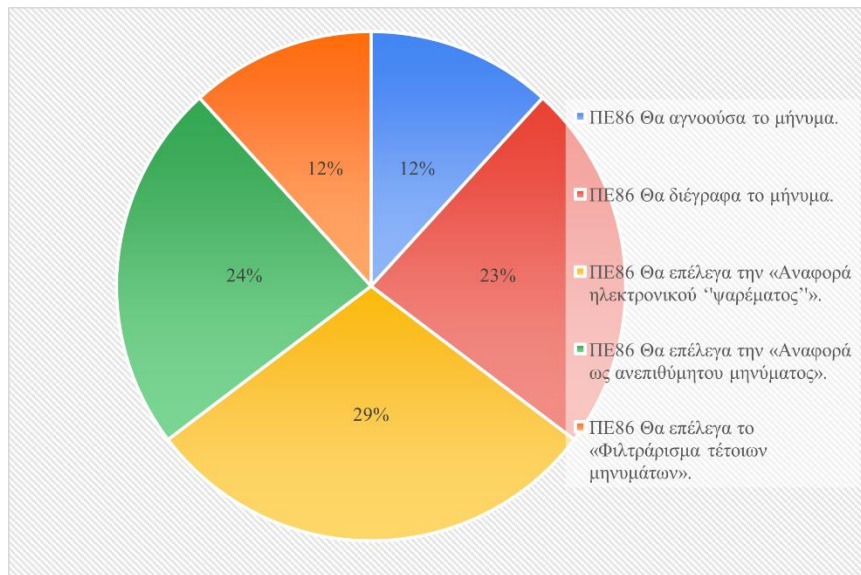
πληροφορικής που υπηρετούν την παρούσα χρονική στιγμή στο ελληνικό εκπαιδευτικό σύστημα έχουν επίγνωση, αν όχι βαθιά, τουλάχιστον πολύ καλή, των ηλεκτρονικών κινδύνων, πλην ελαχίστων εξαιρέσεων. Παρόλα αυτά προτείνουν και οι ίδιοι ότι το μάθημα της πληροφορικής δεν επαρκεί από μόνο του ή στη μορφή που έχει πάρει, περιεχόμενο και ώρες διδασκαλίας, για την εξοικείωση των μαθητών με τα ζητήματα της ηλεκτρονικής ασφάλειας.

Αναλυτικότερα, οι απαντήσεις που έδωσαν, μόνο οι καθηγητές της πληροφορικής, διαμορφώνονται ως εξής. Χωρίς να μας προκαλεί απορία, όλοι οι εκπαιδευτικοί απάντησαν θετικά στην ερώτηση 8, «Γνωρίζεις τι είναι το τι είναι το Phishing;» (βλ. εικόνα 24).



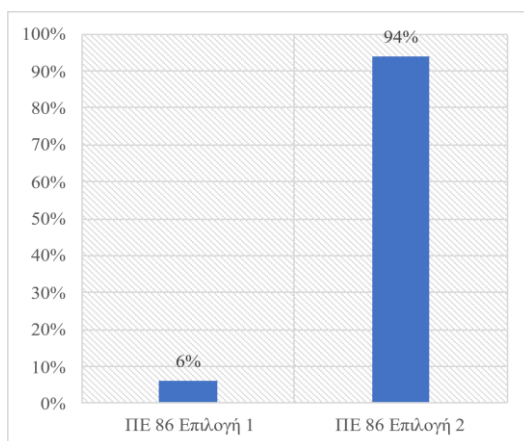
Εικόνα 24: Γνωρίζεις τι είναι το τι είναι το Phishing;

Όπως επίσης κανένας δεν επέλεξε τις απαντήσεις «Θα ακολουθούσα τον σύνδεσμο (Verify Now>>)» και «Θα απαντούσα στο μήνυμα» στην ερώτηση 9, «Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;». Αντιθέτως, το 29% επέλεξε την απάντηση «Θα επέλεγα την «Αναφορά ηλεκτρονικού 'ψαρέματος'»», το 24% την απάντηση «Θα επέλεγα την «Αναφορά ως ανεπιθύμητου μηνύματος»», το 23% την απάντηση «Θα διέγραφα το μήνυμα», το 12% την απάντηση «Θα επέλεγα το «Φιλτράρισμα τέτοιων μηνυμάτων»» και το υπόλοιπο 12% την απάντηση «Θα αγνοούσα το μήνυμα» (βλ. εικόνα 25).

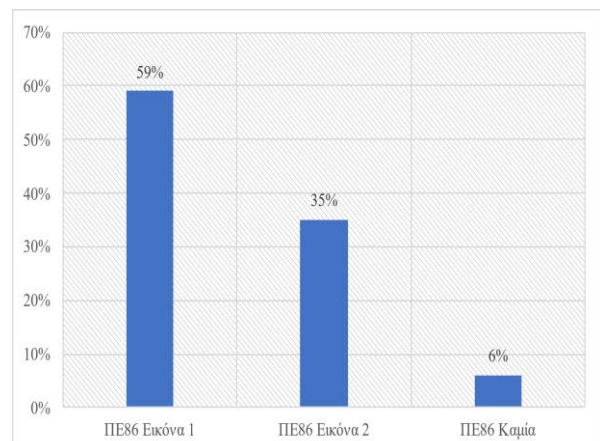


Εικόνα 25: Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου; (ΠΕ86)

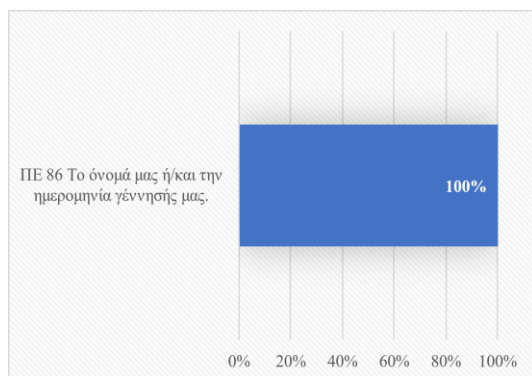
Λίγο πιο ανησυχητικά είναι τα ποσοστά στις επόμενες απαντήσεις, λαμβάνοντας υπόψη την ειδικότητα των ερωτηθέντων. Αν και στην ερώτηση 10, «Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;» το 94% απάντησε σωστά (βλ. εικόνα 26), μόλις το 59% ήταν σε θέση να αναγνωρίσει το ύποπτο url στην ερώτηση 11 «Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;» (βλ. εικόνα 27). Αλλά στις ερωτήσεις 12, «Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;» και 13, «Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;» το 100% έδωσε την ορθή απάντηση (βλ. εικόνες 28 & 29).



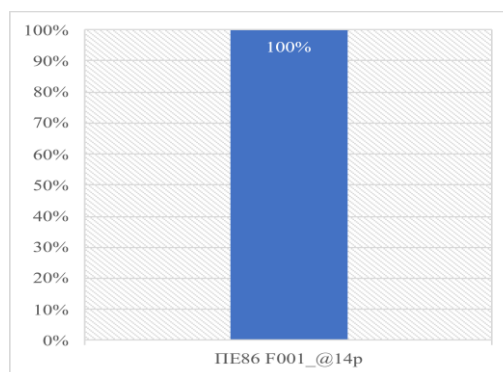
Εικόνα 26: Ποιο από τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής; (ΠΕ86)



Εικόνα 27: Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη; (ΠΕ86)

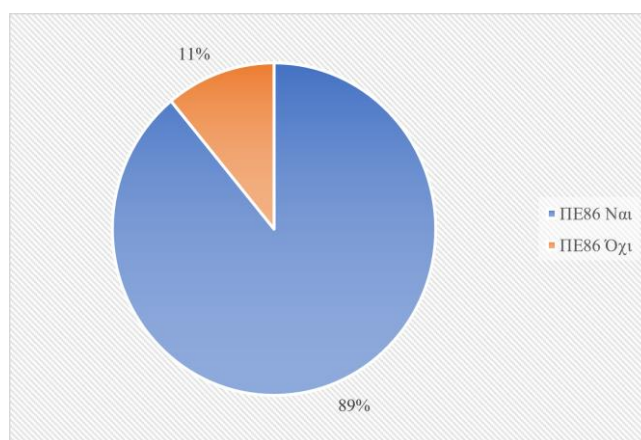


Εικόνα 28: Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας; (ΠΕ86)



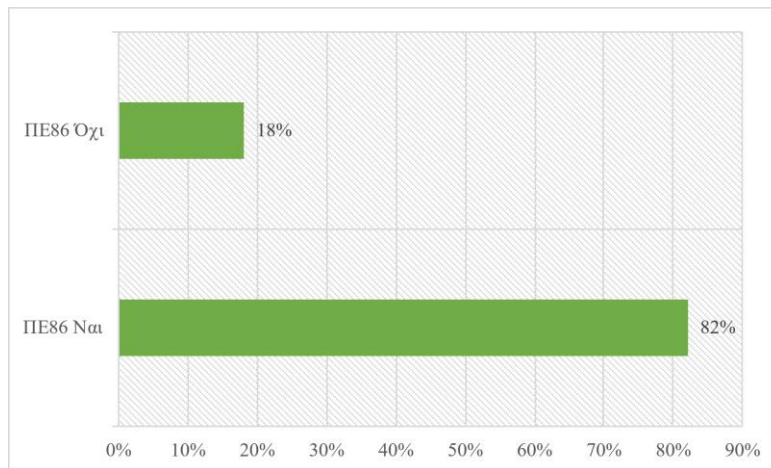
Εικόνα 29: Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης; (ΠΕ86)

Στο επόμενο σετ ερωτήσεων, που περιλαμβάνουν τις καθημερινές εμπειρίες των μαθητών τους, φαίνεται ότι το μάθημα της πληροφορικής δίνει στους μαθητές περισσότερες ευκαιρίες για διατύπωση αποριών και προβληματισμών τους πάνω στο θέμα. Συγκεκριμένα το 89% των καθηγητών πληροφορικής απάντησε θετικά στην ερώτηση 14, «Κατά τη διάρκεια του μαθήματος έχεις μιλήσει ποτέ με τους μαθητές για τους κινδύνους του διαδικτύου;» (βλ. εικόνα 30).

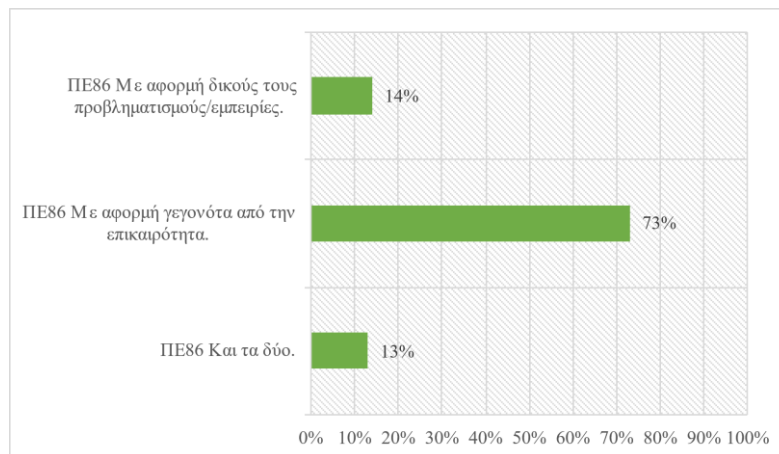


Εικόνα 30: Κατά τη διάρκεια του μαθήματος έχεις μιλήσει ποτέ με τους μαθητές για τους κινδύνους του διαδικτύου; (ΠΕ86)

Επιπλέον, το 82% απάντησε θετικά και στην ερώτηση 15, «Οι μαθητές σου έχουν διατυπώσει απορίες για την ασφάλεια στο διαδίκτυο κατά τη διάρκεια του μαθήματος;» (βλ. εικόνα 31), με αφορμή τόσο τα γεγονότα από την επικαιρότητα, όσο και τους προβληματισμούς ή τις εμπειρίες των μαθητών (βλ. εικόνα 32).

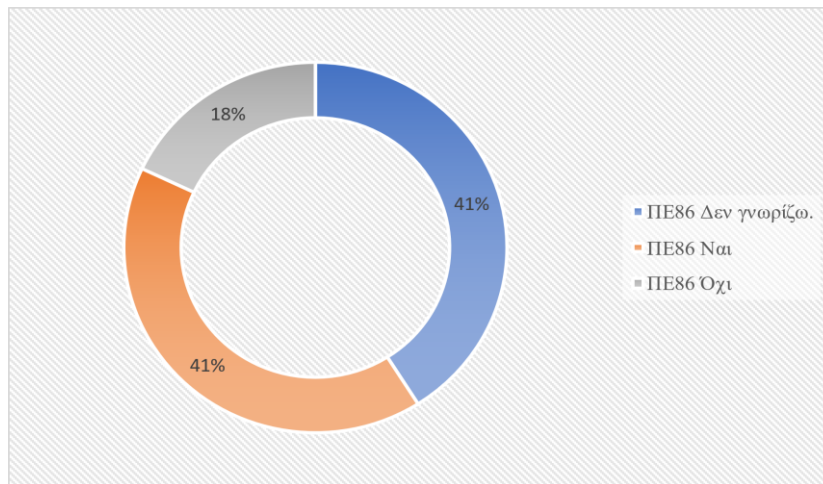


Εικόνα 31: Οι μαθητές σου έχουν διατυπώσει απορίες για την ασφάλεια στο διαδίκτυο κατά τη διάρκεια του μαθήματος; (ΠΕ86)



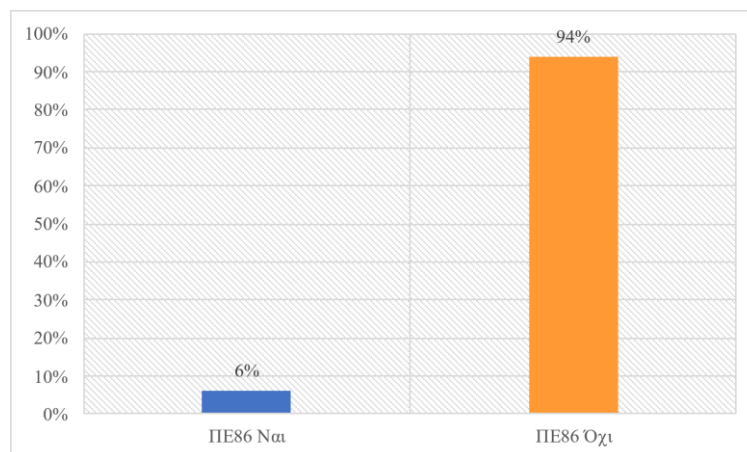
Εικόνα 32: Αν ναι, με αφορμή γεγονότα από την επικαιρότητα ή τους δικούς τους προβληματισμούς/απορίες; (ΠΕ86)

Αντιπαραβάλλοντας τις απαντήσεις με αυτές του συνολικού δείγματος βλέπουμε μια σημαντική αύξηση τόσο στην ερώτηση 14, όπου το ποσοστό θετικών απαντήσεων ήταν 79%, και ακόμα περισσότερο στην ερώτηση 15, όπου το ποσοστό θετικών απαντήσεων στο σύνολο του δείγματος ήταν 65%. Τέλος, οι καθηγητές πληροφορικής φαίνονται να είναι πιο ενήμεροι για τις περιπτώσεις όπου ένας μαθητής έχει πέσει θύμα κάποιας μορφής ηλεκτρονικής απειλής, με το 41% να απαντάει ότι δεν γνωρίζει στην ερώτηση 17(βλ. εικόνα 33), σε αντίθεση με το 56% των απαντήσεων του συνολικού δείγματος.



Εικόνα 33: Έχουν υπάρξει περιπτώσεις στο σχολείο που υπηρετείς, όπου μαθητής έχει πέσει θύμα κάποιας μορφής ηλεκτρονικής απειλής; (ΠΕ86)

Στην ερώτηση 18, «Για την αντιμετώπιση ηλεκτρονικών κινδύνων πιστεύεις ότι επαρκεί το μάθημα της πληροφορικής;», δεν υπάρχει σημαντική απόκλιση από το συνολικό δείγμα, με το 94% να απαντάει αρνητικά (βλ. εικόνα 34).



Εικόνα 34: Για την αντιμετώπιση των ηλεκτρονικών κινδύνων πιστεύεις ότι επαρκεί το μάθημα της πληροφορικής; (ΠΕ86)

Υπάρχουν όμως ποσοτικές και ποιοτικές διαφορές στις απαντήσεις που έδωσαν στην ερώτηση 19, «Αν όχι, τι πιστεύεις ότι θα ήταν αποτελεσματικότερο;». Συγκεκριμένα ένα πολύ μικρότερο ποσοστό πιστεύει ότι επαρκεί η ένταξη της ενότητας στα πλαίσια των εργαστηρίων δεξιοτήτων, 23% σε αντίθεση με το 49% του συνολικού δείγματος, και μόλις το 12% ότι επαρκεί το σεμινάριο. Αντίθετα το 47% των καθηγητών του μαθήματος της πληροφορικής πιστεύει ότι χρειάζεται η ένταξη ενός ξεχωριστού μαθήματος για την αντιμετώπιση των ηλεκτρονικών κινδύνων (βλ. εικόνα 35).



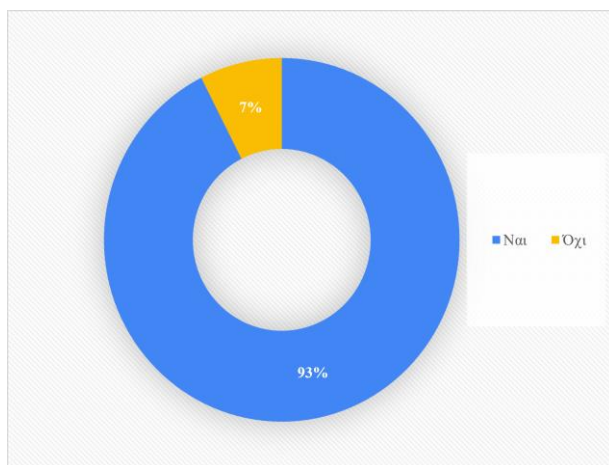
Εικόνα 35: Αν όχι, τι πιστεύεις ότι θα ήταν αποτελεσματικότερο; (ΠΕ86)

Τέλος, σύμφωνα με τις ελεύθερες απαντήσεις που έδωσαν πιστεύουν επίσης ότι απαιτείται ένας συνδυασμός των παραπάνω μεθόδων, η ταυτόχρονη επιμόρφωση των εκπαιδευτικών, όπως επίσης και ότι θα πρέπει να αλλάξει το αναλυτικό πρόγραμμα σπουδών, με την παράλληλη αύξηση των ωρών διδασκαλίας του μαθήματος, ενώ οι καθηγητές των υπόλοιπων ειδικοτήτων πρότειναν σεμινάρια από ειδικούς ή τη Δίωξη Ηλεκτρονικού Εγκλήματος και την παροχή συμβουλών από τον ψυχολόγο του σχολείου.

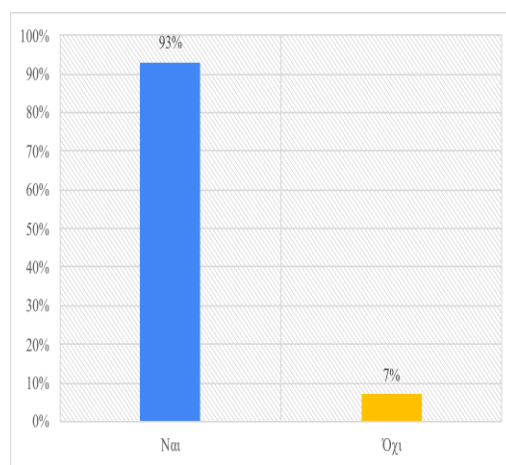
Συμπερασματικά, παρατηρείται ότι ένα ικανοποιητικό ποσοστό των Ελλήνων εκπαιδευτικών μπορεί να διακρίνει τους ηλεκτρονικούς κινδύνους. Ακόμα περισσότερο ικανοποιητικά είναι τα αποτελέσματα των καθηγητών πληροφορικής, αν και θα ήταν ιδιαίτερα χρήσιμη και σημαντική η συνεχής επιμόρφωση γύρω από τα θέματα της ηλεκτρονικής ασφάλειας και των ηλεκτρονικών κινδύνων. Όπως καταδείχθηκε και στο θεωρητικό κομμάτι της εργασίας αυτού τους είδους οι κίνδυνοι είναι διαρκείς και εξελισσόμενοι. Επομένως οι γνώσεις καθίστανται συνεχώς παρωχημένες και ανάγκης διεύρυνσης. Το ίδιο παρατηρείται και από τους ίδιους τους εκπαιδευτικούς, με ένα υψηλό ποσοστό των οποίων να πιστεύει ότι το μάθημα της πληροφορικής στο σχολείο δεν είναι σε θέση από μόνο του και στην παρούσα του μορφή να αντιμετωπίσει τους ηλεκτρονικούς κινδύνους.

3.2 Στάσεις και απόψεις μαθητών

Όπως αναφέρθηκε το διαδίκτυο αποτελεί μια βασική συνιστώσα στη ζωή των εφήβων σήμερα. Αυτό φαίνεται και από τις απαντήσεις που έδωσαν οι μαθητές στις ερωτήσεις 4-6. Συγκεκριμένα, στην ερώτηση 4, «Διαθέτεις e-mail;» απάντησε θετικά το 93% των μαθητών (βλ. εικόνα 36), όπως και στην ερώτηση 5, «Έχεις δημιουργήσει λογαριασμό κοινωνικής δικτύωσης (facebook, Instagram κλπ.);» (βλ. εικόνα 37).

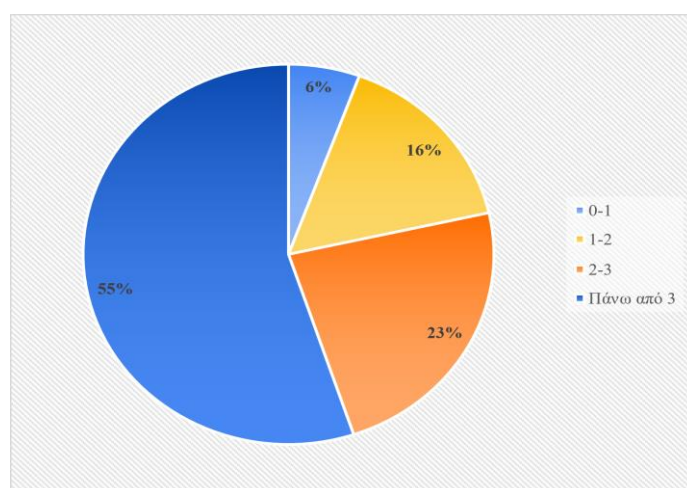


Εικόνα 36: Διαθέτεις email;



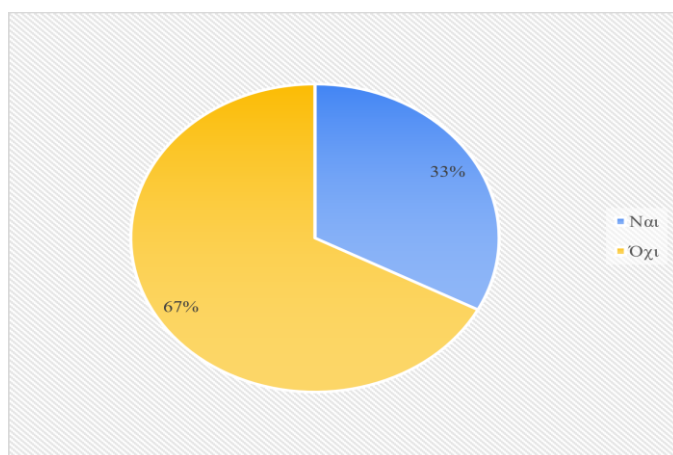
Εικόνα 37: Έχεις δημιουργήσει λογαριασμό κοινωνικής δικτύωσης (facebook, instagram κλπ);

Επιπλέον πάνω από τους μισούς μαθητές περνάνε πάνω από 3 ώρες ημερησίως στο διαδίκτυο, σύμφωνα με τις απαντήσεις στην ερώτηση 6, «Πόσες ώρες την ημέρα χρησιμοποιείς το διαδίκτυο;» (βλ. εικόνα 38).



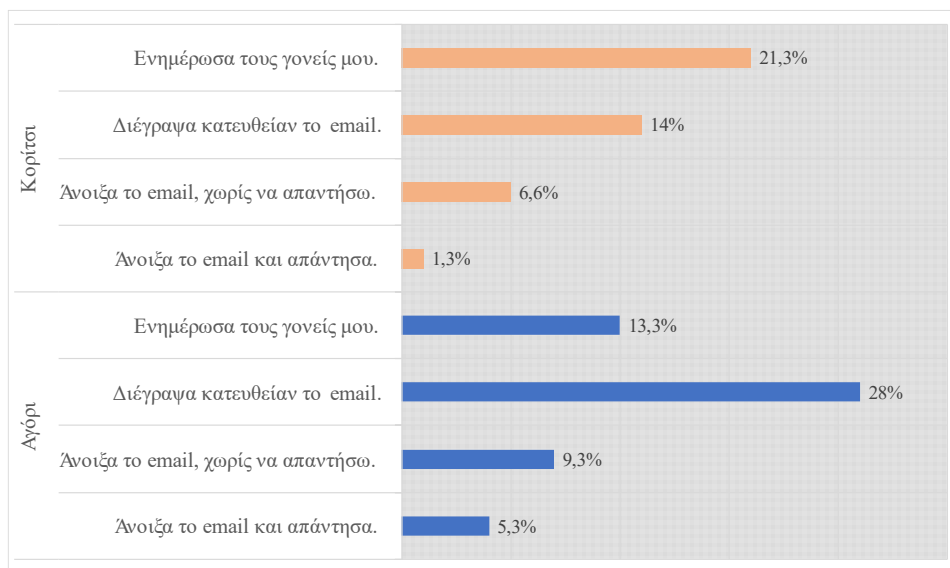
Εικόνα 38: Πόσες ώρες την ημέρα χρησιμοποιείς το διαδίκτυο;

Προχωρώντας στις ερωτήσεις σχετικά με τις προσωπικές εμπειρίες των μαθητών βλέπουμε ότι το 33% των μαθητών έχει λάβει, ή έχει πέσει στην αντίληψή του ότι έχει λάβει email από ύποπτη πηγή, το οποίο ζητάγε προσωπικά δεδομένα δικά τους ή των γονιών τους (βλ. εικόνα 39). Λαμβάνοντας υπόψη την ηλικία των μαθητών, ένας στους τρεις μαθητές είναι ένα πολύ υψηλό ποσοστό ατόμων που ενδέχεται να πέσει θύμα ηλεκτρονικών επιθέσεων.



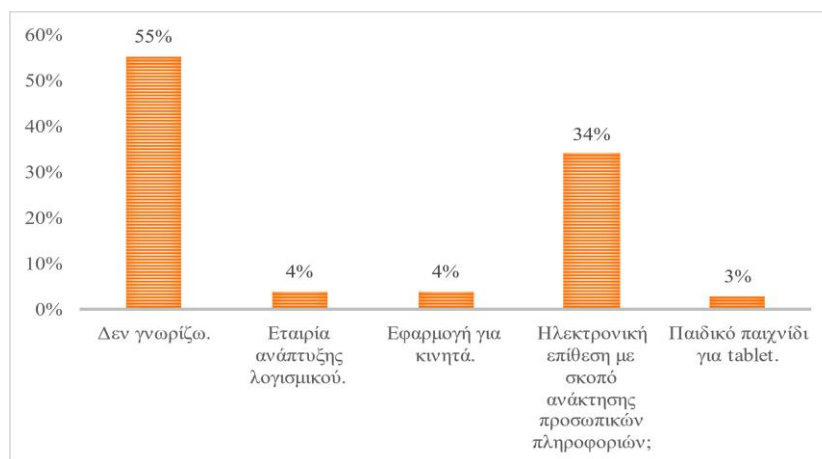
Εικόνα 39: Σου έχει σταλεί, ή έχει πέσει στην αντίληψή σου, email που να σου ζητάει προσωπικά δεδομένα, δικά σου ή των γονιών σου;

Πιο ενθαρρυντικές είναι οι απαντήσεις της επόμενης ερώτησης «Αν, ναι, πώς αντέδρασες;», όπου το 42% απάντησε «Διέγραψα κατευθείαν το email» και το 35% έδωσε την απάντηση «Ενημέρωσα τους γονείς μου». Ιδιαίτερα ενδιαφέρον είναι το γεγονός ότι από τις απαντήσεις διαπιστώθηκε η τάση των κοριτσιών για ενημέρωση των γονιών τους, με το 61% από τους μαθητές που έδωσαν αυτήν την απάντηση να είναι κορίτσια. Σε αυτό το συμπέρασμα είχε προβεί και στην έρευνα του ο Alwanain, όπως διατυπώθηκε σε προηγούμενο κομμάτι της εργασίας, ο οποίος μελετώντας τις αντιδράσεις μαθητών σε μηνύματα ηλεκτρονικού ψαρέματος μέσω της εφαρμογής WhatsApp, κατέληξε στο συμπέρασμα ότι τα κορίτσια είναι πιο πιθανό να ζητήσουν τη βοήθεια των γονιών τους, αν καταλάβουν ότι έχουν πέσει θύμα ηλεκτρονικής επίθεσης. Παραμένουν όμως περιπτώσεις όπου οι μαθητές δεν αντέδρασαν σωστά στην προκείμενη κατάσταση με το 16% να απαντάει «Άνοιξα το email, χωρίς να απαντήσω» και το 7% «Άνοιξα το email και απάντησα» (βλ. εικόνα 40), με τα αγόρια να είναι αυτά, που δίνουν κυρίως αυτές τις απαντήσεις.



Εικόνα 40: Αν ναι, πώς αντέδρασες;

Τα τελευταία αυτά ποσοστά φαίνονται μικρά αλλά πρέπει να ληφθεί υπόψη και η επόμενη ερώτηση «Γνωρίζεις τι είναι το Phishing;», όπου μόνο το 34% απάντησε ότι πρόκειται για «ηλεκτρονική επίθεση με σκοπό ανάκτησης προσωπικών πληροφοριών». Το 55% απάντησε ότι δεν γνωρίζει, το 4% έδωσε την απάντηση «εφαρμογή για κινητά», το 4% την απάντηση «εταιρία ανάπτυξης λογισμικού» και το 3% «παιδικό παιχνίδι για tablet» (βλ. εικόνα 41).

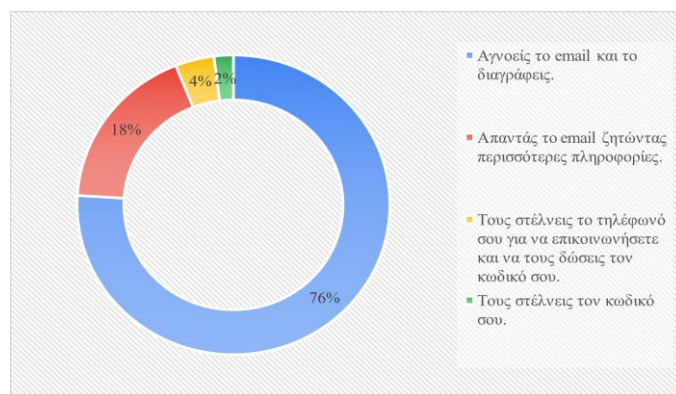


Εικόνα 41: Γνωρίζεις τι είναι το phishing;

Επομένως είναι μόνο λογικό να υποθέσουμε ότι και τα αποτελέσματα της ερώτησης 7 ενδέχεται να είναι στην πραγματικότητα πολύ διαφορετικά, από τη στιγμή που γίνεται λόγος για ένα δείγμα που δεν ξέρει τι περιλαμβάνει το ηλεκτρονικό ψάρεμα. Ιδιαίτερα αξιοσημείωτο, όμως, είναι το γεγονός ότι η συντριπτική πλειοψηφία των μεγαλύτερων μαθητών, με ηλικίες 15-18 ετών, με ποσοστό 72%, δεν γνωρίζει τι είναι ή τι

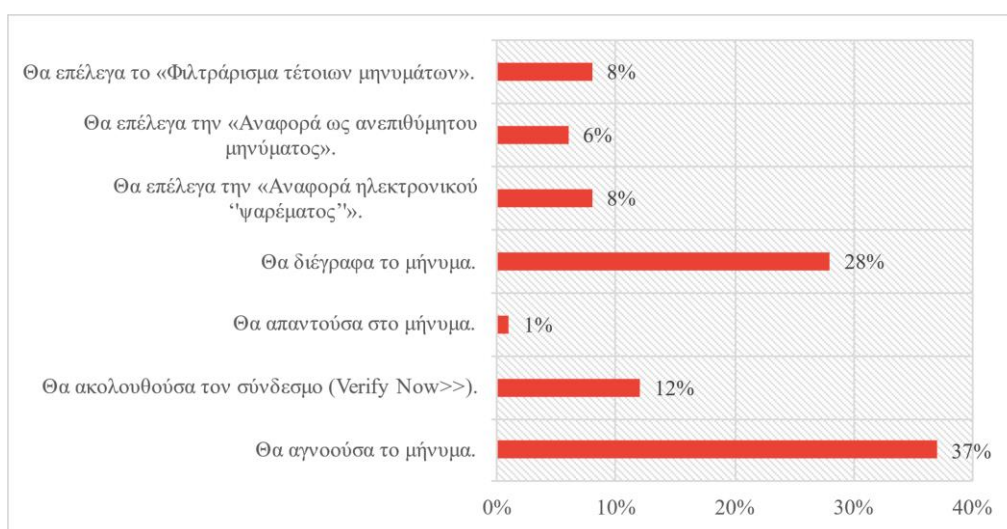
περιλαμβάνει το ηλεκτρονικό ψάρεμα. Ενώ στις μικρότερες ηλικίες το αντίστοιχο ποσοστό είναι 64%. Βλέποντας τις ηλικίες των μαθητών, κάποιος θα περίμενε περισσότερος μαθητές λυκείου να είναι σε θέση να γνωρίζουν τι περιλαμβάνει το ηλεκτρονικό ψάρεμα, σε αντίθεση με μαθητές γυμνασίου. Τα αποτελέσματα, όμως, αυτά έστω και με μία διαφορά μικρότερη του 10% έρχονται να ενισχύσουν την υπόθεση ότι η ένταξη της ηλεκτρονικής ασφάλειας, είτε ως ξεχωριστό μάθημα, είτε στα πλαίσια του μαθήματος της πληροφορικής από τις πρώτες τάξεις της δευτεροβάθμιας εκπαίδευσης, ίσως και της πρωτοβάθμιας, είναι αναγκαία. Οι συνεχόμενοι κίνδυνοι, μαζί με τη μεγαλύτερη δημοσιότητα που πλέον παίρνουν, προκαλούν όλο και περισσότερες απορίες και αφορμές συζητήσεων στα πλαίσια του μαθήματος, που μπορεί να μη γίνονταν στο πρόσφατο παρελθόν, και σίγουρα διατυπώνονται πιο εύκολα από παιδιά μικρότερης ηλικίας. Επομένως, μπορούμε να υποθέσουμε ότι αυτή η μεγάλη διαφορά ανάμεσα στις απαντήσεις των μικρότερων και των μεγαλύτερων μαθητών αποτελεί και μια λογική συνέπεια της προσπάθειας ενημέρωσης των μαθητών για τα ζητήματα της ηλεκτρονικής ασφάλειας, ή ακόμα και της πρόσφατης ένταξης των εργαστηρίων δεξιοτήτων κυρίως στο γυμνάσιο, τα οποία περιλαμβάνουν και αυτή τη θεματική.

Στις επόμενες ερωτήσεις φαίνεται όμως ότι τα ένστικτα των μαθητών ήταν σωστά. Στην ερώτηση 10, «Λαμβάνεις email από το αγαπημένο σου site ζητώντας να τους προωθήσεις τον κωδικό σου για να κάνουν κάποιες τροποποιήσεις στο λογαριασμό σου. Τι κάνεις;» το 76% των μαθητών απάντησε «Αγνοείς το email και το διαγράφεις». Αυτό όμως δε θα πρέπει να μας καθησυχάζει καθώς το υπόλοιπο 24% των απαντήσεων διαμορφώνεται ως εξής. Το 18% απάντησε «Απαντάς το email ζητώντας περισσότερες πληροφορίες», το 4% «Τους στέλνεις τον κωδικό σου» και το 2% «Τους στέλνεις το τηλέφωνό σου για να επικοινωνήσετε και να τους δώσεις τον κωδικό σου» (βλ. εικόνα 42). Και εδώ, πρέπει να λαμβάνεται υπόψη η ηλικία των συμμετεχόντων και ότι ο κίνδυνος πολλαπλασιάζεται όταν γίνεται λόγος για ανήλικα θύματα του ηλεκτρονικού ψαρέματος.



Εικόνα 42: Λαμβάνεις email από το αγαπημένο σου site αναζητώντας να τους προωθήσεις τον κωδικό σου για να κάνουν κάποιες τροποποιήσεις στο λογαριασμό σου. Τι κάνεις;

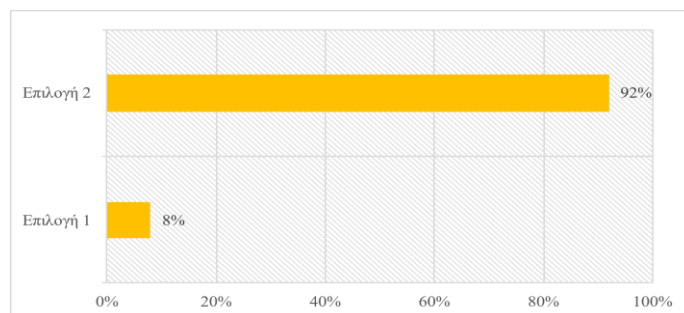
Αντίστοιχα και στην ερώτηση 11, «Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;» λήφθηκαν σχετικά ικανοποιητικά αποτελέσματα. Το 37% απάντησε «Θα αγνοούσα το μήνυμα», το 28% «Θα διέγραφα το μήνυμα», το 8% «Θα επέλεγα το «Φιλτράρισμα τέτοιων μηνυμάτων»», το 8% «Θα επέλεγα την «Αναφορά ηλεκτρονικού 'ψαρέματος'»», το 6% «Θα επέλεγα την «Αναφορά ως ανεπιθύμητου μηνύματος»». Το υπόλοιπο όμως 13% μοιράζεται σε 12% με απάντηση «Θα ακολουθούσα τον σύνδεσμο (Verify Now>>)» και ένα 1% με απάντηση «Θα απαντούσα στο μήνυμα» (βλ. εικόνα 43).



Εικόνα 43: Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;

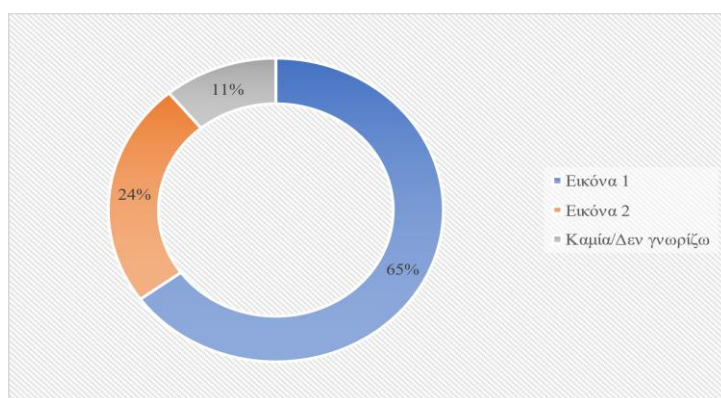
Όσον αφορά την αναγνώριση ύποπτων ιστοσελίδων στην ερώτηση 12 «Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;» το 92% έδωσε τη σωστή απάντηση - εικόνα 2- (βλ. εικόνα 44), με τους μαθητές που απάντησαν

λάθος να είναι κατά κύριο λόγο κορίτσια, ηλικιών 12-15 ετών. Αλλά στην επόμενη ερώτηση «Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;» το ένα τρίτο δεν ήταν σε θέση να αναγνωρίσει την ύποπτη εικόνα.



Εικόνα 44: Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;

Συγκεκριμένα το 65% ήταν σε θέση να πει ποια από τις δύο ιστοσελίδες ήταν η ύποπτη, το 24% έδωσε τη λανθασμένη απάντηση και ένα 11% απάντησε ότι δεν γνωρίζει ποια ιστοσελίδα είναι η ύποπτη (βλ. εικόνα 45).

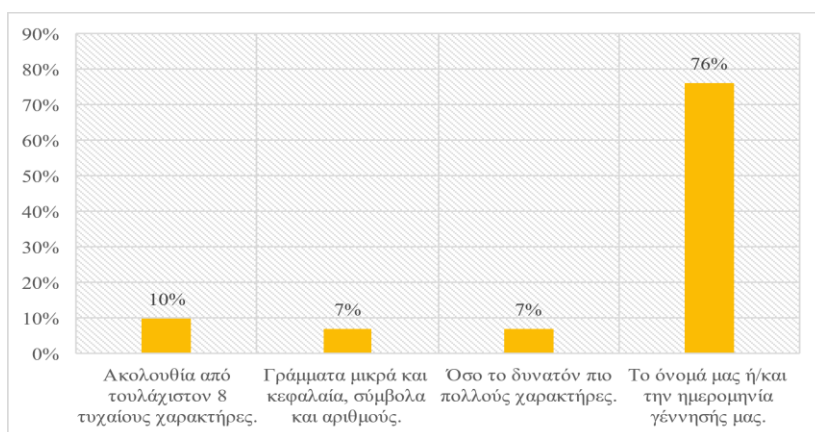


Εικόνα 45: Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη και γιατί;

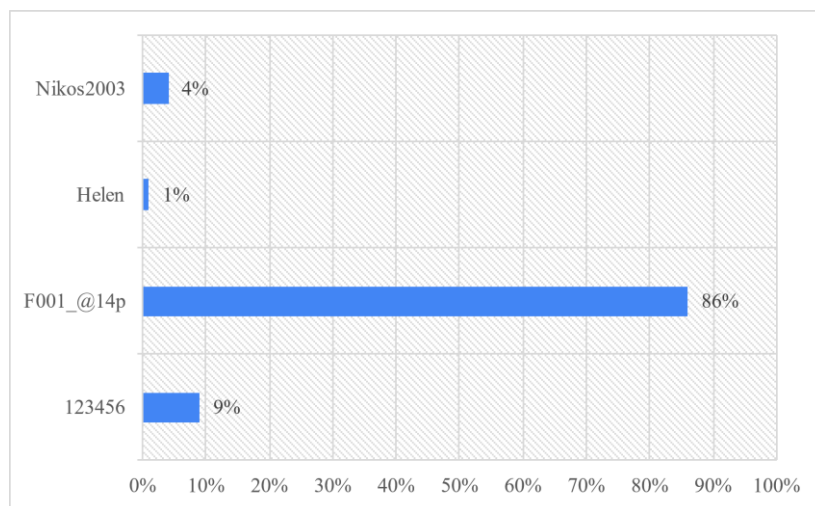
Επιπλέον από τους μαθητές που έδωσαν ως απάντηση την εικόνα 1, μόνο λίγοι δικαιολόγησαν την απάντησή τους στη βάση του ανακριβούς url. Οι περισσότερες απαντήσεις, βάσει της δικαιολόγησης, ήταν αποτέλεσμα υποθέσεων ή δεν έδωσαν καν δικαιολόγηση. Συγκεκριμένα μόνο 14 μαθητές πρόσεξαν ότι το url της σελίδας ήταν περίεργο, και από αυτούς μόνο μία μαθήτρια 12 ετών πρόσεξε ότι έγραφε Facelook αντί για Facebook (idn spoofing), αν και σε όλες τις υπόλοιπες ερωτήσεις έδωσε τις λανθασμένες απαντήσεις.

Σχετικά με τις γνώσεις των μαθητών πάνω στην προστασία των κωδικών τους παρατηρούμε ότι ένα ικανοποιητικό ποσοστό έχει επίγνωση για τη σημασία της ισχύς των κωδικών. Συγκεκριμένα το 76% στην ερώτηση 14 «Ποιο από τα παρακάτω ΔΕΝ

θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;» έδωσε τη σωστή απάντηση «Το όνομά μας ή/και την ημερομηνία γέννησής μας», το 10% «Ακολουθία από τουλάχιστον 8 τυχαίους χαρακτήρες», το 7% «Γράμματα μικρά και κεφαλαία, σύμβολα και αριθμούς» και το 7% «Όσο το δυνατόν πιο πολλούς χαρακτήρες» (βλ. εικόνα 46). Στην ερώτηση 15 «Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;» το 86% απάντησε «F001_@14p», το 9% «123456», το 4% «Nikos2003» και το 1% «Helen» (βλ. εικόνα 47).



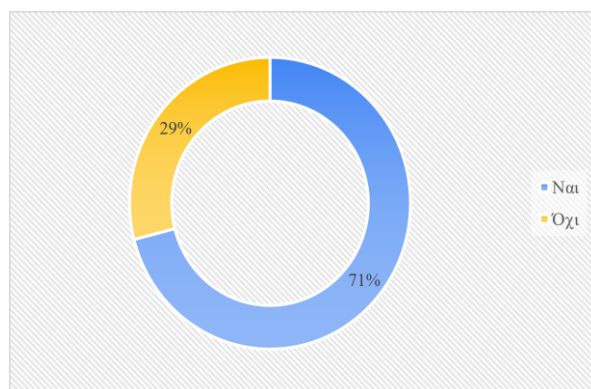
Εικόνα 46: Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;



Εικόνα 47: Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;

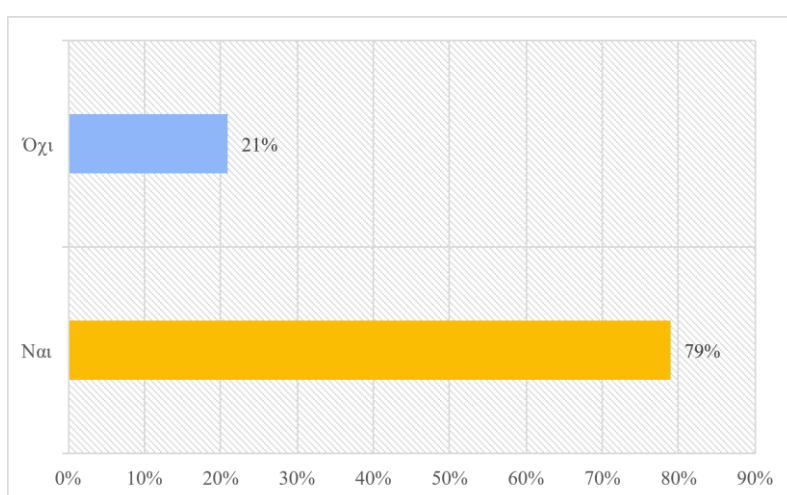
Τέλος, όσον αφορά τις απόψεις των μαθητών σχετικά με την αποτελεσματικότητα του ισχύοντος προγράμματος σπουδών έχουν ληφθεί αντιθετικά μεταξύ τους αποτελέσματα. Στην ερώτηση 16 «Πιστεύεις, με όσα έχεις μάθει στο σχολείο, ότι

μπορείς να αναγνωρίσεις ηλεκτρονικές απειλές;» το 71% απάντησε θετικά (βλ. εικόνα 48).



Εικόνα 48: Πιστεύεις, με όσα έχεις μάθει στο σχολείο, ότι μπορείς να αναγνωρίσεις ηλεκτρονικές απειλές;

Παράλληλα το 79% στην ερώτηση 17 «Θα ήθελες να γίνονται περισσότερα μαθήματα στο σχολείο για την ασφάλεια στο Διαδίκτυο;» απάντησε επίσης θετικά (βλ. εικόνα 49). Ενδιαφέρον παρουσιάζει το γεγονός ότι τα κορίτσια ήταν πιο δεκτικά στην εισαγωγή νέων μαθημάτων στο πρόγραμμα σπουδών, σε αντίθεση με τα αγόρια που έδειξαν μια τάση άρνησης προς αυτή. Πέρα από αυτήν την ερώτηση, όμως δε βρέθηκαν άλλες μεγάλες στατιστικές διαφορές ανάμεσα στις απαντήσεις αγοριών και κοριτσιών. Επιπλέον, φαίνεται ότι οι μαθητές με αγαπημένα μαθήματα αυτά των ανθρωπιστικών και κοινωνικών επιστημών δείχνουν να είναι πιο θετικοί στην ένταξη νέων μαθημάτων, σε σχέση με τους συμμαθητές τους με αγαπημένα μαθήματα, αυτά των θετικών επιστημών, που ήταν συγκριτικά περισσότερο αρνητικοί.



Εικόνα 49: Θα ήθελες να γίνονται περισσότερα μαθήματα στο σχολείο για την ασφάλεια στο Διαδίκτυο;

Οι μαθητές που απάντησαν την πληροφορική ως το αγαπημένο τους μάθημα παρουσιάζουν τις εξής τάσεις. Παρά την απάντησή τους ότι η πληροφορική είναι το αγαπημένο τους μάθημα, μόνο το 50% απάντησε ότι γνωρίζει τι είναι το ηλεκτρονικό ψάρεμα, με το υπόλοιπο 50% να δηλώνει ότι δεν γνωρίζει, χωρίς όμως να δίνει κάποια από τις λανθασμένες απαντήσεις. Αλλά όλοι θα αγνοούσαν και θα διέγραφαν το μήνυμα στην ερώτηση «Λαμβάνεις email από το αγαπημένο σου site ζητώντας να τους προωθήσεις τον κωδικό σου για να κάνουν κάποιες τροποποιήσεις στο λογαριασμό σου. Τι κάνεις;». Στην επόμενη ερώτηση, όμως, «Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν η ενέργειά σου;» το 30% θα ακολουθούσε το σύνδεσμο. Επιπλέον το σύνολο των μαθητών έδειξε ότι ξέρει να αναγνωρίζει μία ασφαλή ιστοσελίδα, στην ερώτηση «Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;», αν και μόνο το 70% αναγνώρισε την ύποπτη ιστοσελίδα στην ερώτηση «Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη;». Ενθαρρυντικό είναι το γεγονός ότι το 90% απάντησε σωστά στην ερώτηση «Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;» και το 100% στην ερώτηση «Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;». Τέλος, η πλειονότητα των μαθητών, 80%, θεωρεί επαρκές το πρόγραμμα σπουδών για την αναγνώριση των ηλεκτρονικών απειλών, αν και το 60% θα επιθυμούσε την εισαγωγή νέων επιπλέον μαθημάτων για την ηλεκτρονική ασφάλεια. Η γενικότερη τάση δείχνει ότι μαθητές με αγαπημένο μάθημα την πληροφορική είναι σε θέση να αναγνωρίσουν τις ηλεκτρονικές απειλές και θα μπορούσαν να προστατεύσουν τα προσωπικά τους δεδομένα σε ενδεχόμενες επιθέσεις.

Αντιπαραβάλλοντας τις απαντήσεις μόνο των μαθητών που απάντησαν σωστά στην ερώτηση 9, «Γνωρίζεις τι είναι το Phishing» με τις υπόλοιπες μπορούμε να βρούμε μερικά ενδιαφέροντα ευρήματα. Γενικώς, παρατηρείται ότι παρά τη φαινομενικά θεωρητική γνώση, σε πρακτικό επίπεδο πολλοί από τους μαθητές θα έπεφταν ή έχουν πέσει θύματα ηλεκτρονικού ψαρέματος. Στην αμέσως επόμενη ερώτηση, «Λαμβάνεις email από το αγαπημένο σου site ζητώντας να τους προωθήσεις τον κωδικό σου για να κάνουν κάποιες τροποποιήσεις στο λογαριασμό σου. Τι κάνεις;», μόνο το 70% απάντησε ότι θα αγνοούσε και θα διέγραφε το email. Επιπλέον, αν και μικρό, ένα 5% στην ερώτηση «Αν λάμβανες αυτό το email το οποίο σε παραπέμπει να ακολουθήσεις το Link (Verify Now>>) για να επαληθεύσεις τα προσωπικά σου στοιχεία, ποια θα ήταν

η ενέργειά σου;», απάντησε ότι θα ακολουθούσε το σύνδεσμο. Τα αποτελέσματα ήταν πιο θετικά στις επόμενες ερωτήσεις. Στην ερώτηση «Ποιο από αυτά τα δύο εικονίδια δείχνει ότι η ιστοσελίδα που έχεις επισκεφθεί είναι ασφαλής;», μόλις το 3% απάντησε λανθασμένα, αν και στην ερώτηση «Ποια από τις παρακάτω εικόνες σου φαίνεται ύποπτη», μόλις το 70% αναγνώρισε την ύποπτη ιστοσελίδα. Το 87% όμως απάντησε σωστά στην ερώτηση «Ποιο από τα παρακάτω ΔΕΝ θα πρέπει να έχει ένας ισχυρός κωδικός ασφάλειας;» και το 92% στην ερώτηση «Ποιος από τους παρακάτω θεωρείται ισχυρός κωδικός πρόσβασης;» αναγνώρισε τον ισχυρό κωδικό. Αυτό που προκαλεί εντύπωση είναι μόλις το 65% των μαθητών που γνωρίζουν τι είναι το ηλεκτρονικό ψάρεμα θεωρεί επαρκές το υπάρχον πρόγραμμα σπουδών για την αναγνώριση των ηλεκτρονικών απειλών, αν και η τάση στην επόμενη ερώτηση παραμένει ίδια με αυτή του συνολικού δείγματος με το 78 % των μαθητών να απαντάει ότι θα επιθυμούσε την εισαγωγή νέου μαθήματος για την ασφάλεια στο διαδίκτυο.

Επιπλέον παρατηρούνται και δύο πολύ αντιθετικές τάσεις ανάμεσα σε δύο μερίδες μαθητών. Συνολικά από όλους τους μαθητές σωστά σε όλες τις ερωτήσεις απάντησαν 15. Οι συγκεκριμένοι μαθητές, αγόρια και κορίτσια όλων των ηλικιών με κλίση στις θετικές επιστήμες, βάσει των απαντήσεών τους στην ερώτηση «Ποιο είναι το αγαπημένο σου μάθημα», δείχνουν μια γενική ικανοποίηση από όσα έχουν μάθει από το σχολείο σχετικά με την ηλεκτρονική ασφάλεια. Παρόλα αυτά, εξακολουθούν να δηλώνουν ότι θα ήθελαν να γίνονται περισσότερα μαθήματα πάνω σε αυτό το ζήτημα. Από την άλλη πλευρά 4 από τους μαθητές, 3 αγόρια και ένα κορίτσι ηλικιών 12-15 ετών που κάνουν πολύ συχνή χρήση διαδικτύου, πάνω από 3 ώρες την ημέρα, δεν κατάφεραν να δώσουν καμία σωστή απάντηση. Σε αντίθεση με τους συμμαθητές τους παραπάνω, δήλωσαν ότι δεν αισθάνονται ότι έχουν μάθει αρκετά, στα πλαίσια του σχολείου, για την αντιμετώπιση των ηλεκτρονικών απειλών, δεν επιθυμούν όμως την ένταξη νέων μαθημάτων για την ηλεκτρονική ασφάλεια. Από αυτό μπορούμε να συμπεράνουμε ότι ίσως και οι συνολικές σχολικές επιδόσεις ή η σχολική συμπεριφορά έχουν έναν αντίκτυπο στον τρόπο που διαχειρίζονται τις ηλεκτρονικές απειλές. Οι μαθητές που απάντησαν σωστά δέχονται την ένταξη ακόμα περισσότερων μαθημάτων σε αντίθεση με τους συμμαθητές τους που απάντησαν λάθος. Ίσως βιωματικά εργαστήρια ή παιχνίδια προσομοίωσης αποτελούν την ενδεδειγμένη λύση για την προσέλκυση της προσοχής και του ενδιαφέροντος. Άλλωστε καταδείχθηκε και από τη βιβλιογραφία με την έρευνα των Pencheva, Hallett και Rashid ότι αυτή η προσέγγιση

οδηγεί σε καλύτερα αποτελέσματα, δεδομένης της θέλησης των καθηγητών αλλά και της διοικητικής υποστήριξης για την υλοποίηση τέτοιων πρακτικών.

Συμπερασματικά, βλέποντας συγκεντρωτικά όλες τις απαντήσεις που λήφθηκαν παρατηρούμε μια ανακολουθία μεταξύ τους, εκτός ίσως από τους μαθητές με αγαπημένο μάθημα την πληροφορική. Σε αυτό το σημείο θα πρέπει να λάβουμε υπόψη το νεαρό της ηλικίας των μαθητών. Οι απαντήσεις, όπως αυτές δόθηκαν, δείχνουν μια επιπολαιότητα στον τρόπο απάντησης. Όπως αναφέρθηκε και στο θεωρητικό κομμάτι της παρούσας εργασίας, αυτός ο τρόπος σκέψης είναι κάτι το αναμενόμενο από τους έφηβους, οπότε δεν πρέπει να προκαλούν έκπληξη οι απαντήσεις που έδωσαν ή ο τρόπος δικαιολόγησης των απαντήσεών τους. Επιπλέον, το αίσθημα ότι είναι αδιάτρητοι, που χαρακτηρίζει τα άτομα αυτών των ηλικιών, όπως και η υπερβολική αυτοπεποίθηση στην κατοχή των απαραίτητων γνώσεων σε θέματα πληροφορικής και τεχνολογίας τους καθιστά ευάλωτους να πέσουν θύματα επιθέσεων ηλεκτρονικού ψαρέματος, ακόμα και αν σε θεωρητικό επίπεδο μπορούν να διακρίνουν τους κινδύνους. Για μια πιο ολοκληρωμένη ματιά κρίνεται απαραίτητη η παρατήρηση των αντιδράσεών τους και σε ένα περιβάλλον προσομοίωσης, ούτως ώστε να προβούμε σε ασφαλή συμπεράσματα για την εξοικείωση τους με τους ηλεκτρονικούς κινδύνους.

4. Συμπεράσματα

Η καθημερινή και συνεχόμενη ένταξη του διαδικτύου στη ζωή μας αποτελεί γεγονός. Η ολοένα και σταδιακή μεταστροφή προς την εξ αποστάσεως εργασία, όπως και η παγκόσμια και μαζική χρήση των πλατφόρμων ηλεκτρονικής εκπαίδευσης κατά τη διάρκεια της πανδημίας του Covid-19 καθιστούν το διαδίκτυο κάτι παραπάνω από ένα σημαντικό εργαλείο. Η ένταξη αυτή όμως έρχεται με τους αντίστοιχα αυξανόμενους κινδύνους και απειλές. Αυτές εξελίσσονται με τη σειρά τους, με νέες μεθόδους, όπως και τρόπους απόκτησης προσωπικών δεδομένων και πληροφοριών επίδοξων θυμάτων, να αντικαθιστούν τις προηγούμενες. Οι έφηβοι, ειδικά, αποτελούν μια ιδιαίτερα ευάλωτη ομάδα. Λόγω του νεαρού της ηλικίας τους και της εκτεταμένης χρήσης του διαδικτύου, από αυτούς, μπορούν να πέσουν πιο συχνά θύματα ηλεκτρονικών επιθέσεων, των οποίων στόχος είναι οι προσωπικές πληροφορίες των ίδιων και των γονιών τους.

Το σχολείο, και ειδικά η δευτεροβάθμια εκπαίδευση, θα μπορούσε να επιτελέσει ένα πολύ σημαντικό ρόλο στην αντιμετώπιση αυτών των κινδύνων. Η δομή όμως και το περιεχόμενο του μαθήματος της πληροφορικής δεν επαρκεί από μόνο του για μια πιο ολιστική αντιμετώπιση των κινδύνων. Το γεγονός ότι μόνο το 34% των μαθητών του δείγματός μας ήξερε τι σημαίνει phishing, πιστοποιεί από μόνο του αυτήν την πρόταση. Επιπλέον, η έλλειψη συνεχούς επιμόρφωσης, όπως και οι μειωμένοι πόροι των σχολείων αποτελούν και αυτά τροχοπέδη στην επιμόρφωση και εξοικείωση των μαθητών με τα θέματα της ηλεκτρονικής ασφάλειας και του ηλεκτρονικού ψαρέματος. Η ένταξη νέου εξειδικευμένου μαθήματος, σεμιναρίων και τεχνικών προσομοίωσης θα μπορούσε ωστόσο να γεμίσει αυτό το κενό, τα οποία όμως προϋποθέτουν μια επαναπροσέγγιση και αναπροσαρμογή του γενικού προγράμματος σπουδών.

Όπως φάνηκε και από τις απαντήσεις των καθηγητών πληροφορικής, υπάρχουν οι γνώσεις όπως και η θέληση, από πλευράς των εκπαιδευτικών τουλάχιστον, μίας μορφής επέκτασης του αρχικού προγράμματος σπουδών του μαθήματος της πληροφορικής. Αυτό υποδηλώνει ότι αυτή τη στιγμή στο ελληνικό εκπαιδευτικό σύστημα υπάρχει μια, τουλάχιστον, ικανοποιητική έως μεγάλη, μερίδα του ανθρώπινου δυναμικού που θα μπορούσε να βοηθήσει προς την αύξηση της επίγνωσης των μαθητών πάνω σε θέματα ηλεκτρονικής ασφάλειας και προστασίας. Το γεγονός ότι

ήδη οι μαθητές με αγαπημένο μάθημα την πληροφορική είναι αισθητά πιο ενήμεροι και αυτοπροστατευμένοι από τους υπόλοιπους συμμαθητές τους απλώς ενισχύει αυτήν την πρόταση, με τα ποσοστά σωστών απαντήσεων που δόθηκαν από αυτούς να είναι αισθητά υψηλότερα από αυτά του συνολικού δείγματος. Αν οι εβδομαδιαίες ώρες πληροφορικής ήταν περισσότερες ή υπήρχε εξειδικευμένο μάθημα ή κάποιας μορφής σεμιναρίου ή προγράμματος πάνω στα ζητήματα ηλεκτρονικής ασφάλειας, μόνο να υποθέσει μπορεί κανείς τα γεωμετρικώς καλύτερα αποτελέσματα, όχι μόνο των μαθητών που τους ενδιαφέρει το μάθημα της πληροφορικής αλλά στο σύνολο του μαθητικού πληθυσμού.

Φυσικά εδώ προκύπτει και το ζήτημα της θέλησης, σε πολιτικό και διοικητικό επίπεδο, για την υλοποίηση τέτοιων προγραμμάτων, όπως και της εκπαιδευτικής και υλικής υποστήριξης των ίδιων των εκπαιδευτικών, καθώς, όπως ειπώθηκε, πέραν την θέλησης των εκπαιδευτικών για την επιτέλεση αυτού του έργου, απαιτείται και η κατάλληλη υποστήριξη και ο κατάλληλος εξοπλισμός των σχολικών μονάδων. Αν αυτό επιτευχθεί τότε το αποτέλεσμα δε θα είναι μόνο μαθητές εξοικειωμένοι με τα ζητήματα της ηλεκτρονικής ασφάλειας, αλλά και η εκπαίδευση και καλλιέργεια ενός αυριανού ανθρώπινου δυναμικού, που θα μπορούσε να δραστηριοποιηθεί έμπρακτα και ενεργά σε αυτόν τον τομέα.

Βιβλιογραφία

- [1]. Alwanain, M. I. (2021). How Do Children Interact with Phishing Attacks? *IJCSNS International Journal of Computer Science and Network Security*, pp. 127–133.
- [2]. Cyber Innovation Center. (2020). *The State of Cybersecurity Education in K-12 Schools*. Retrieved from <https://cyber.org/news/state-cybersecurity-education-k-12-schools>
- [3]. Facebook. (n.d.). Retrieved from <https://www.facebook.com/>
- [4]. Frauenstein, E. D. (2018). An Investigation Into Students Responses to Various Phishing Emails and Other Phishing-Related Behaviours. *Information Security for South Africa*, pp. 49-64.
- [5]. Hacker Academy. (n.d.). Retrieved from <https://www.hackeracademy.org/how-to-hack-facebook-by-creating-a-custom-phishing-page/>
- [6]. Hanafi, A., Hanafia, A., Rokmana, H., Ibrahim, Z.-A., Zawawi, M., & Rahimb, F. (2021). Scenario CTF-Based Approach in Cybersecurity Education for Secondary School Students. *electronic Journal of Computer Science and Information Technology*, pp. 1-8.
- [7]. Javidi, G., & Sheybani, E. (2018). K-12 Cybersecurity Education, Research, and Outreach. *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1-5.
- [8]. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M., & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security*, pp. 1-12.
- [9]. Lastdrager, E., Carvajal Gallardo, I., Hartel, P., & Junger, M. (2017). How Effective is {Anti-Phishing} Training for Children? *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pp. 229--239.
- [10]. Microsoft. (2019). *The quiet evolution of phishing*. Retrieved from <https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/>
- [11]. Mountroudou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., . . . Yuen, T. T. (2019). Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, pp. 157-176.
- [12]. Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P. (2020). Investigating Teenagers' Ability to Detect Phishing Messages. *2020 IEEE European Symposium on Security and Privacy Workshops*, pp. 140-149.
- [13]. Online Education. (n.d.). *Student Guide to Phishing Attacks*. Retrieved from <https://www.onlineeducation.com/features/student-guide-to-phishing-attacks>

- [14]. Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy*, pp. 68-74.
- [15]. phishing.org. (n.d.). *History of Phishing*. Retrieved from <https://www.phishing.org/history-of-phishing>
- [16]. Quora. (n.d.). Retrieved from <https://www.quora.com/What-is-the-URL-of-a-phishing-page-on-Facebook>.
- [17]. saferinternet4kids.gr. (n.d.). Retrieved from <https://saferinternet4kids.gr/>
- [18]. Samsel, H. (2020). *Schools Could Face Increase in Phishing Attacks Targeting Staff, Students and Parents*. Retrieved from <https://campuslifesecurity.com/articles/2020/05/06/schools-could-face-increase-in-phishing-attacks-targeting-staff-students-and-parents.aspx>
- [19]. Softpedia News. (n.d.). Retrieved from https://news.softpedia.com/news/Your-Apple-ID-Frozen-Phishing-Emails-Come-as-Users-Upgrade-to-Mavericks-394301.shtml#sgal_0
- [20]. Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pp. 223-228.
- [21]. Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. (2019). Cyber security education is as essential as “the three R's”. *Heliyon*, pp. 1-8.
- [22]. Weanquoi, P., Johnson, J., & Zhang, J. (2018). Using a Game to Improve Phishing Awareness. *Journal of Cybersecurity Education, Research and Practice*, pp. 1-14.