ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων

ΠΟΛΥΜΕΣΙΚΟ ΥΛΙΚΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Αθανασία Τζιώλη

Η εργασία υποβάλλεται για τη μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του Μεταπτυχιακού Διπλώματος Σπουδών στη Διδακτική της Τεχνολογίας και τα Ψηφιακά Συστήματα

Ιανουάριος 2013

ΠΕΡΙΛΗΨΗ

Παρά το γεγονός ότι το Διαδίκτυο συνθέτει ένα χώρο που προσφέρει ικανοποίηση στους μαθητές, ωστόσο οι πιθανοί κίνδυνοι που ενέχει για την ιδιωτική ζωή και την προσωπική τους ασφάλεια είναι πάρα πολλοί. Γι' αυτό το λόγο οι μαθητές χρειάζεται να ενημερωθούν σχετικά με τους κινδύνους που ελλοχεύουν πριν την απόκτηση πρόσβασης στο Διαδίκτυο.

Η παρούσα έρευνα έχει ως στόχο αρχικά την ενημέρωση των εκπαιδευτικών για την ασφάλεια στο διαδίκτυο με τη συνδρομή πολυμεσικού υποστηρικτικού υλικού η οποία διευκολύνεται μέσα από μια ιστοσελίδα, το όνομα της οποίας είναι BEsafe, όπου παρουσιάζονται ιδέες για δραστηριότητες τόσο σε εκπαιδευτικούς όσο και σε γονείς ώστε να βοηθήσουν τους μαθητές να κατανοήσουν και να οχυρωθούν απέναντι στους κινδύνους που ενέχει το διαδίκτυο. Επίσης, η εν λόγω ιστοσελίδα περιέχει συνοδευτικό υλικό μιας άλλης δικτυακής τοποθεσίας, δηλαδή της www.safesocialmedia.org.

Αρχικά, αναλύεται ο τρόπος και τα μέσα που χρησιμοποιήθηκαν για τη δημιουργία του συγκεκριμένου ιστοτόπου, του BEsafe. Συγκεκριμένα, ο ιστότοπος αυτός περιέχει υλικό που απευθύνεται σε τρεις κατηγορίες χρηστών, δηλαδή στα παιδιά, στους εκπαιδευτικούς και στους γονείς, από όπου η κάθε μια κατηγορία μπορεί να λάβει τις απαραίτητες γνώσεις σχετικά με το θέμα της «Ασφαλής χρήσης του Διαδικτύου». Στο πλαίσιο αυτής της έρευνας, χρησιμοποιήθηκε ως ερευνητικό εργαλείο ένα ερωτηματολόγιο κλίμακας Likert το οποίο απαντήθηκε από μια ομάδα εκπαιδευτικών, έτσι ώστε να συγκεντρωθούν τα κατάλληλα αποτελέσματα για τη βελτίωση των δυο ιστοτόπων. Σύμφωνα με τα αποτελέσματα που προέκυψαν κατόπιν της ανάλυσης του ερωτηματολογίου, προκύπτει το συμπέρασμα πως οι δύο αυτοί ιστότοποι καλύπτουν επαρκώς τις ανάγκες των εκπαιδευτικών σχετικά με την ενημέρωσή εκείνων αλλά και των παιδιών και των γονέων για το συγκεκριμένο ζήτημα.

Τέλος, η έρευνα αυτή παρέχει προτάσεις για μελλοντική έρευνα. Συγκεκριμένα, προτείνεται η επίσκεψη σε σχολεία όπου και θα παρουσιαστούν οι ιστότοποι αρχικά στους εκπαιδευτικούς και εν συνεχεία στους γονείς και στα παιδιά, έτσι ώστε να λάβουν ανατροφοδότηση για τυχόν βελτίωση των ιστοτόπων.

ABSTRACT

Notwithstanding the fact that the Internet is broadly acknowledged as a fascinating place for young students to wander around and indulge in, it concomitantly poses great risks to their privacy and personal security. Based on this perspective, students need to be soundly informed about the dangers involved before accessing it.

The present research work is principally aimed at informing educators about internet safety through multimedia-enhanced, supportive material, facilitated by a website, titled 'BEsafe'. In this website, ideas for innovative activities, targeted at both educators and parents so as to help young students comprehend and fortify themselves against the potential dangers posed by the Internet, are extensively offered. Supportive material for another website, titled 'Safe Social Media' (www.safesocialmedia.org), is also encompassed in 'BEsafe'.

Initially, the architecture and the resources employed to create the 'BEsafe' website are thoroughly presented. The proposed website includes material intended for use by three types of users, namely children, teachers and parents, who can profit immensely from enriching their knowledge regarding the issue of 'Safe Internet use'. A typical Likert-scale questionnaire has served as the research tool within the context of this thesis, in order to gather data central to improving the aforementioned sites. According to the results obtained through the analysis of the questionnaire, answered by teachers, it could be stated that these two sites satisfy teachers', students' and parents' needs in terms of the Internet safety issue sufficiently.

Finally, suggestions for further research are discussed within this thesis. In more specific terms, a visit to a school, where the abovementioned websites will be presented to teachers, parents and children, is proposed to enable the provision of constructive feedback that can tremendously assist their being improved.

ΕΥΧΑΡΙΣΤΙΕΣ

Δε θα ήταν δυνατόν να γράψω αυτή τη θέση χωρίς τη βοήθεια και την υποστήριξη κάποιων πολύ σημαντικών ανθρώπων γύρω μου.

Πάνω απ 'όλα, θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή, κ. Συμεών Ρετάλη για την εξαιρετική συνεργασία που είχαμε, και ελπίζω να συνεχίσουμε να έχουμε στο μέλλον. Τον ευχαριστώ θερμά για την εξαιρετική καθοδήγηση, την ατελείωτη υπομονή και κατανόηση που μου προσέφερε σε όλη τη διάρκεια των μεταπτυχιακών μου σπουδών τα οποία συνέβαλαν σημαντικά και στην υλοποίηση της διπλωματικής μου εργασίας.

Θα ήθελα επίσης να εκφράσω την εκτίμησή μου προς τον Αναπληρωτή Καθηγητή, κ. Δημήτριο Σάμψων, ο οποίος με καθοδήγησε στο πολύ ενδιαφέρον και ευρύ αντικείμενο της ηλεκτρονικής μάθησης και ο οποίος κατά τη διάρκεια της διδασκαλίας του μου μετέφερε το πάθος του σχετικά με την έρευνα.

Επιπλέον, θα ήθελα να ευχαριστήσω την Επίκουρη Καθηγήτρια, κα Φωτεινή Παρασκευά για τις πολύτιμες γνώσεις που μου μετέδωσε κατά τη διάρκεια των μεταπτυχιακών μου σπουδών. Ελπίζω να συνεχίζει με τον ίδιο τρόπο και με τον ίδιο ενθουσιασμό να υποστηρίζει τους φοιτητές της.

Θα ήθελα, επίσης, να ευχαριστήσω όλους τους εκπαιδευτικούς, οι οποίοι κατανάλωσαν χρόνο και βοήθησαν στη συμπλήρωση του ερωτηματολογίου. Αυτοί αποτελούν τους κύριους συντελεστές της συγκεκριμένης έρευνας.

Ευχαριστίες οφείλονται επίσης σε όλους τους ανθρώπους που συμμετέχουν ενεργά στην ολοκλήρωση της έρευνάς μου. Οι άνθρωποι που δέχτηκαν με μεγάλη προθυμία να συμμετάσχουν αλλά και για την ενθάρρυνση τους στο πρόσωπό μου σε όλη αυτή τη διάρκεια είναι ο Άκης, ο Νίκος, η Χριστίνα και η Χριστίνα. Θα ήθελα, επίσης, να ευχαριστήσω τους φίλους μου που μου συμπαραστάθηκαν σε όλη τη διάρκεια των σπουδών μου.

Σε καμία περίπτωση δε θα ήμουν σε θέση να ολοκληρώσω τη διπλωματική μου εργασία χωρίς την αμέριστη υποστήριξη της οικογένειάς μου. Ευχαριστώ θερμά τον πατέρα μου, Αποστόλη, τη μητέρα μου, Μαρία και την αδελφή μου, Γιώτα, για τη μεγάλη τους αγάπη, κατανόηση και υπομονή που μου έδειξαν κατά τη διάρκεια ολοκλήρωσης όλων των σπουδών μου, των οποίων η πίστη στις δυνατότητες μου αποτέλεσε αρωγό σε όλους τους στόχους και τα όνειρά μου, για τους οποίους μια απλή αναφορά μου στις ευχαριστίες, φυσικά και δεν αρκεί.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Η αξία της άρτιας ενημέρωσης για ασφαλή πλοήγηση στο Διαδίκτυο

Μολονότι το Διαδίκτυο συνθέτει ένα χώρο που προσφέρει ικανοποίηση στους μαθητές, ωστόσο οι πιθανοί κίνδυνοι που ενέχει για την ιδιωτική ζωή και την προσωπική τους ασφάλεια είναι υπαρκτοί. Κατά τη διάρκεια της περιήγησης τους στο διαδίκτυο, είναι πιθανό οι μαθητές να έρθουν αντιμέτωποι με ενοχλητικές πληροφορίες και εικόνες ή απερίσκεπτα να αποδεχθούν και να διαμοιραστούν αρχεία που εκθέτουν πληροφορίες ζωτικής σημασίας σε απατεώνες του Διαδικτύου. Ενδέχεται να αποδεχτούν άθελα τους κακόβουλο λογισμικό που μπορεί να καταστρέψει, να σβήσει ή να αντιγράψει δεδομένα. Ενδέχεται επίσης να αντιμετωπίσουν εκφοβισμό μέσω Διαδικτύου, από άτομα που επιθυμούν να τους φέρουν σε δύσκολη θέση ή να τους φοβίσουν. Στη χειρότερη περίπτωση, υπάρχει το ενδεχόμενο επικοινωνίας με απαγωγείς παιδιών χωρίς καν να το αντιληφθούν. Τα άτομα αυτά χρησιμοποιούν το Διαδίκτυο ώστε να προσεγγίσουν ευάλωτα παιδιά, υποκρινόμενα πως είναι κάποιο άλλο παιδί ή κάποιος έμπιστος ενήλικας και στη συνέχεια προσπαθούν να τα πείσουν να συναντηθούν πρόσωπο με πρόσωπο. Η λίστα των κινδύνων που μπορεί να συναντήσει ένα μαθητής κατά την περιδιάβαση του στο Διαδίκτυο είναι ανεξάντλητη.

Στόχος είναι οι θετικές εμπειρίες που απορρέουν από τη χρήση του Διαδικτύου να αντισταθμίσουν τους κινδύνους, μέσω της υιοθέτησης ρεαλιστικών και επιτεύξιμων μεθόδων. Υπάρχουν διαθέσιμα εργαλεία που μπορούν να συνδράμουν γονείς και εκπαιδευτικούς στη δημιουργία ενός ασφαλέστερου διαδικτυακού περιβάλλοντος, αν και η έλλειψη γνώσεων σχετικών με τους κινδύνους, ελαχιστοποιούν την αποτελεσματικότητα των εργαλείων αυτών. Οι μαθητές χρειάζεται να ενημερωθούν σχετικά με τους κινδύνους που ελλοχεύουν πριν την απόκτηση πρόσβασης στο Διαδίκτυο. Στην περίπτωση που δεν παρέχονται επαρκείς πληροφορίες στους μαθητές, ή οι ασφαλείς πρακτικές πλοήγησης που εφαρμόζονται στο πλαίσιο της σχολικής εκπαίδευσης δε μεταφέρονται στο σπίτι, το παιδί εξακολουθεί να τίθεται σε κίνδυνο. Τούτων λεχθέντων, η χρήση μιας και μόνο μεθόδου προστασίας δεν επαρκεί για την παροχή ασφάλειας στο Διαδίκτυο για τους

μαθητές. Δυστυχώς, η έλλειψη παιδείας σχετικά με το εν λόγω ζήτημα δίνει στους γονείς και στους εκπαιδευτικούς την ψευδαίσθηση πως μια μέθοδος προστασίας είναι ο μοναδικός τρόπος προστασίας και απομάκρυνσης των παιδιών από τους κινδύνους του Διαδικτύου. Η απουσία γνώσης, κατά συνέπεια, οδηγεί γονείς και εκπαιδευτικούς στη μείωση του χρόνου παραμονής των μαθητών στο Διαδίκτυο ή στο άλλο άκρο, δηλαδή στην άκριτη και αλόγιστη πλοήγηση τους σε αυτό.

Το γεγονός ότι διαπράττονται εγκλήματα στο Διαδίκτυο δεν αποτελεί λόγο για την αποφυγή χρήσης των υπηρεσιών που προσφέρει. Το να ζητήσει κανείς από ένα παιδί να σταματήσει να χρησιμοποιεί το Διαδίκτυο θα μπορούσε να παρομοιαστεί με το να ζητήσει κανείς από το παιδί να μη φύγει από το σπίτι λόγω των κινδύνων που παραμονεύουν στον έξω κόσμο. Από την άλλη πλευρά, το να επιτραπεί σε ένα παιδί η αλόγιστη χρήση του Διαδικτύου παρουσιάζει αρκετά κοινά στοιχεία με την περίπτωση κατά την οποία επιτρέπεται στο παιδί να βγει από το σπίτι για πρώτη φορά χωρίς καθοδήγηση ή υποστήριξη. Μια στρατηγική προς τη κατεύθυνση αυτή είναι η ενημέρωση των παιδιών σχετικά με τα οφέλη και τους κινδύνους που επιφυλάσσει το Διαδίκτυο. Κατόπιν συζήτησης με αρκετούς εκπαιδευτικούς και γονείς, είναι εύκολο να αντιληφθεί κανείς πως οι τελευταίοι βρίσκονται σε σύγχυση όσον αφορά στην απουσία ελέγχου καθώς δε γνωρίζουν μεθόδους με τις οποίες μπορούν να εξασφαλίσουν την πρόσβαση των παιδιών τους στο Διαδίκτυο με ασφάλεια και υπευθυνότητα.

1.2 Στόχος της εργασίας

Η παρούσα έρευνα έχει ως στόχο την ενημέρωση των εκπαιδευτικών για την ασφάλεια στο διαδίκτυο με τη συνδρομή πολυμεσικού υποστηρικτικού υλικού η οποία διευκολύνεται μέσα από μια ιστοσελίδα, το όνομα της οποίας είναι BEsafe, όπου παρουσιάζονται ιδέες για δραστηριότητες τόσο σε εκπαιδευτικούς όσο και σε γονείς ώστε να βοηθήσουν τους μαθητές να κατανοήσουν και να οχυρωθούν απέναντι στους κινδύνους που ενέχει το διαδίκτυο.

Επίσης, η εν λόγω ιστοσελίδα περιέχει συνοδευτικό υλικό μιας άλλης δικτυακής τοποθεσίας, δηλαδή της www.safesocialmedia.org. Η τοποθεσία αυτή στοχεύει στην καταπολέμηση της βίας των μέσων κοινωνικής δικτύωσης και στην ενίσχυση της επίγνωσης των παιδιών, των εκπαιδευτικών και των γονέων σχετικά με

τους κινδύνους των μέσων αυτών. Επίσης, αποσκοπεί στην ενημέρωσή τους σε ό, τι αφορά την ασφαλή τους χρήση. Συγκεκριμένα, σχετίζεται με:

1. Δημιουργία ψηφιακών μαθησιακών αντικειμένων σε όλες τις γλώσσες των εταίρων (Ελληνικά, Αυστριακά, Ιταλικά και Αγγλικά) για τους τρόπους προστασίας και καταπολέμησης ενάντια στους κινδύνους των εφαρμογών κοινωνικής δικτύωσης.

2. Ανάπτυξη σχεδίων μαθήματος που θα συνοδεύουν τα ψηφιακά μαθησιακά αντικείμενα, ώστε οι εκπαιδευτικοί στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση να μπορούν να τα χρησιμοποιήσουν στην τάξη. Επίσης, η δημιουργία των σχεδίων μαθήματος θα μπορούσε να αξιοποιηθεί και για την εκπαίδευση των γονέων.

3. Οργάνωση εργαστηρίων, ημερίδων και ειδικών εκδηλώσεων για την εκπαίδευση των γονέων από τους εκπαιδευτικούς πρόσωπο με πρόσωπο ώστε να ενημερώνονται καλύτερα τα παιδιά τους σχετικά με τους τρόπους που μπορούν να προστατευθούν από τους κινδύνους των εφαρμογών κοινωνικής δικτύωσης.

4. Διεξαγωγή δραστηριοτήτων διάδοσης αξιοποιώντας παραδοσιακά (φυλλάδια, σεμινάρια, δελτία τύπου) και ιδιαίτερα διαδικτυακά μέσα κοινωνικής δικτύωσης.

5. Δημιουργία επαφών με άλλα συναφή προγράμματα και πρωτοβουλίες των ΜΚΟ, με οργανισμούς κατάρτισης, με συλλόγους εκπαιδευτικών και με τα υπουργεία παιδείας.

1.3 Δομή της εργασίας

Η εργασία οργανώνεται στα πέντε παρακάτω κεφάλαια:

- Κεφάλαιο 1: Το κεφάλαιο αυτό αποτελεί τη βάση για την έρευνα, στο οποίο επισημαίνεται η αξία της άρτιας ενημέρωσης για την ασφαλή πλοήγηση στο Διαδίκτυο η οποία αποτέλεσε το κίνητρο για τη συγγραφή της παρούσας εργασίας, ο στόχος της έρευνας καθώς και ο τρόπος με τον οποίο δομήθηκε η εργασία.
- Κεφάλαιο 2: Το κεφάλαιο αυτό εξετάζει την υπάρχουσα σχετική βιβλιογραφία όσον αφορά στο θέμα της Ασφαλής χρήσης του Διαδικτύου. Αρχικά, γίνεται αναφορά στο Διαδίκτυο, και συγκεκριμένα στα πλεονεκτήματα και μειονεκτήματά του καθώς και στις υπηρεσίες και εφαρμογές που παρέχει στο κοινό. Στη συνέχεια, αναλύεται ο όρος ασφάλεια στο Διαδίκτυο και με ποιον

τρόπο επηρεάζει την κάθε κατηγορία (εκπαιδευτικοί, γονείς, παιδιά). Επίσης, αναφέρονται οι κίνδυνοι που παραμονεύουν στο διαδίκτυο καθώς και οι τρόποι προστασίας από αυτούς. Τέλος, γίνεται εκτενής αναφορά για την υφιστάμενη κατάσταση του φαινομένου στην Ελλάδα και στο εξωτερικό.

- Κεφάλαιο 3: Το κεφάλαιο αυτό ξεκινά με μια υπενθύμιση του σκοπού της έρευνας. Αρχικά, περιγράφει την ερευνητική μέθοδο, το δείγμα που χρησιμοποιήθηκε για την αξιολόγηση, τα υλικά και τα ερευνητικά εργαλεία που χρησιμοποιούνται για τη συλλογή στοιχείων στο πλαίσιο της παρούσας έρευνας. Στο υπόλοιπο μέρος του κεφαλαίου, γίνεται εκτενής ανάλυση του τρόπου ανάπτυξης της εκπαιδευτικής ιστοσελίδας "BEsafe".
- Κεφάλαιο 4: Το συγκεκριμένο κεφάλαιο πραγματεύεται τα αποτελέσματα που συγκεντρώθηκαν από το ερωτηματολόγιο, τα οποία και αναλύονται.
- Κεφάλαιο 5: Στο κεφάλαιο αυτό ολοκληρώνεται η έρευνα με μια γενική επισκόπηση και συζήτηση σχετικά με τα αποτελέσματα που προέκυψαν από το προηγούμενο κεφάλαιο καθώς και οι προτάσεις για μελλοντική έρευνα.

ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Εισαγωγή – Διαδίκτυο

Διαδίκτυο (Internet) είναι το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο (**Inter**national **Net**work). Αποτελείται από εκατομμύρια διασυνδεδεμένους υπολογιστές και εκτείνεται σχεδόν σε κάθε σημείο του πλανήτη, παρέχοντας τις υπηρεσίες του σε εκατομμύρια χρήστες.

Το διαδίκτυο είναι πραγματικά ένα εργαλείο όπου μικρής και μεγάλης ηλικίας χρήστες μπορούν να βρεθούν σε έναν απέραντο εικονικό χώρο γεμάτο εκατομμύρια πληροφορίες. Μπορούν να ασχοληθούν με παιχνίδια, να αναζητήσουν πληροφορίες, να αλληλογραφήσουν και να συνομιλήσουν, να βρουν αρχεία κάθε είδους. Με τη συνεχή εξέλιξη των νέων τεχνολογιών, οι χρήστες του διαδικτύου είναι πια σε θέση να πραγματοποιούν ηλεκτρονικές αγορές, συναλλαγές με το Δημόσιο και τις τράπεζες και να ασχοληθούν με την εκπαίδευση και την εργασία εξ αποστάσεως. Όλα τα παραπάνω οι ανήλικοι τα κάνουν συνήθως χωρίς επίβλεψη, με μια ελευθερία που δεν υπάρχει στην πραγματική τους ζωή. Για το θέμα των κινδύνων που εγκυμονούν στο διαδίκτυο έχουν γραφεί τα τελευταία χρόνια πολλά άρθρα. Κανείς δεν ξέρει που σταματάει η αλήθεια και πού αρχίζει η υπερβολή. Αναμφίβολα το διαδίκτυο εξασκεί μεγάλη γοητεία σε άτομα όλων των ηλικιών και οι λόγοι είναι κατανοητοί (Μυλωνάς, 2009).

2.1.1 Πλεονεκτήματα του διαδικτύου

Αναμφίβολα ο χρήστης μπορεί να αντλήσει από το διαδίκτυο πολλές χρήσιμες πληροφορίες. Αυτό όμως κρύβει και τις σκοτεινές πλευρές του. Ένας ενήλικας μπορεί να κρίνει και να αποφύγει τους κινδύνους που κρύβει το διαδίκτυο, για ένα παιδί, όμως, τα πράγματα είναι τελείως διαφορετικά. Ο ενήλικας, γονιός είτε εκπαιδευτικός, έχει μεγάλη ευθύνη να το προστατεύσει και η ευθύνη επεκτείνεται σε όλη την κοινωνία. Η προστασία αυτή δεν είναι απλή υπόθεση. Η λύση δεν είναι ούτε η πλήρης απαγόρευση της πρόσβασης στο διαδίκτυο ούτε η απουσία οποιασδήποτε επιτήρησης. Είναι πολύ σημαντικό να αναφερθούν τα θετικά και τα αρνητικά του διαδικτύου προτού γίνει μια εκτενής αναφορά σε αυτό το ζήτημα (Μυλωνάς, 2009).

Τα βασικά πλεονεκτήματα της χρήσης του διαδικτύου μπορούν να κατηγοριοποιηθούν στα εξής:

i) Επικοινωνία

Ο πρώτιστος στόχος του διαδικτύου είναι πάντα η επικοινωνία και το διαδίκτυο υπερέχει σε αυτό και έχει ξεπεράσει τις προσδοκίες. Οι μελέτες και οι έρευνες έχουν στόχο τις καινοτομίες που πρόκειται να το καταστήσουν γρηγορότερο και πιο αξιόπιστο. Τώρα η επικοινωνία γίνεται σε ένα κλάσμα του δευτερολέπτου με ένα πρόσωπο που κάθεται στο άλλο μέρος του κόσμου. Σήμερα για την καλύτερη επικοινωνία, μπορούν να χρησιμοποιηθούν οι υπηρεσίες του ηλεκτρονικού ταχυδρομείου. Υπάρχουν πάρα πολλές υπηρεσίες για επικοινωνία, με τις οποίες έχει γίνει πολύ εύκολη η καθιέρωση της παγκόσμιας φιλίας όπου μπορούν να μοιραστούν οι σκέψεις του καθενός και να ερευνηθούν πολιτισμοί διαφορετικού έθνους.

ii) Πληροφορίες

Οι πληροφορίες είναι πιθανώς το μεγαλύτερο πλεονέκτημα του διαδικτύου διότι είναι ένας εικονικός θησαυρός πληροφοριών. Οποιοδήποτε είδος πληροφοριών για οποιοδήποτε θέμα είναι διαθέσιμο στο διαδίκτυο. Μπορεί να βρεθεί σχεδόν οποιοδήποτε τύπο στοιχείων όσον αφορά οποιοδήποτε είδος θέματος που ψάχνει ο καθένας. Υπάρχει ένα τεράστιο ποσό πληροφοριών διαθέσιμο στο διαδίκτυο για κάθε θέμα που είναι γνωστό στον άνθρωπο, που επεκτείνεται από τον κυβερνητικό νόμο και τις υπηρεσίες του, τις εμπορικές εκθέσεις και τις διασκέψεις, πληροφορίες αγοράς, νέες ιδέες και τεχνική υποστήριξη, ο κατάλογος είναι ατελείωτος. Οι σπουδαστές και τα παιδιά είναι μεταξύ των χρηστών που κάνουν πλοήγηση στο διαδίκτυο για την έρευνα. Σήμερα, σχεδόν απαιτείται ότι οι σπουδαστές πρέπει να χρησιμοποιήσουν το διαδίκτυο για την έρευνα με σκοπό τη συλλογή στοιχείων. Οι καθηγητές έχουν αρχίσει τις αναθέσεις που απαιτούν την έρευνα στο διαδίκτυο.

iii) Ψυχαγωγία

Η ψυχαγωγία είναι ένα δημοφιλές ερέθισμα γιατί πολλοί άνθρωποι προτιμούν να κάνουν απλά πλοήγηση και αναζήτηση στο διαδίκτυο. Τα μέσα του διαδικτύου έχουν γίνει αρκετά επιτυχή στο θέμα της ψυχαγωγίας. Η λήψη (downloading) των παιχνιδιών, η επίσκεψη στα δωμάτια συνομιλίας ή απλά το «surfing» στο διαδίκτυο είναι μερικές από τις χρήσεις που έχουν ανακαλύψει. Υπάρχουν πολυάριθμα παιχνίδια που μπορούν να ληφθούν από το διαδίκτυο δωρεάν. Η βιομηχανία του online τυχερού παιχνιδιού (τζόγου) έχει εγκλωβίσει δραματικά τους εραστές αυτών

των παιχνιδιών. Στην Ελλάδα τα δωμάτια συνομιλίας είναι τα πιο δημοφιλή επειδή οι χρήστες μπορούν να συναντήσουν εικονικά άλλους ενδιαφέροντες ανθρώπους. Η πλοήγηση στο διαδίκτυο μπορεί να προσφέρει πολυάριθμα πράγματα για λήψη στον προσωπικό υπολογιστή. Η μουσική, τα χόμπι, οι ειδήσεις και άλλα περισσότερα μπορούν να βρεθούν και να διαμοιραστούν στο διαδίκτυο.

2.1.2 Μειονεκτήματα του διαδικτύου

Το Διαδίκτυο, όπως αναφέρθηκε και παραπάνω, προσφέρει στα παιδιά και τους νέους απίθανες ευκαιρίες να ανακαλύπτουν, να συνδέονται και να δημιουργούν ηλεκτρονικά. Ωστόσο, η χρήση του Διαδικτύου ενέχει και κινδύνους. Για παράδειγμα, είναι ένα ανοιχτό παράθυρο σε έναν κόσμο που συμμετέχουν και οι ενήλικοι και περιέχει υλικό ακατάλληλο για τα παιδιά.

Συγκεκριμένα υποβόσκουν αρκετοί κίνδυνοι, όπως η έκθεση σε υλικό το οποίο χαρακτηρίζεται πορνογραφικό, βίαιο, ρατσιστικό ή γενικά προσβλητικό, που προωθεί το μίσος και την επιθετικότητα. Οι νέοι, τα παιδιά και οι έφηβοι αποτελούν την πιο δυναμική ομάδα στο διαδίκτυο. Οι γνώσεις τους κατά κανόνα ξεπερνούν τις γνώσεις των γονέων τους. Γι' αυτό είναι απαραίτητο όχι μόνο αντι-ικά προγράμματα και αναχώματα ασφάλειας αλλά και φιλτράρισμα περιεχομένου (content filtering) σε συνδυασμό με το γονικό έλεγχο (parental control) για τους ανήλικους χρήστες.(Μακροβασίλης, 2007)

Στη συνέχεια θα αναφερθούν μερικά από τα κυριότερα μειονεκτήματα της χρήσης του διαδικτύου.

i) Κλοπή προσωπικών στοιχείων

Όταν κάποιος χρησιμοποιεί το διαδίκτυο, μπορεί να αντιμετωπίσει το σοβαρό κίνδυνο κλοπής των δεδομένων του, των προσωπικών πληροφοριών του όπως το όνομα, τη διεύθυνση, οι αριθμοί των πιστωτικών καρτών του κ.λπ

ii) Spamming

Το Spamming αναφέρεται στην αποστολή ανεπιθύμητων ηλεκτρονικών emails σε μεγάλη ποσότητα, τα οποία δεν παρέχουν κανένα σκοπό και εμποδίζουν την ορθή λειτουργία του συστήματος. Τέτοιες παράνομες δραστηριότητες μπορούν να είναι πολύ απογοητευτικές, και δεν πρέπει απλώς να αγνοούνται από τον κάθε χρήστη αλλά πρέπει να καταβληθεί προσπάθεια να σταματήσουν αυτές τις

δραστηριότητες έτσι ώστε η χρησιμοποίηση του διαδικτύου να μπορεί να γίνει ασφαλέστερη.

iii) Απειλή ιών

Ο ιός δεν είναι παρά ένα πρόγραμμα που εμποδίζει την κανονική λειτουργία των συστημάτων και των ηλεκτρονικών υπολογιστών. Οι υπολογιστές που συνδέονται με το διαδίκτυο είναι περισσότερο ευάλωτοι σε επιθέσεις ιών και μπορούν ακόμα να καταλήξουν στην καταστροφή ολόκληρου του σκληρού δίσκου.

iv) Πορνογραφία

Αυτή είναι ίσως η μεγαλύτερη απειλή σχετικά με την υγιή διανοητική ζωή των παιδιών. Ένα πολύ σοβαρό ζήτημα σχετικά με το διαδίκτυο. Υπάρχουν χιλιάδες πορνογραφικές περιοχές στο διαδίκτυο που μπορούν να βρεθούν εύκολα και μπορούν να είναι ένας καταστρεπτικός παράγοντας όταν τα παιδιά χρησιμοποιούν το διαδίκτυο χωρίς έλεγχο.

2.1.3 Υπηρεσίες του διαδικτύου

Ένα «Παγκόσμιο Ηλεκτρονικό Χωριό», όπως το Διαδίκτυο, δεν μπορεί παρά να είναι πολύ καλά οργανωμένο και να παρέχει στους κατοίκους του διάφορες υπηρεσίες, για να διευκολύνει την καθημερινότητά τους, ακριβώς όπως θα συνέβαινε και σε ένα πραγματικό χωριό.

Έτσι λοιπόν στο Διαδίκτυο συναντάμε κάποιες από τις βασικότερες υπηρεσίες, όπως:

- Ηλεκτρονικό ταχυδρομείο μέσω του οποίου οι χρήστες ανταλλάσουν γραπτά μηνύματα και αρχεία (email).
- Ηλεκτρονικά καταστήματα διαφόρων ειδών από όπου οι χρήστες μπορούν να ψωνίσουν χρησιμοποιώντας την πιστωτική τους κάρτα (eshops).
- Ηλεκτρονικά «δωμάτια» συνάντησης όπου οι χρήστες συναντιούνται και επικοινωνούν σε πραγματικό κυρίως χρόνο χρησιμοποιώντας είτε γραπτά μηνύματα είτε απευθείας συνομιλία (chat rooms).
- Ηλεκτρονικά μουσεία τα οποία μπορούν οι χρήστες να επισκεφτούν από οποιοδήποτε μέρος του πλανήτη, να περιηγηθούν σε αυτά και να δουν τα εκθέματά τους (emuseums).
- Ηλεκτρονικές βιβλιοθήκες όπου οι χρήστες μπορούν να αναζητήσουν και να διαβάσουν σε ηλεκτρονική μορφή (elibraries).

- Παιχνίδια με σενάριο στα οποία ο χρήστης που συνδέεται παίρνει ένα προσωπικό ρόλο και αλληλεπιδρά στο περιβάλλον του παιχνιδιού με τους υπόλοιπους απομακρυσμένους παίκτες καθώς και Διαδικτυακά παιχνίδια που παίζονται σε πραγματικό και όχι μόνο χρόνο (egames).
- Υπηρεσία η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα και χωρίς κόστος. Οι συνομιλίες αυτές γίνονται μέσω Ηλεκτρονικού Υπολογιστή συνδεδεμένου με το Διαδίκτυο ο οποίος διαθέτει μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό (voip).

2.1.4 Εφαρμογές του διαδικτύου

Οι Εφαρμογές Κοινωνικής Δικτύωσης (Social Networks) επιτρέπουν στους χρήστες να δημιουργούν προσωπικές σελίδες μέσω εικονικών διαδικτυακών προφίλ, στοχεύοντας στη δημιουργία on-line κοινοτήτων: ανθρώπων, δηλαδή, με κοινά ενδιαφέροντα και - ή δραστηριότητες. Οι χρήστες μπορούν να δημοσιοποιούν προσωπικές πληροφορίες, φωτογραφίες, βίντεο και μηνύματα τα οποία μπορούν να δουν και να σχολιάσουν οι φίλοι τους.

Μερικές από τις πιο γνωστές Εφαρμογές Κοινωνικής Δικτύωσης είναι:

- **Facebook** αποτελεί ένα δωρεάν Social Network στο οποίο οι χρήστες μπορούν να επικοινωνούν μέσω μηνυμάτων με τις επαφές τους και να τους ειδοποιούν όταν ανανεώνουν τις προσωπικές πληροφορίες τους. Παρέχει παιχνίδια και υπάρχει η δυνατότητα δημοσίευσης φωτογραφιών και βίντεο.
- **Twitter** αποτελεί ένα δωρεάν Social Network που επιτρέπει στους χρήστες να γράφουν σύντομα μηνύματα και να διαβάζουν τα μηνύματα άλλων χρηστών της υπηρεσίας (τα γνωστά ως tweets).
- **Youtube** αποτελεί ένα δημοφιλές Social Network το οποίο επιτρέπει αποθήκευση, αναζήτηση και αναπαραγωγή βίντεο. Τα εγγεγραμμένα μέλη αποθηκεύουν απεριόριστο αριθμό βίντεο (έως 15 λεπτά το ένα), αφήνουν σχόλια σε κάθε βίντεο, πατούν το κουμπί «Μου αρέσει» και βαθμολογούν σχόλια άλλων. Τα βίντεο μπορούν να τα δουν όλοι οι χρήστες και να πουν αν τους αρέσουν ή όχι. Για κάθε βίντεο φαίνεται ο αριθμός των μελών που το έχει δει, ώστε να φαίνονται τα πιο δημοφιλή.
- **MySpace** αποτελεί ένα αρκετά δημοφιλές Social Network, όπου κάθε χρήστης έχει τη δυνατότητα να διαμορφώσει το προφίλ του, αλλά και να έρθει

σε επικοινωνία με φίλους του και να μοιραστεί μαζί τους μηνύματα, φωτογραφίες, βίντεο κ.τ.λ. Οι χρήστες του Myspace μπορούν να ανεβάσουν μουσική και να δημιουργήσουν λίστες αναπαραγωγής.

2.2 Ασφάλεια στο Διαδίκτυο

Στην καθομιλουμένη γλώσσα, ασφάλεια είναι η κατάσταση εκείνη, στην οποία υπάρχει η αίσθηση ότι δεν υπάρχει κίνδυνος ή απειλή. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας. Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του.

Αλλά και στον ίδιο ευρύτερο επαγγελματικό κλάδο, η οπτική γωνία θεωρήσεως του όρου ασφάλεια είναι εντελώς διαφορετική. Έτσι π.χ. διαφορετικά αντιλαμβάνεται τον όρο «ασφάλεια» ο τεχνικός ασφάλειας δικτύων υπολογιστικών συστημάτων και διαφορετικά ο τεχνικός ασφάλειας τραπεζικών πληροφοριακών συστημάτων.

Σε κάθε περίπτωση όμως όλοι όσοι ασχολούνται με θέματα ασφάλειας, «συναντώνται» στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν τη σιγουριά και τη βεβαιότητα κατά την εξάσκηση του έργου τους.

Είναι ευνόητο βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες.

Καθώς λοιπόν το διαδίκτυο είναι πλέον ένα ισχυρότατο μαθησιακό εργαλείο, η ανάγκη ενημέρωσης εκπαιδευτικών αλλά και γονέων πάνω σε θέματα καλής και ασφαλούς χρήσης του κρίνεται ολοένα και πιο επιτακτική. Το καλύτερο «τείχος προστασίας» είναι η επαφή των γονέων και των εκπαιδευτικών με τα παιδιά. Εάν ο νέος για ο,τιδήποτε ασυνήθιστο εμφανισθεί στο διαδίκτυο, απευθύνεται σε αρμόδια άτομα της οικογένειας και του σχολείου του, τότε σε πολύ μεγάλο βαθμό θα προλαμβάνονται οι πιθανές αρνητικές επιπτώσεις.

2.2.1 Ασφάλεια στο Διαδίκτυο για τους εκπαιδευτικούς

Ποιος όμως πρέπει να είναι ο ρόλος του εκπαιδευτικού στη διαμόρφωση τάσεων και συμπεριφορών ασφαλούς χρήσης του διαδικτύου από την πλευρά των μαθητών;

Ο ρόλος του εκπαιδευτικού είναι να κάνει γνωστούς τους κινδύνους στους μαθητές και να τους εφοδιάσει με δεξιότητες, εργαλεία και διαδικασίες ασφαλούς χρήσης. Ένας εκπαιδευτικός που γνωρίζει καλά τους κινδύνους και τις στρατηγικές αντιμετώπισής τους καλείται να σταθεί δίπλα στο μαθητή ως συνοδοιπόρος και σύμβουλος των μαθητών στη χρήση του διαδικτύου μέσα και έξω από το σχολείο. Ο εκπαιδευτικός δεν πρέπει να αρκείται στην εποπτεία είτε με τη φυσική του παρουσία είτε με τεχνικά μέσα. Η χρήση των φίλτρων κατά την πλοήγηση στο διαδίκτυο, αν και απαραίτητη στις μικρές ηλικίες, μπορεί να δράσει μόνο επικουρικά (Valcke et al. 2007).

Ουσιαστικά πρώτη γραμμή άμυνας στους κινδύνους από τη χρήση του διαδικτύου και των νέων μέσων επικοινωνίας είναι ο ίδιος ο μαθητής. Αποτελεί λοιπόν ανάγκη, πρωτίστως, ο εκπαιδευτικός να κατανοήσει τις ανάγκες των μαθητών που αφορούν στη χρήση του διαδικτύου και στη συνέχεια να τους ενθαρρύνει να μοιραστούν τις επιθυμίες, τους φόβους, αλλά και τις γνώσεις και τον ενθουσιασμό τους σχετικά με τα νέα «εργαλεία» και τους νέους κοινωνικούς χώρους. Οι μαθητές μέσα από μια ανοιχτή και ειλικρινή διαδικασία κοινότητας και διαλόγου είναι ανάγκη να νιώσουν ασφάλεια και εμπιστοσύνη ώστε να μιλήσουν στον εκπαιδευτικό για τη «ζωή τους στο διαδίκτυο». Αυτό προϋποθέτει, συν τοις άλλοις, την πολύ καλή γνώση από την πλευρά του εκπαιδευτικού των σύγχρονων εργαλείων, των απειλών αλλά και των στρατηγικών αντιμετώπισής τους, γεγονός που συνδέεται με την συνεχή και ουσιαστική επιμόρφωσή του. Κάτω από αυτές τις προϋποθέσεις, υπάρχουν περισσότερες πιθανότητες να κερδίσει την εμπιστοσύνη των μαθητών, ώστε από τη μια μεριά, να αναδείξει τους κινδύνους από τη χρήση του διαδικτύου και από την άλλη να διδάξει συγκεκριμένες στρατηγικές αντιμετώπισής τους (για παράδειγμα, διαφύλαξη των προσωπικών στοιχείων στο Facebook) (Valcke et al. 2007).

Συγκεκριμένα, αυτά που πρέπει να κάνει ένας εκπαιδευτικός είναι:

i. Να κάνει συζήτηση με τους μαθητές, στο επίπεδο της τάξης, για τη χρήση του Internet.

ii. Να δημιουργήσει τη δική του λίστα με προτεινόμενες σελίδες, με κατάλληλο περιεχόμενο που θα αναδεικνύει τις ανθρωπιστικές αξίες και θα προάγει το γνωστικό και πνευματικό επίπεδο των μαθητών.
iii. Να διδάξει στους μαθητές να μη δίνουν ποτέ προσωπικά στοιχεία και πληροφορίες.
iv. Να ελέγχει τα Αγαπημένα (Bookmarks) και το Ιστορικό (History) του προγράμματος φυλλομετρητή (browser), για να δει ποιες σελίδες επισκέπτονται οι μαθητές.
v. Να επιβλέπει τους μαθητές κατά τη χρήση του διαδικτύου στο σχολικό εργαστήριο ή στη σχολική τάξη.
vi. Με τις ενέργειες και το παράδειγμά του μπορεί να προωθήσει στην πράξη τις πρακτικές καλής χρήσης του Internet και των διαδικτυακών υπηρεσιών.(Πανελλήνιο Σχολικό Δίκτυο, 2010)

2.2.1.1 Σχολείο και ασφαλής χρήση του διαδικτύου

Η σύγχρονη έρευνα έχει δείξει ότι οι γονείς αλλά και η κοινωνία θεωρούν ότι το σχολείο πρέπει να παίξει έναν κεντρικό ρόλο στην ανάπτυξη στάσεων και συμπεριφοράς ασφαλούς χρήσης του διαδικτύου από τους μαθητές (Media Awareness Network, 2001; NCTE, 2001). Από την άλλη πλευρά, η αλλαγή της συμπεριφοράς των μαθητών προς την ασφαλέστερη χρήση του διαδικτύου αποτελεί ένα δύσκολο εγχείρημα, το οποίο δύσκολα στέφεται με επιτυχία παρά τη θέσπιση κανόνων και πολιτικών από την πλευρά του σχολείου. Πολλές φορές μάλιστα, η αντικοινωνική ή και επικίνδυνη χρήση του διαδικτύου εμφανίζεται ως ενσωματωμένη στην κουλτούρα των νέων (Berson, 2000). Ίσως αυτό να έχει κάποια βάση αν αναρωτηθούμε πόσες φορές μαθητές έχουν ζητήσει από τους εκπαιδευτικούς να μάθουν να φτιάχνουν ιούς αλλά και να αποκτούν πρόσβαση σε ξένα συστήματα και λογαριασμούς (hacking).

2.2.2 Ασφάλεια στο Διαδίκτυο για τους γονείς

Πώς θα πρέπει οι γονείς να ενισχύουν τα παιδιά τους προκειμένου να ελαχιστοποιήσουν τους κινδύνους αυτούς; Δεν υπάρχει μία εύκολη απάντηση - οι κίνδυνοι ποικίλλουν, ανάλογα με την ηλικία του παιδιού και το πόσο εξοικειωμένο είναι με τον υπολογιστή.

Το σημαντικότερο είναι να προστατεύει κανείς τα προσωπικά του στοιχεία, που είναι αποθηκευμένα στον υπολογιστή του, δηλαδή να προστατεύεται ο υπολογιστής από τους ιούς και να αναβαθμίζεται το λογισμικό του. Όσον αφορά στα παιδιά, οι γονείς έχουν τη δυνατότητα να αυξήσουν την ασφάλεια των δεδομένων χρησιμοποιώντας τις ρυθμίσεις των φίλτρων και τις επιλογές φιλτραρίσματος περιεχομένου που διαθέτουν διάφορα προγράμματα.

Βέβαια, σημαντικό είναι να λειτουργεί σωστά ο υπολογιστής. Ωστόσο, για τα παιδιά και τους νέους, το Διαδίκτυο είναι κυρίως ένα κοινωνικό περιβάλλον, όπου μπορεί κανείς να συναντήσει φίλους, αλλά και ξένους. Στο Διαδίκτυο μπορεί να πληγωθείς, να υποστείς παρενοχλήσεις, ακόμα και να σε εξαπατήσουν. Η καλύτερη προστασία είναι η χρήση της κοινής λογικής. Το σημαντικότερο είναι να πληροφορηθούν τα παιδιά για τους κινδύνους που ενέχει το Διαδίκτυο, έτσι ώστε να συμπεριφέρονται με ασφαλή τρόπο και οι γονείς να παραμένουν για να συζητήσουν μαζί τους τυχόν προβλήματα που ενδέχεται να αντιμετωπίσουν κατά τη χρήση του Διαδικτύου.

Όταν αρκετοί γονείς βρίσκονται αντιμέτωποι με ανησυχητικές στατιστικές που αφορούν τα παιδιά σχετικά με την ασφάλεια στο διαδίκτυο, πολλοί γονείς αναρωτιούνται εάν ο καλύτερος τρόπος που πρέπει να ακολουθήσουν είναι να απαγορευθεί η χρήση του υπολογιστή στο σπίτι. Ωστόσο, είναι σημαντικό να θυμούνται ότι το Διαδίκτυο μπορεί να είναι ένας πολύτιμος πόρος. Τα παιδιά πρέπει να μάθουν πώς να χρησιμοποιούν το Διαδίκτυο για την ακαδημαϊκή τους έρευνα και συχνά αποτελεί ένα σημαντικό εργαλείο για τη διατήρηση επαφής με φίλους που βρίσκονται μακριά και με την οικογένεια. Για να είναι τα μικρότερα παιδιά και οι έφηβοι ασφαλείς, ενώ χρησιμοποιούν το Διαδίκτυο, θα πρέπει οι γονείς να θυμούνται και να ακολουθούν τις παρακάτω συμβουλές (Adomaitis, 2006):

1. Θα πρέπει να είναι ενημερωμένοι για τη σύγχρονη δικτυακή πραγματικότητα, τις δυνατότητες και τους κινδύνους που υπάρχουν.
2. Θα πρέπει να γνωρίζουν τι κάνουν τα παιδιά τους στο διαδίκτυο και με τι σκοπό το χρησιμοποιούν.
3. Έχουν δικαίωμα να επιβλέπουν και να φιλτράρουν το περιεχόμενο του διαδικτύου, ώστε να ελέγχουν πως τα παιδιά τους δεν έχουν πρόσβαση σε περιεχόμενο που είναι επιβλαβές γι’ αυτά.

4. Καλό θα ήταν να ενημερωθούν για λογισμικό, το οποίο είναι διαθέσιμο για τον έλεγχο του περιεχομένου, και να εξετάσουν τη δυνατότητα εφαρμογής κάποιου τέτοιου λογισμικού στους ηλεκτρονικούς υπολογιστές του σπιτιού.
5. Πρέπει να συστρατευτούν στην καταπολέμηση του παράνομου περιεχομένου στο διαδίκτυο και να επιβλέπουν τα παιδιά τους κατά τη χρήση του διαδικτύου. Ακόμη πρέπει:

i. Να συμφωνήσουν με τα παιδιά τους για τον τρόπο και το χρόνο χρήσης του διαδικτύου.
ii. Να συνοδεύουν τα μικρότερα παιδιά, όταν συνδέονται στο διαδίκτυο, ειδικά την πρώτη φορά.
iii. Να βάζουν τους ηλεκτρονικούς υπολογιστές με σύνδεση στο διαδίκτυο σε ένα συχνά χρησιμοποιούμενο χώρο σπιτιού.
iv. Να διδάξουν τα παιδιά τους, ώστε να μη δίνουν ποτέ προσωπικά στοιχεία και πληροφορίες.
v. Αν είναι εφικτό, να δημιουργήσουν τη δική τους λίστα με τις προτεινόμενες παιδικές σελίδες και να συμπεριλάβουν μηχανές αναζήτησης φιλικές στη χρήση τους για παιδιά.
vi. Να ελέγχουν τα Αγαπημένα (Bookmarks) και το Ιστορικό (History) του προγράμματος φυλλομετρητή ιστοσελίδων (browser), για να δουν ποιες σελίδες έχουν επισκεφτεί τα παιδιά τους πρόσφατα.

Γι' αυτό και η κυριότερη συμβουλή των ειδικών προς τους γονείς είναι η ηλεκτρονική φιλία με τα παιδιά τους, η οποία αποτελεί βασικό συστατικό για την ασφάλεια των ανηλίκων που διατηρούν λογαριασμούς καθιστώντας τα πιο προσεκτικά στη συνολική «διαδικτυακή» συμπεριφορά τους.

2.2.3 Ασφάλεια στο Διαδίκτυο για τα παιδιά

Η σημερινή γενιά των μαθητών γνωρίζει περισσότερα σχετικά με τη χρήση του διαδικτύου από ότι ίσως κάποιοι εκπαιδευτικοί, δεν γνωρίζει όμως ποιες είναι οι κακοτοπιές και πώς να τις αποφεύγει (Redding, 2008).

Σήμερα οι μαθητές χρησιμοποιούν το διαδίκτυο (α) για τις σχολικές τους εργασίες, (β) για την αναζήτηση ψυχαγωγικού υλικού (βίντεο, μουσική κ.α.), (γ) για τη δημιουργία προφίλ ή λογαριασμού σε ιστότοπους κοινωνικής δικτύωσης ή διαμοίρασης βίντεο (facebook, hi5, youtube κ.α.) και λιγότερο για τη δημιουργία

προσωπικών ιστολογίων. Επίσης το χρησιμοποιούν για να δημιουργήσουν και να δημοσιεύσουν μουσική, φωτογραφίες και βίντεο, να συνομιλήσουν με φίλους, να κάνουν νέους φίλους και κυρίως να παίξουν ηλεκτρονικά παιχνίδια (Κορμάς, 2009).

Εντούτοις, η ελευθερία και η δημιουργικότητα που προσδίδουν οι νέες τεχνολογίες στους μαθητές δεν είναι χωρίς κινδύνους: Οι μαθητές κατά την περιήγησή τους στο διαδίκτυο είναι δυνατόν (α) να συναντήσουν επιβλαβές ή/και παράνομο υλικό, (β) να αντιμετωπίσουν προσπάθειες αποπλάνησης και προσηλυτισμού, (γ) να υπάρξουν θύτες ή θύματα παρενόχλησης και κακής χρήσης ευαίσθητων προσωπικών δεδομένων, αλλά και (δ) να εθιστούν στη χρήση του (Κορμάς, 2009).

Τίθεται λοιπόν το ερώτημα: Για την αντιμετώπιση αυτών των προβλημάτων και την αποφυγή των κινδύνων είναι λύση η αποχή από τη χρήση του διαδικτύου ή απλώς ο έξωθεν επιβαλλόμενος περιορισμός της χρήσης του; Πρέπει να απαγορεύσουμε στους μαθητές να χρησιμοποιούν το διαδίκτυο;

Από τη μια, ο στόχος της απαγόρευσης κρίνεται ανέφικτος (Valcke et al., 2007). Οι μαθητές θα βρουν τον τρόπο να αποκτήσουν πρόσβαση στο διαδίκτυο, εφόσον το επιδιώξουν, ιδιαίτερα αν βρίσκονται στην εφηβεία, η οποία προσδίδει στους μαθητές χαρακτηριστικά όπως «Αμφισβήτηση γονικής εξουσίας», «Περιέργεια-Πειραματισμός», «Προσκόλληση στον παρόντα χρόνο» κ.α. (Κορμάς, 2009). Από την άλλη, ερευνητές υποστηρίζουν ότι η απαγόρευση της χρήσης του διαδικτύου, στερεί από τους μαθητές κάποια εκπαιδευτικά αλλά και ψυχολογικά οφέλη (Tynes, 2007).

Η Tynes (2007) υποστηρίζει ότι (α) η χρήση των forums βοηθάει στην ανάπτυξη επιχειρηματολογίας και κριτικής σκέψης, (β) οι τεχνολογίες Web 2.0 (blogs, wikis, social networks) στην εξ αποστάσεως υποστήριξη της μάθησης, (γ) κατάλληλα ηλεκτρονικά παιχνίδια στην καλλιέργεια δεξιοτήτων ανάγνωσης εικόνων και παράλληλης διαχείρισης αντικειμένων στον ίδιο χώρο, ενώ (δ) γενικότερα η χρήση του διαδικτύου ως μέσο επικοινωνίας και αναζήτησης πληροφοριών προσφέρει κυρίως σε απομονωμένες γεωγραφικά περιοχές ένα κοινωνικό «άνοιγμα» και μια πλούσια εναλλακτική πηγή πληροφόρησης και γνώσης (Εκπαιδευτικά οφέλη). Επίσης, η ίδια ερευνήτρια ισχυρίζεται ότι η χρήση του διαδικτύου ως εργαλείου επικοινωνίας είναι δυνατόν να συνεισφέρει (α) στη διερεύνηση της ταυτότητας του ατόμου/χρήστη, (β) στην ανάπτυξη κοινωνικών δεξιοτήτων, (γ) στην ανάγκη για

διαμόρφωση απόψεων από την πλευρά του χρήστη/μαθητή, (δ) ως μέσο κοινωνικής υποστήριξης σε περιστάσεις που το άτομο είναι απομονωμένο φυσικά ή και κοινωνικά και βρίσκει υποστήριξη μέσω κάποιας ηλεκτρονικής κοινότητας, ενώ (ε) τα κοινωνικά δίκτυα είναι δυνατό να ικανοποιήσουν, εν μέρει, και την ανάγκη για οικειότητα και αυτονομία.

Οι μαθητές θα πρέπει να διδαχθούν από τους δασκάλους και τους γονείς:

i. Να συζητούν μαζί τους για τις δραστηριότητές τους στο διαδίκτυο, ιδιαίτερα αν αντιμετωπίσουν ο,τιδήποτε περίεργο ή ασυνήθιστο.
ii. Να είναι επιφυλακτικοί σε ο,τιδήποτε διαβάζουν στους διάφορους δικτυακούς τόπους του διαδικτύου και σε ο,τιδήποτε αναφέρουν οι άλλοι χρήστες.
iii. Να τηρούν τη δεοντολογία του διαδικτύου και τα μηνύματά τους να μην έχουν υβριστικό χαρακτήρα ή ρατσιστική χροιά.
iv. Να μη δίνουν προσωπικά στοιχεία και να μην αποκαλύπτουν λεπτομέρειες της προσωπικής τους ζωής σε άλλους χρήστες στο διαδίκτυο.
v. Να μη γνωστοποιούν σε αγνώστους μέσω του διαδικτύου τα στοιχεία επικοινωνίας (e-mail, αριθμούς τηλεφώνων κ.τ.λ.).
vi. Να μην αποκαλύπτουν τους κωδικούς πρόσβασης (password), τους οποίους χρησιμοποιούν.
vii. Να μη δίνουν ποτέ στοιχεία που αφορούν πιστωτικές κάρτες, χωρίς τη συμφωνία των γονέων.
viii. Να μην συμπληρώνουν φόρμες στοιχείων κατά την επίσκεψή τους σε διάφορους δικτυακούς τόπους.
ix. Να μη στέλνουν υλικό από τον δικό τους υπολογιστή (φωτογραφίες, μουσική κ.τ.λ.), ιδιαίτερα σε αγνώστους.
x. Να μη χρησιμοποιούν οποιοδήποτε πρόγραμμα βρίσκεται στο διαδίκτυο. Δεν είναι όλα τα προγράμματα ασφαλή, ακόμα και αν εμφανίζονται ως παιχνίδια (προγράμματα «Δούρειοι Ίπποι»).
xi. Να μην ανοίγουν e-mails από αγνώστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. (Πανελλήνιο Σχολικό Δίκτυο, 2010)

2.3 Κίνδυνοι στο Διαδίκτυο

Η θετική επίδραση των Νέων Τεχνολογιών στη σημερινή εκπαίδευση είναι γεγονός αδιαφιλονίκητο. Ο ηλεκτρονικός υπολογιστής καταφέρνει να ενεργοποιεί το

ενδιαφέρον των παιδιών κατά τρόπο διαφορετικό από αυτόν της τάξης. Ο αμφίδρομος χαρακτήρας διδασκαλίας, η επιλογή πλοήγησης μέσα στο πρόγραμμα αλλά και η εξατομικευμένη εκπαίδευση με τον απεριόριστο πειραματισμό είναι από τα στοιχεία που σαγηνεύουν τα παιδιά. Το διαδίκτυο έχει καταργήσει κάθε εμπόδιο ανταλλαγής πληροφοριών ανάμεσα στους χρήστες του σε όλο τον κόσμο και έτσι μικροί και μεγάλοι μπορούν να αποκτήσουν πρόσβαση σε πληθώρα πληροφοριών διαφόρων πηγών, όπως εγκυκλοπαίδειες, βιβλιοθήκες, ειδησεογραφικά πρακτορεία και πολλούς άλλους οργανισμούς. Η φύση του διαδικτύου είναι τέτοια που ελκύει τα παιδιά. Με το πάτημα ενός κουμπιού μπορούν να ικανοποιήσουν την περιέργειά τους αλλά και την ανάγκη τους για επικοινωνία και άμεση ανταπόκριση. Εξάλλου, ο αυθορμητισμός είναι χαρακτηριστικό των παιδιών, ιδιαίτερα στις μικρότερες ηλικίες. (Κωστάκη, χ.η.)

Πέρα όμως από τη σημαντική συμβολή του στην εκπαιδευτική διαδικασία, το διαδίκτυο υποκρύπτει σοβαρότατους κινδύνους. Πρόκειται για ένα αχανές δίκτυο το οποίο, στην ουσία, δεν ελέγχεται από κανέναν. Πάμπολλα περιστατικά εξαπάτησης ή και κακοποίησης παιδιών έχουν καταγραφεί παγκοσμίως, από επιτήδειους οι οποίοι χρησιμοποιούν την ανωνυμία του διαδικτύου προκειμένου να επιτύχουν τους στόχους τους. Άλλοι κίνδυνοι, τους οποίους δε θα έπρεπε να παραλείψουμε, είναι οι εξής: τα παιδιά μπορεί να επισκεφτούν σελίδες ακατάλληλες για εκείνα ή σελίδες που προωθούν τη βία, το μίσος και την πορνογραφία (όπως αναφέρθηκε και παραπάνω), ενώ μπορεί εύκολα να πέσουν θύματα έντονης, καλοστημένης διαφημιστικής εκστρατείας. Τέλος, δε θα πρέπει να παραβλέπεται ο κίνδυνος της κοινωνικής απομόνωσης των παιδιών, όταν εκείνα ξοδεύουν πάρα πολλές ώρες στο διαδίκτυο, χάνοντας πολύτιμο χρόνο στον οποίο θα μπορούσαν να αναπτύξουν κοινωνικές ικανότητες. (Κωστάκη, χ.η.)

2.3.1 Κακόβουλο Λογισμικό

Κακόβουλο Λογισμικό είναι οποιοδήποτε πρόγραμμα το οποίο έχει σκοπό να προκαλέσει κάποιου είδους καταστροφή ή να χρησιμοποιήσει χωρίς εξουσιοδότηση πόρους του συστήματος.

2.3.1.1Virus:

Ιός ή Virus είναι πρόγραμμα το οποίο είναι συνδεδεμένο να «μπαίνει» στον ηλεκτρονικό υπολογιστή σου χωρίς την άδειά σου και να τον «μολύνει» δημιουργώντας ανεπιθύμητες παρενέργειες (αδυναμία έναρξης του ηλεκτρονικού

υπολογιστή, λάθος λειτουργία των εφαρμογών που χρησιμοποιούμε, ξαφνική εμφάνιση διαφόρων χαρακτήρων ή αριθμών στην οθόνη μας) έως και σοβαρές ή ανεπανόρθωτες βλάβες (καταστροφή αρχείων από το σκληρό δίσκο του ηλεκτρονικού υπολογιστή σου).

Ένας Ιός έχει γραφτεί με σκοπό να αναπαράγεται. Προσκολλάται σε ένα αρχείο «ξενιστή» και προσπαθεί να διαδοθεί από ηλεκτρονικό υπολογιστή σε ηλεκτρονικό υπολογιστή.

2.3.1.2Worm

Σκουλήκι ή Worm είναι μια υποκατηγορία ιού που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του διαμέσου των δικτύων του ηλεκτρονικού υπολογιστή. Μόλις φτάσει σε έναν προορισμό, ενεργοποιείται και διαχέεται περαιτέρω χωρίς να χρειάζεται κάποιο φορέα (όπως γίνεται με τους ιούς).

Ένα σκουλήκι μπορεί να βλάψει ένα δίκτυο και να μειώσει την ταχύτητα της σύνδεσής του χρήστη στο Διαδίκτυο καταναλώνοντας όλους τους πόρους του ηλεκτρονικού υπολογιστή οδηγώντας τον και σε κλείσιμο.

2.3.1.3Trojan Horse

Δούρειος Ίππος ή Trojan Horse είναι ένα φαινομενικά χρήσιμο και αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Περιέχει κρυμμένο κώδικα που αν εκτελεστεί, επιτελεί λειτουργίες για τις οποίες δεν έχει άδεια.

Μπαίνει στον ηλεκτρονικό υπολογιστή ανοίγοντας ένα πρόγραμμα που θεωρούμε ότι προέρχεται από νόμιμη πηγή και προκαλεί βλάβες. Χρησιμοποιείται για να γίνουν πράγματα που υπό κανονικές συνθήκες δε θα γίνονταν. Μπορεί να δράσει και ως κατάσκοπος καταγράφοντας ο,τιδήποτε πληκτρολογούμε.

2.3.1.4Spyware

Πρόγραμμα Παρακολούθησης ή Spyware είναι λογισμικό το οποίο προσκολλάται κρυφά σε αρχεία που κατεβάζεις, αυτο-εγκαθίσταται στον ηλεκτρονικό υπολογιστή του χρήστη και παρακολουθεί τη διαδικτυακή του δραστηριότητα συλλέγοντας προσωπικά δεδομένα. Αυτά αποστέλλονται σε τρίτους που δημιουργούν το προφίλ του και του στέλνουν διαφημιστικό υλικό.

Κάποια είδη spyware προκαλούν αλλαγές (στην κεντρική σελίδα ή τη σελίδα αναζήτησης του browser) στον ηλεκτρονικό υπολογιστή χωρίς τη συγκατάθεση του

χρήστη, οι οποίες είναι ενοχλητικές και μειώνουν την ταχύτητά του ή τον κάνουν να «κολλάει».

2.3.1.5Keylogger

Πρόγραμμα Καταγραφής Πληκτρολογήσεων ή Keylogger είναι λογισμικό το οποίο καταγράφει όλες τις πληροφορίες που κάποιος χρήστης πληκτρολογεί και τις αποστέλλει σε αυτόν που τον έχει μολύνει.

Πρόκειται για ένα πολύ επικίνδυνο λογισμικό κυρίως για όσους κάνουν διαδικτυακές χρηματικές συναλλαγές, γιατί εκτελείται σχεδόν αόρατα και μπορεί να χρησιμοποιηθεί για κλοπή ευαίσθητων προσωπικών δεδομένων (αριθμοί πιστωτικών καρτών και κωδικοί πρόσβασης).

2.3.2 Επιθέσεις Dialer

Ένας Dialer είναι ένα πρόγραμμα το οποίο χωρίς τη συγκατάθεση του χρήστη σταματά τη σύνδεση στο Διαδίκτυο μέσω του παρόχου του και καλεί αυτόματα έναν υψηλής χρέωσης αριθμό, με αποτέλεσμα ο λογαριασμός του τηλεφώνου να χρεώνεται υπερβολικά. Προέρχεται από επισκέψεις σε συγκεκριμένες ιστοσελίδες με αμφίβολο περιεχόμενο, καθώς και με τη μορφή συνημμένων αρχείων σε e-mail. Από τους dialer κινδυνεύουν κυρίως οι συνδρομητές υπηρεσιών PSTN ή ISDN και τα συστήματα με εγκατεστημένο modem συνδεδεμένο σε τηλεφωνική γραμμή. Οι συνδρομητές υπηρεσιών ADSL δε διατρέχουν κίνδυνο (συνδέονται στο διαδίκτυο χωρίς τηλεφωνική κλήση).

2.3.3 Επιθέσεις Χάκερ και Κράκερ

Οι Χάκερ (Hackers) είναι τα άτομα, που με τη χρήση κακόβουλου λογισμικού, και χωρίς εξουσιοδότηση αποκτούν πρόσβαση σε κάποιον ηλεκτρονικό υπολογιστή ή σύστημα υπολογιστών και στα δεδομένα τους, βλέποντας και αντιγράφοντας τα αρχεία που υπάρχουν σε αυτούς τους υπολογιστές, χωρίς όμως να έχουν καμία πρόθεση να προκαλέσουν ζημιά.

Οι Κράκερ (Cracker) είναι τα άτομα, που με τη χρήση κακόβουλου λογισμικού, και χωρίς εξουσιοδότηση αποκτούν παράνομη πρόσβαση σε κάποιον ηλεκτρονικό υπολογιστή ή σύστημα υπολογιστών και στα δεδομένα τους, έχοντας ως μοναδικό στόχο να προκαλέσουν διαφόρων ειδών ζημιές και να κλέψουν πληροφορίες.

2.3.4 "Ψάρεμα" Προσωπικών Δεδομένων

Αρκετές φορές όταν ο χρήστης «σερφάρει» στο Διαδίκτυο εμφανίζονται στην οθόνη του κάποια αναδυόμενα παράθυρα (pop-up) με διάφορα μηνύματα ή συνδέσμους (links) προσφέροντας δώρα! Πρόκειται για παραπλανητικά μηνύματα που έχουν σκοπό να τον ξεγελάσουν για να δώσει κάποια προσωπικά δεδομένα του. Το φαινόμενο αυτό ονομάζεται «ψάρεμα προσωπικών δεδομένων» ή Phishing. Το phishing είναι πλέον αρκετά εξελιγμένο: μπορεί ένα τέτοιο μήνυμα να τον παραπέμπει σε μία ψεύτικη ιστοσελίδα η οποία όμως να είναι πιστό αντίγραφο της αυθεντικής.

2.3.5 Πειρατεία

Αρκετές φορές στο Διαδίκτυο είναι πιθανό ο χρήστης να εμπλακεί σε παράνομες πράξεις χωρίς να έχει την πρόθεση αυτή. Κατεβάζοντας ή αντιγράφοντας video, ταινίες, τραγούδια, παιχνίδια ή προγράμματα που δεν είναι αυθεντικά ο χρήστης συμμετέχει σε μια παράνομη πράξη που ονομάζεται Πειρατεία (Piracy). Τα άτομα που εμπλέκονται σε τέτοιου είδους πράξεις μπορεί να έχουν σοβαρές νομικές επιπτώσεις.

2.3.6 Παραπλάνηση

Αρκετές φορές ο χρήστης χρησιμοποιεί το Διαδίκτυο για να βρει κάποιες πληροφορίες. Μερικοί ιστότοποι εμφανίζουν πληροφορίες ψεύτικες ή παραποιημένες. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε κάποιο προσωπικό όφελος του δημιουργού τους είτε η χαρά της παραπλάνησης των υπόλοιπων χρηστών του Διαδικτύου. Ο όρος που περιγράφει αυτού του τύπου τη παραπλάνηση είναι “Hoax”. Επίσης και μεγάλος αριθμός ηλεκτρονικών μηνυμάτων (e-mail) περιέχει ψεύτικες πληροφορίες (π.χ.: «Αν αγνοήσεις αυτό το e-mail και δεν το προωθήσεις στους φίλους σου κάτι κακό θα σου συμβεί μέσα σε 5 μέρες!»).

2.3.7 Αποπλάνηση Ανηλίκων

Η Αποπλάνηση ανηλίκου (Grooming) είναι μια πολύ σοβαρή διαδικτυακή απειλή. Υπάρχουν κάποιοι χρήστες στο Διαδίκτυο που χρησιμοποιούν ψεύτικα στοιχεία στο προφίλ τους με σκοπό να επικοινωνούν με παιδιά προκειμένου να κερδίσουν την εμπιστοσύνη τους και να τα εκμεταλλευτούν σεξουαλικά ή να τα

παρασύρουν σε παράνομες δραστηριότητες όπως είναι η παιδική πορνεία ή η παιδική πορνογραφία.

2.3.8 Διαδικτυακός Εκφοβισμός

Ως χρήστης του Διαδικτύου υπάρχει πιθανότητα ο καθένας να λάβει κάποια πρόστυχα ηλεκτρονικά μηνύματα, φωτογραφίες ή βίντεο με εκφοβιστικό, ρατσιστικό ή προσβλητικό περιεχόμενο (μέσω ηλεκτρονικού ταχυδρομείου, δωματίων συναντήσεων, σελίδων διαμοιρασμού και προβολής βίντεο και ιστολογίων). Το φαινόμενο αυτό ονομάζεται Διαδικτυακός Εκφοβισμός (Cyberbullying) και μπορεί να βλάψει συναισθηματικά και να αποκλείσει κάποιους ανθρώπους από κάποιους άλλους.

2.3.9 Κλοπή Ταυτότητας

Κλοπή ταυτότητας στο Διαδίκτυο ονομάζεται η παράνομη χρήση της εικονικής ταυτότητας ενός άλλου ατόμου σε υπηρεσίες και εφαρμογές του Διαδικτύου. Επιτυγχάνεται είτε υποκλέπτοντας τους κωδικούς πρόσβασης (όνομα χρήστη και κωδικός πρόσβασης), είτε ανοίγοντας ένα ψεύτικο προφίλ ή λογαριασμό με το όνομα άλλου ατόμου. Ο κλέφτης ταυτότητας μπορεί να επικοινωνεί με επαφές του ατόμου, να αναρτά φωτογραφίες και άλλο υλικό με σκοπό την οικονομική εξαπάτηση ή τον εξευτελισμό και τη διάδοση φημών για το άτομο αυτό στο διαδικτυακό του περιβάλλον.

2.3.10 Εθισμός στο Διαδίκτυο

Τα τελευταία χρόνια έχει παρατηρηθεί ότι αρκετά παιδιά αφιερώνουν πολλές ώρες στο Διαδίκτυο παίζοντας παιχνίδια ή συνομιλώντας σε σελίδες κοινωνικής δικτύωσης, με αποτέλεσμα να αποξενώνονται από τους πραγματικούς τους φίλους, να κλείνονται στον εαυτό τους, να παραμελούν τα μαθήματά τους ακόμα και την υγεία τους κάποιες φορές. Το φαινόμενο αυτό ονομάζεται «Εθισμός στο Διαδίκτυο» (Internet Addiction).

2.3.11 Αλλοίωση της Γλώσσας ("Greeklish")

Τα "Greeklish" περιγράφουν ελληνικές λέξεις γραμμένες με λατινικούς χαρακτήρες. Διαδόθηκαν πολύ γρήγορα και καθιερώθηκαν ως κοινός κώδικας επικοινωνίας μεταξύ νέων στην επικοινωνία τους στο Διαδίκτυο. Οι ειδικοί επιμένουν ότι η χρήση τους έχει πολύ σοβαρές συνέπειες, γιατί γίνονται συνήθεια στους νέους

με αποτέλεσμα να τα μεταφέρουν στην πραγματική ζωή, ακόμα και στο γραπτό λόγο αλλοιώνοντας την ελληνική γλώσσα σε επίπεδο ορθογραφίας, γραμματικής και σύνταξης. Έρευνα έδειξε ότι σε ποσοστό 64,3% οι φιλόλογοι παρατήρησαν λέξεις γραμμένες με αυτή τη γραφή σε σχολικά διαγωνίσματα.

2.3.12 Παράνομη Εμπορία Ανθρώπων

Ως παράνομη διακίνηση και εμπορία ανθρώπων (trafficking) ορίζεται η στρατολόγηση, μεταφορά, μετακίνηση, εγκατάσταση ή παραλαβή προσώπων μέσω απειλής, χρήσης βίας, εξαναγκασμού, απαγωγής, δόλου, εξαπάτησης, παροχής οικονομικού ή άλλου οφέλους με σκοπό την εκμετάλλευσή τους, η οποία περιλαμβάνει εξαναγκαστική εργασία, διαμόρφωση συνθηκών σκλαβιάς ή δουλείας, λήψη σωματικών οργάνων, πορνεία και σεξουαλική εκμετάλλευση.

Η εξάπλωση του Διαδικτύου και η αυξανόμενη χρήση των «δωματίων επικοινωνίας» (chatrooms) και των εφαρμογών κοινωνικής δικτύωσης (social networks) διευκολύνει τους εμπόρους ανθρώπων να παγιδεύουν τα θύματά τους και να διακινούν παράνομο υλικό.

2.4 Τρόποι Προστασίας από τους κινδύνους του διαδικτύου

2.4.1 Προστασία από Κακόβουλο λογισμικό

Για την προστασία από επιθέσεις χάκερ (Hacker) και κράκερ (Cracker) ή από επιθέσεις κακόβουλου λογισμικού (Malware) ο κάθε χρήστης θα πρέπει να ακολουθήσει τις παρακάτω ενέργειες.

2.4.1.1 Ενημέρωση του λειτουργικού συστήματος

Οι εταιρίες εκδίδουν ανά τακτά χρονικά διαστήματα ενημερωμένες εκδόσεις ασφαλείας (updates) του λειτουργικού συστήματος και των προγραμμάτων πλοηγήσεως (browser), που χρησιμοποιεί ο ηλεκτρονικός υπολογιστής, οι οποίες πρέπει οπωσδήποτε να εγκαθίστανται, πάντα, από επίσημη ιστοσελίδα της κατασκευάστριας εταιρίας.

2.4.1.2 Χρήση λογισμικού Antivirus

Το λογισμικό Antivirus χρησιμοποιείται για να προστατεύει τον ηλεκτρονικό υπολογιστή από ιούς και άλλο βλαβερό υλικό. Με την εγκατάστασή του στον

υπολογιστή γίνεται έλεγχος όλων των αρχείων (του ηλεκτρονικού υπολογιστή και τα συνημμένα σε e-mail). Στην περίπτωση που βρεθούν ιοί γίνεται άμεση ενημέρωση και στη συνέχεια απομόνωση ή επιδιόρθωση των μολυσμένων από τον ιό αρχείων. Για να είναι όμως το antivirus αποτελεσματικό χρειάζεται συνεχή ενημέρωση.

2.4.1.3 Χρήση λογισμικού Antisryware

Το antisryware είναι πρόγραμμα που αναγνωρίζει και στη συνέχεια μπλοκάρει ή αφαιρεί κακόβουλο λογισμικό τύπου spyware. Ελέγχει το περιεχόμενο των αρχείων του λειτουργικού συστήματος και των εγκατεστημένων προγραμμάτων σε έναν υπολογιστή και αφαιρεί τα αρχεία που περιέχουν λογισμικό spyware. Επιπλέον παρεμποδίζει τις προσπάθειες να τροποποιηθούν οι ρυθμίσεις των μηχανών αναζήτησης ή να προστεθούν καινούργια στοιχεία στο πρόγραμμα περιήγησής που χρησιμοποιεί ο χρήστης (browser). Το antisryware απαιτεί συχνή εγκατάσταση των ενημερώσεων δεδομένου ότι συνεχώς κυκλοφορούν καινούρια είδη απειλών spyware.

2.4.1.4 Χρήση «τείχους προστασίας»

Το «τείχος προστασίας» ή Firewall είναι είτε συσκευή είτε λογισμικό που προστατεύει τον ηλεκτρονικό υπολογιστή από επιθέσεις μη εξουσιοδοτημένων χρηστών. Ελέγχει όλα τα αρχεία που μπαίνουν ή βγαίνουν από τον υπολογιστή και αν βρει κάτι ύποπτο το μπλοκάρει και του απαγορεύει την πρόσβαση στον υπολογιστή προφυλάσσοντας τον από πιθανές επιθέσεις.

2.4.1.5 Δημιουργία Αντιγράφων Ασφαλείας (Back-up)

Αρκετές φορές λόγω απροσεξίας του χρήστη ή λόγω κάποιας κακόβουλης επίθεσης στον υπολογιστή του μπορεί να χαθεί μέρος ή το σύνολο των αρχείων του (καταστροφή σκληρού δίσκου). Λύση σε αυτό το φαινόμενο αποτελεί η δημιουργία αντιγράφων ασφαλείας ή back-up την οποία πρέπει να εκτελεί ανά τακτά χρονικά διαστήματα. Με τη διαδικασία αυτή γίνεται αντιγραφή σημαντικών εγγράφων του ηλεκτρονικού υπολογιστή σε εξωτερικές συσκευές αποθήκευσης (CD ή/και DVD), συσκευές αποθήκευσης USB ή εξωτερικούς σκληρούς δίσκους με σκοπό να υπάρχει η δυνατότητα ανάκτησής του σε περίπτωση απώλειας.

2.4.2 Προστασία από Dialers

Αν ο χρήστης χρησιμοποιεί modem (PSTN ή ISDN) για τη σύνδεσή του στο Διαδίκτυο πρέπει να επικοινωνήσει με τον τηλεπικοινωνιακό πάροχό του και να του ζητήσει φραγή διεθνών κλήσεων και κλήσεων αριθμών υψηλής χρέωσης

προκειμένου να μην πέσει θύμα κάποιου dialer. Ο πάροχός του θα του δώσει έναν κωδικό τον οποίο θα πρέπει να καλεί πριν από κάθε κλήση του προς τους αριθμούς που προστατεύονται με φραγή. Έτσι, ο dialer δε θα μπορεί να εκτρέψει τη σύνδεσή του στο εξωτερικό, καθώς το τηλέφωνό του θα φράζει την εξερχόμενη κλήση.

2.4.3 Προστασία από ανεπιθύμητη Αλληλογραφία

Ανεπιθύμητη αλληλογραφία ή Spam ονομάζεται η μαζική αποστολή μεγάλου αριθμού ηλεκτρονικών μηνυμάτων που διανέμεται σε τεράστιο αριθμό παραληπτών του Διαδικτύου χωρίς αυτοί να το επιθυμούν. Το περιεχόμενό τους είναι συνήθως διαφημιστικό ή ενημερωτικό και σχετίζεται με προϊόντα ή υπηρεσίες για τα οποία όμως δεν έχουν ζητήσει να ενημερωθούν.

Για να αντιμετωπιστεί το φαινόμενο της Ανεπιθύμητης Αλληλογραφίας (Spam) θα πρέπει να ακολουθηθούν οι παρακάτω ενέργειες:

i. Να μη γίνεται δημοσίευση ποτέ του προσωπικό e-mail του χρήστη σε δημόσια προσβάσιμες εφαρμογές (forums, chat rooms, λίστες αλληλογραφίας, social networks κ.τ.λ.).
ii. Να γίνεται χρήση δύο e-mail. Το ένα (προσωπικό) για να επικοινωνεί αποκλειστικά με τους φίλους και τους συμμαθητές του και το άλλο (δημόσιο) για να επικοινωνεί με όσους γνωρίζει στο Διαδίκτυο μέσω των δημόσια προσβάσιμων εφαρμογών.
iii. Κατά τη διάρκεια της δημιουργίας του e-mail θα πρέπει να επιλέξει συνδυασμό γραμμάτων του ονόματος και επιθέτου του, καθώς επίσης και αριθμούς. Οι αποστολείς spam συνδυάζουν μικρά ονόματα, λέξεις και αριθμούς για τη δημιουργία πιθανών e-mail.
iv. Να μην απαντά σε spam και να μην επισκέπτεται συνδέσμους (από ύποπτες πηγές) με σκοπό τη διαγραφή του από μία λίστα στην οποία δε θέλει να ανήκει, γιατί αυτό επιβεβαιώνει ότι η διεύθυνσή του είναι ενεργή. Όσο περισσότερο απαντά, τόσο περισσότερα spam θα λαμβάνει.
v. Να εγκαθιστά πάντα στον ηλεκτρονικό υπολογιστή του λογισμικό προστασίας από ανεπιθύμητη αλληλογραφία (anti-spam) το οποίο θα φιλτράρει τα e-mail και θα τα ξεχωρίζει από τα ανεπιθύμητα.

2.4.4 Προστασία από Κλοπή Ταυτότητας

Ο μαθητής για να μειώσει τις πιθανότητες να βρεθεί αντιμέτωπος με περιστατικά κλοπής της Διαδικτυακής του Ταυτότητας θα πρέπει:

i. Οι κωδικοί πρόσβασης του στις υπηρεσίες και τις εφαρμογές του Διαδικτύου που χρησιμοποιεί να μη μαντεύονται εύκολα (π.χ.: ημερομηνία γέννησης) και να μην είναι πολύ απλοί (π.χ.: μικρό όνομα).
ii. Ανά τακτά διαστήματα να ελέγχει την εικονική του παρουσία! Να επιλέξει μια μηχανή αναζήτησης (π.χ.: google), να εισαγάγει το όνομα ή το ψευδώνυμο που χρησιμοποιεί και να δει τι αποτελέσματα θα πάρει από την αναζήτηση. Έτσι θα μπορεί να είναι σίγουρη / σίγουρος πως όλα θα πάνε καλά.

2.4.5 Προσωπική Προστασία

Ο μαθητής για να είναι προσεκτικός στην περιήγησή του στο Διαδίκτυο θα πρέπει να ακολουθεί πιστά τις παρακάτω συμβουλές:

1. Να μη χρησιμοποιεί το Διαδίκτυο άσκοπα και υπερβολικά.
2. Να μην ακολουθεί συνδέσμους (links) των οποίων δε γνωρίζει το περιεχόμενο.
3. Να διαγράφει e-mail που λαμβάνει από αποστολείς που δε γνωρίζει, χωρίς να τα ανοίγει.
4. Αν δει ο,τιδήποτε που τον φοβίζει ή τον αγχώνει να κλείνει τον ηλεκτρονικό υπολογιστή και να αναφέρει το συμβάν στους γονείς ή τους δασκάλους του.(Πανούτσου, 2010)

2.5 Υφιστάμενη κατάσταση στην Ελλάδα και στο Εξωτερικό

Στην Ελλάδα το διαδίκτυο έχει μπει στη ζωή των ανθρώπων σε μεγάλο βαθμό σχετικά πρόσφατα. Αλλά τι είναι για τους ανθρώπους το διαδίκτυο και κατά πόσο έχουν γνώση των προβλημάτων αναφορικά με τα προσωπικά δεδομένα, την παρενόχληση και την εξάρτηση;

Το μεγαλύτερο ποσοστό των χρηστών βλέπει το διαδίκτυο ως μια απέραντη θάλασσα πληροφοριών και μόνο εκεί μπορεί να εστιάσει το πρόβλημα της πλοήγησής του σε αυτό. Όμως, τόσο η ασφάλεια των προσωπικών δεδομένων, όσο και ο ηλεκτρονικός εκφοβισμός και εξύβριση είναι τα καίρια ζητήματα, ειδικά στις μικρές

ηλικίες, ενώ το ποσοστό εξάρτησης κάθε χρόνο παρουσιάζεται μεγαλύτερο. Τα νούμερα για την Ελλάδα –και σε αυτή την περίπτωση- είναι τρομακτικά[1]:

- Το 1% των εφήβων έχει εθιστεί στη χρήση του Διαδικτύου, ενώ στη Νορβηγία το 1,98%, στην Κίνα το 2,4% και στην Κορέα το 14% - παραδείγματα προς αποφυγή.
- Το 12,8% των μαθητών παρουσιάζει περιοδικά ή συχνά προβλήματα κατάχρησης του διαδικτύου.
- Το 26% το μαθητών χρησιμοποιεί καθημερινά το διαδίκτυο και το 8% για περισσότερες από 20 ώρες.
- Το 10% των παιδιών παραδέχεται πως έχει ενοχληθεί ή νοιώσει άσχημα για κάτι που είδε στο διαδίκτυο.
- Το 79% των γονιών δηλώνει άγνοια ότι τα παιδιά τους μπορεί να έχουν υποστεί διαδικτυακό bullying/ εκφοβισμό και εξύβριση.

Οι ιστοσελίδες κοινωνικής δικτύωσης έχουν μπει στο παιχνίδι τόσο σε επίπεδο επικοινωνίας με γνωστούς και φίλους όσο και σε επιχειρηματικών δραστηριοτήτων και πλάνων. Μια νέα ιδιάζουσα κοινωνία έχει δημιουργηθεί στις εν λόγω πλατφόρμες, με πολίτες/χρήστες ιδιαίτερα διαχυτικούς και επικοινωνιακούς, που ενώ στην καθημερινότητά τους στον «πραγματικό κόσμο» μπορεί να ήταν ιδιαίτερα συγκρατημένοι στον «ψηφιακό κόσμο» φαίνονται να σχολιάζουν, να δηλώνουν τι τους αρέσει –ακόμα και αν πραγματικά τους αφήνει αδιάφορους- να ανεβάζουν φωτογραφίες, προσωπικές πληροφορίες. Δεν είναι πολλοί εκείνοι οι οποίοι έχουν επίγνωση στο ότι όλος ο κόσμος είναι ένα «κλικ» απόσταση και πόσο εύκολα μπορούν να βρεθούν εκτεθειμένοι.

Το Facebook έχει 845 εκατομμύρια ενεργούς χρήστες, εκ των οποίων οι μισοί «συνδέονται» τουλάχιστον μια φορά την ημέρα. Αν ήταν χώρα, θα ήταν η τρίτη σε μέγεθος στον κόσμο, μετά την Κίνα και την Ινδία.

Η ελληνική κοινωνία και οικογένεια έρχεται λοιπόν να αντιμετωπίσει άλλο ένα πρόβλημα εξάρτησης, παρενόχλησης και εκφοβισμού, αυτό του διαδικτύου. Πόσο μάλλον όταν σε περιόδους «κρίσης» τα ποσοστά εξαρτήσεων αυξάνονται ραγδαία, χρειάζεται να είναι όλοι ενημερωμένοι και ενεργοποιημένοι και σε αυτό. Δε

[1]Τα στοιχεία προέρχονται από έρευνα της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) της Β΄ Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών στο Νοσοκομείο Παίδων «Π. & Α. Κυριακού», από την ιστοσελίδα «safer internet» και την εφημερίδα «Καθημερινή».

χρειάζονται ακρότητες και απαγορεύσεις. Η γνώση βασικών κανόνων ασφάλειας χρειάζεται, όπως και η ανάπτυξη κριτικής σκέψης, ως καθοριστικοί παράγοντες για την προστασία των χρηστών από κακόβουλους ανθρώπους και τη διαφύλαξη των προσωπικών τους δεδομένων, ώστε να μπορούν να απολαύσουν τις δυνατότητες ψυχαγωγίας, επικοινωνίας και διασκέδασης που τους παρέχονται. Και πάνω απ' όλα να μη ξεχνούν πως τα παιδιά χρειάζονται τους γονείς να είναι ουσιαστικά δίπλα τους και πως ο πραγματικός κόσμος είναι εκεί έξω.(Δίκτυο Υπεύθυνων Οργανισμών & Ενεργών Πολιτών, 2011)

Συγκεκριμένα, μόνο ως ανησυχητικά θα μπορούσε να χαρακτηρίσει κάποιος τα ευρήματα έρευνας που δείχνει ότι ένας στους τρεις ανηλίκους (το 33%), ηλικίας από 9 έως 13 ετών στην Ελλάδα διαθέτει προσωπικό λογαριασμό στα μέσα κοινωνικής δικτύωσης (facebook, twitter κ.α.), παρά το γεγονός ότι αυτό απαγορεύεται από τους όρους χρήσης των περισσότερων.

Οι κίνδυνοι της ανεξέλεγκτης χρήσης του Διαδικτύου είναι πολλοί και το γεγονός ότι σχεδόν σε κάθε σπίτι υπάρχει πρόσβαση, δημιουργεί έναν επιπρόσθετο «πονοκέφαλο» στους γονείς που νιώθουν ότι τα παιδιά τους είναι εκτεθειμένα, ακόμη και μέσα στο ίδιο τους το σπίτι.

Η έρευνα του EU Kids Online, η οποία διενεργείται σε 25 χώρες της Ευρώπης, δείχνει ακόμη ότι το δικό τους προσωπικό προφίλ σε κάποιο δίκτυο διαθέτουν επτά στους δέκα Έλληνες εφήβους μεταξύ 13 και 16 ετών.

Όπως αναφέρει η εφημερίδα «Καθημερινή», στην πλειονότητά τους οι έφηβοι στην Ελλάδα αποδέχονται άκριτα τα αιτήματα φιλίας μέσω facebook (και άλλων κοινωνικών δικτύων), ακολουθώντας τα βήματα των Ευρωπαίων συνομηλίκων τους. Ανησυχία ωστόσο προκαλεί το γεγονός ότι «ανοιχτό» προφίλ (προσβάσιμο δηλαδή από όλους τους χρήστες χωρίς απαραιτήτως να τους συνδέει «φιλική» σχέση με το χρήστη) διατηρούν πάρα πολλά από τα παιδιά.

Βέβαια, οι ανήλικοι που επιτρέπουν την πρόσβαση στο προφίλ τους έχουν περισσότερες πιθανότητες να δημοσιοποιήσουν σε αυτές προσωπικά στοιχεία, όπως είναι το τηλέφωνο και η διεύθυνσή τους, σύμφωνα με τα στοιχεία της έρευνας.

ΚΕΦΑΛΑΙΟ 3: ΜΕΘΟΔΟΛΟΓΙΑ

3.1 Στόχος της έρευνας

Η παρούσα έρευνα έχει ως στόχο την ενημέρωση των εκπαιδευτικών για την ασφάλεια στο διαδίκτυο με τη συνδρομή πολυμεσικού υποστηρικτικού υλικού η οποία διευκολύνεται μέσα από μια ιστοσελίδα, την BEsafe, όπου παρουσιάζονται ιδέες για δραστηριότητες τόσο σε εκπαιδευτικούς όσο και σε γονείς ώστε να βοηθήσουν τους μαθητές να κατανοήσουν και να οχυρωθούν απέναντι στους κινδύνους που ενέχει το διαδίκτυο.

Επίσης, η εν λόγω ιστοσελίδα περιέχει συνοδευτικό υλικό μιας άλλης δικτυακής τοποθεσίας, δηλαδή της www.safesocialmedia.org. Η τοποθεσία αυτή στοχεύει στην καταπολέμηση της βίας των μέσων κοινωνικής δικτύωσης και στην ενίσχυση της επίγνωσης των παιδιών, των εκπαιδευτικών και των γονέων σχετικά με τους κινδύνους των μέσων αυτών. Επίσης, αποσκοπεί στην ενημέρωσή τους σε ό, τι αφορά την ασφαλή τους χρήση. Συγκεκριμένα, σχετίζεται με:

1. Δημιουργία ψηφιακών μαθησιακών αντικειμένων σε όλες τις γλώσσες των εταίρων (Ελληνικά, Αυστριακά, Ιταλικά και Αγγλικά) για τους τρόπους προστασίας και καταπολέμησης ενάντια στους κινδύνους των εφαρμογών κοινωνικής δικτύωσης.

2. Ανάπτυξη σχεδίων μαθήματος που θα συνοδεύουν τα ψηφιακά μαθησιακά αντικείμενα, ώστε οι εκπαιδευτικοί στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση να μπορούν να τα χρησιμοποιήσουν στην τάξη. Επίσης, η δημιουργία των σχεδίων μαθήματος θα μπορούσε να αξιοποιηθεί και για την εκπαίδευση των γονέων.

3. Οργάνωση εργαστηρίων, ημερίδων και ειδικών εκδηλώσεων για την εκπαίδευση των γονέων από τους εκπαιδευτικούς πρόσωπο με πρόσωπο ώστε να ενημερώνονται καλύτερα τα παιδιά τους σχετικά με τους τρόπους που μπορούν να προστατευθούν από τους κινδύνους των εφαρμογών κοινωνικής δικτύωσης.

4. Διεξαγωγή δραστηριοτήτων διάδοσης αξιοποιώντας παραδοσιακά (φυλλάδια, σεμινάρια, δελτία τύπου) και ιδιαίτερα διαδικτυακά μέσα κοινωνικής δικτύωσης.

5. Δημιουργία επαφών με άλλα συναφή προγράμματα και πρωτοβουλίες των ΜΚΟ, με οργανισμούς κατάρτισης, με συλλόγους εκπαιδευτικών και με τα υπουργεία παιδείας.

3.2 Λειτουργικοί Ορισμοί

Ασφάλεια είναι η κατάσταση εκείνη, στην οποία υπάρχει η αίσθηση ότι δεν υπάρχει κίνδυνος ή απειλή. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας. Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του. Συγκεκριμένα, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες.

Καθώς λοιπόν το διαδίκτυο είναι πλέον ένα ισχυρότατο μαθησιακό εργαλείο, η ανάγκη ενημέρωσης εκπαιδευτικών αλλά και γονέων πάνω σε θέματα καλής και ασφαλούς χρήσης του κρίνεται ολοένα και πιο επιτακτική. Το καλύτερο «τείχος προστασίας» είναι η επαφή των εκπαιδευτικών και των γονέων με τα παιδιά.

3.3 Ερευνητική Μέθοδος

Η ερευνητική μέθοδος που χρησιμοποιήθηκε για την αξιολόγηση των ιστοτόπων BEsafe και Safesocialmedia ήταν η έρευνα. Η έρευνα, η πιο δημοφιλής μέθοδος που ευνοείται από τους υπολογιστές, επιτρέπει ένα μικρό αριθμό πληροφοριών για ένα πιθανό μεγάλο αριθμό ερωτηθέντων. Έχει σα σκοπό να σχεδιάσει, να εφαρμόσει, να επισκοπήσει και να αξιολογήσει τους ιστοτόπους που σχεδιάστηκαν για να λύσει τυχόν προβλήματα που προέκυψαν. Επίσης, να ενδυναμώσει τους συμμετέχοντες μέσω της εμπλοκής τους στην έρευνα.

Η έρευνα χρειάζεται τον καθορισμό μεθόδων δειγματοληψίας και καλοσχεδιασμένες, αποφασιστικές ερωτήσεις, ίσως ένα δοκιμαστικό τεστ και μια λίστα ερωτήσεων που θα είναι όσο το δυνατόν μικρότερη για να εξασφαλίσει τη συνοχή των απαντήσεων, δηλαδή ότι όλες οι ερωτήσεις απαντώνται από κάθε ερωτηθέντα.

Ο συγκεκριμένος τύπος ερευνητικής μεθόδου που βασίζεται σε δειγματοληπτική έρευνα με τυποποιημένο ερωτηματολόγιο, προσφέρει τη δυνατότητα στον ερευνητή να προσεγγίσει μεγάλο μέρος του πληθυσμού για τον έλεγχο της θεωρίας. Όταν τα αποτελέσματα της έρευνας στηρίζονται σε μεγάλο

αριθμό περιπτώσεων, η γενική αντίληψη είναι ότι οι θεωρητικές υποθέσεις υποβάλλονται σε πιο αυστηρό και έγκυρο έλεγχο. Η τυποποίηση των στοιχείων που συλλέγονται, η δυνατότητα προσέγγισης μεγάλου μέρους πληθυσμού και η επιδεκτικότητα των στοιχείων σε στατιστικές μεθόδους ανάλυσης καθιστούν την έρευνα ως την πιο διαδεδομένη μορφή εμπειρικής έρευνας για τη μελέτη των κοινωνικών φαινομένων (Κυριαζή, 2002). Για να καταλήξει ο ερευνητής σε έγκυρα και επιστημονικά αποτελέσματα δύο είναι τα βασικά ζητήματα που πρέπει να εστιάσει. Πρώτον στη συλλογή ενός αντιπροσωπευτικού δείγματος του υπό μελέτη πληθυσμού και δεύτερον στη διαμόρφωση ενός κατάλληλου για την έρευνα ερωτηματολογίου.

3.4 Δείγμα Έρευνας

Σκοπός της παρούσας έρευνας είναι να διαπιστωθεί κατά πόσο οι δύο ιστότοποι συμβάλλουν στην πλήρη ενημέρωση των εκπαιδευτικών για την ασφάλεια στο διαδίκτυο με τη συνδρομή πολυμεσικού υποστηρικτικού υλικού όπου παρουσιάζονται ιδέες για δραστηριότητες τόσο σε εκπαιδευτικούς όσο και σε γονείς ώστε να βοηθήσουν τους μαθητές να κατανοήσουν και να οχυρωθούν απέναντι στους κινδύνους που ενέχει το διαδίκτυο. Για αυτό το λόγο ήταν απαραίτητο οι ερωτηθέντες να είναι εκπαιδευτικοί και να έχουν ένα προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου (e-mail).

Η βάση των εκπαιδευτικών που απάντησαν το συγκεκριμένο ερωτηματολόγιο αποτελείται από τους συμμετέχοντες εκπαιδευτικούς στην περσινή και φετινή έκθεση E-Learning Expo[2] που έδειξαν ένα ιδιαίτερο ενδιαφέρον για την Ασφαλή χρήση του Διαδικτύου. Συγκεκριμένα, το ερωτηματολόγιο στάλθηκε -σε 48 εκπαιδευτικούς, από τους οποίους ανταποκρίθηκαν οι 32 οι οποίοι το απάντησαν και αποτελούν το δείγμα της έρευνας.

[2]Η μοναδική εξειδικευμένη έκθεση στο e-learning πραγματοποιείται εδώ και 4 χρόνια, προσφέροντας τη μοναδική δυνατότητα στους επισκέπτες της να διερευνήσουν τις ευκαιρίες, που κρύβει το e-learning, αλλά και τις μελλοντικές προοπτικές του. Επισκέπτες - γονείς, εκπαιδευτικοί, μαθητές, φοιτητές, στελέχη κατάρτισης και δια βίου μάθησης, σύμβουλοι εκπαίδευσης, στελέχη ανθρωπίνων πόρων, προγραμματιστές και όσοι άλλοι ενδιαφέρονται - έχουν την ευκαιρία να γνωρίσουν από κοντά τα σημαντικότερα θέματα και τις νέες τάσεις της χρήσης των τεχνολογιών, πληροφορικής και επικοινωνιών, στην εκπαίδευση και την κατάρτιση. (Για περισσότερες πληροφορίες: http://www.elearningexpo.gr/)

3.5 Ερευνητικά Εργαλεία

Η έρευνα χρησιμοποιήθηκε ώστε να προβλεφθεί και να κατανοηθεί η συμπεριφορά του τμήματος του δείγματος που μας ενδιαφέρει. Η συλλογή των πληροφοριών έγινε με τη βοήθεια ερωτηματολογίου. Η έρευνα περιλαμβάνει δειγματοληψία, το σχεδιασμό του ερωτηματολογίου, τη συμπλήρωση του ερωτηματολογίου και την ανάλυση των στοιχείων (Σταθακόπουλος, 2005).

Το ερωτηματολόγιο αποτελεί το μέσον επικοινωνίας (interface) μεταξύ του ερευνητή και των ερωτηθέντων, με άμεσο ή έμμεσο τρόπο, ανάλογα με τη μέθοδο συλλογής των δεδομένων. Η κατάρτιση του ερωτηματολογίου, λόγω των ιδιοτήτων που έχει, αποτελεί την πλέον κρίσιμη και λεπτή εργασία, καθοριστικής σημασίας για την επιτυχία μιας στατιστικής έρευνας.

Λέγεται χαρακτηριστικά ότι «*καμία στατιστική έρευνα δεν μπορεί να είναι καλύτερη από το ερωτηματολόγιο που χρησιμοποιήθηκε σ' αυτή*» (Παρασκευόπουλος, 1993). Με τη φράση αυτή τονίζεται το γεγονός ότι σε μια έρευνα ακόμη και αν εφαρμοστεί αποτελεσματικό σχέδιο δειγματοληψίας δεν είναι δυνατόν να εξαχθούν σωστά συμπεράσματα ακόμα και αν έχουν ληφθεί μη συγκρίσιμες απαντήσεις από ένα ακατάλληλο ερωτηματολόγιο με ασαφείς ερωτήσεις.

Η μέθοδος που χρησιμοποιήθηκε για τη συμπλήρωση του ερωτηματολογίου ήταν η συνέντευξη μέσω Internet (online survey). Σύμφωνα με τη μέθοδο αυτή το ερωτηματολόγιο τοποθετήθηκε σε κάποια ιστοσελίδα με τη βοήθεια του surveymonkey (Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://www.surveymonkey.com/s/NRSP8ZT). Η μέθοδος αυτή επιλέχτηκε λόγω της ευκολίας που προσφέρει στο χρήστη καθώς επίσης και της ταχύτητας κα χαμηλού κόστους. Συγκεκριμένα, το ερωτηματολόγιο στάλθηκε μέσω ηλεκτρονικού ταχυδρομείου (e-mail) σε εκπαιδευτικούς. Ο χρόνος συμπλήρωσης του ερωτηματολογίου υπολογίστηκε στα 5-7 λεπτά της ώρας.

3.6 Υλικά

3.6.1 Τι είναι το Weebly

Το Weebly είναι μια από τις διαδικτυακές εφαρμογές που υποστηρίζουν τη δυνατότητα δωρεάν δημιουργίας ιστοχώρου. Αν κάποιος χρήστης θέλει να έχει δικό

του domain τότε θα πρέπει να πληρώσει. Τα sub-domains, όμως, προσφέρονται χωρίς επιβάρυνση.

Η δημιουργία της ιστοσελίδας είναι απλή και γρήγορη και βασίζεται σε μια εύκολη drag-and-drop διασύνδεση**,** χωρίς να απαιτείται γνώση html από το δημιουργό της. Το Weebly προσφέρει μια μεγάλη ποικιλία από πρότυπα (templates) που μπορούν να χρησιμοποιηθούν καθώς, επίσης, και τη δυνατότητα στους κατασκευαστές της να επεξεργαστούν και να προσαρμόσουν την εικόνα της κεφαλίδας.

3.6.1.1 Γενικές πληροφορίες για το Weebly

Το Weebly δημιουργήθηκε το 2006 και ήδη πάνω από 8.000.000 ιδιώτες και επιχειρήσεις το έχουν επιλέξει για να δημιουργήσουν τη διαδικτυακή τους παρουσία. Η πλατφόρμα του Weebly προσφέρει στους χρήστες μια σειρά από πρότυπα, εργαλεία και δυνατότητες για να δημιουργήσει ο καθένας τη δική του ιστοσελίδα χωρίς ιδιαίτερο κόπο και ειδικές γνώσεις HTML ή κάποιας άλλης γλώσσας προγραμματισμού.

Στο Weebly μπορεί ο κάθε χρήστης να φτιάξει το δικό του ηλεκτρονικό κατάστημα, ενσωματώνοντας μάλιστα το PayPal Shopping Cart ή το Google Checkout, προς διευκόλυνση των πελατών του. Επίσης, μπορεί εύκολα να δημιουργήσει το δικό του ιστολόγιο ή την επαγγελματική του ιστοσελίδα.

Αφού καταχωρηθεί το όνομα του δημιουργού, η διεύθυνση e-mail του και το «Captcha» γίνει με επιτυχία, οριστεί το όνομα της ιστοσελίδας και το αντικείμενο της, αν π.χ. θα είναι προσωπική, επαγγελματική κλπ. Αμέσως μετά, ο δημιουργός επιλέγει τη διεύθυνση που επιθυμεί. Μπορεί να χρησιμοποιήσει μια υποδιεύθυνση του Weebly.com, να κατοχυρώσει μια καινούρια διεύθυνση της επιλογής του μέσα από την πλατφόρμα, ή να χρησιμοποιήσει μια διεύθυνση που ήδη έχει στην ιδιοκτησία του. Αφού κάνει την επιλογή του, θα οδηγηθεί στη σελίδα επεξεργασίας της ιστοσελίδας του, όπου θα βρει ένα πρότυπο θέμα εμφάνισης ήδη φορτωμένο και έτοιμο να το επεξεργαστεί. Από εκεί και πέρα, μπορεί να χρησιμοποιήσει τα δεκάδες εργαλεία του Weebly, για να διαμορφώσει τη σελίδα του.

3.6.1.2 Πλεονεκτήματα του Weebly

Στη συγκεκριμένη ενότητα θα γίνει αναφορά στα σημαντικά πλεονεκτήματα του Weebly, τα οποία είναι τα ακόλουθα:

• Είναι εύχρηστο, απλό και κατανοητό, ακόμα και από κάποιον που δεν έχει καμία εμπειρία στη δημιουργία ιστοσελίδων και στην HTML.
• Έχει εκατοντάδες πρότυπα θέματα για όλα τα γούστα και, μετά βεβαιότητας, ο χρήστης θα βρει κάτι που θα τον ενδιαφέρει.
• Παρέχει όλα τα βασικά εργαλεία για τη δημιουργία μιας βασικής ιστοσελίδας και, μάλιστα, με λίγο χρόνο και χωρίς πολλές δυσκολίες.
• Η φιλοξενία του είναι αρκετά αξιόπιστη.

3.6.1.3 Εργαλεία του Weebly

Στη συνέχεια αναφέρονται αναλυτικά τα σημαντικότερα εργαλεία που προσφέρει το Weebly.

Στην καρτέλα **«Elements»**, υπάρχουν όλα τα στοιχεία τα οποία μπορούν να τοποθετηθούν στη σελίδα που πρόκειται να δημιουργηθεί. Μπλοκ κειμένου, παράγραφοι, φωτογραφίες και παρουσιάσεις, φόρμες επικοινωνίας, χάρτες, παιχνίδια ακόμα και περιεχόμενο Flash. Οι πιο προχωρημένοι χρήστες μπορούν να τοποθετήσουν επίσης και RSS Reader, Google AdSense και φυσικά να παρέμβουν στον ίδιο τον κώδικα, μέσω του επεξεργαστή HTML. Το εντυπωσιακό είναι ότι όλες αυτές οι δυνατότητες μπορούν να προστεθούν πολύ εύκολα, με τη χρήση μόνο του ποντικιού.

Στην καρτέλα **«Design»**, ο χρήστης μπορεί να διαμορφώσει το βασικό σχεδιασμό της ιστοσελίδας του, επιλέγοντας από πάρα πολλά πρότυπα και θέματα εμφάνισης. Από εδώ, επίσης με την πολύ γρήγορη και αποτελεσματική λειτουργία επεξεργασίας, μπορεί να επιλεχθεί η γραμματοσειρά και το μέγεθος των γραμμάτων που θα χρησιμοποιηθούν στην ιστοσελίδα.

Στην καρτέλα **«Pages»**, ο χρήστης μπορεί να διαχειριστεί τις σελίδες της διαδικτυακής του τοποθεσίας. Εδώ, μπορεί να δημιουργήσει, να αντιγράψει ή να διαγράψει σελίδες, καθώς και να κατασκευάσει τα μενού πλοήγησης. Σε αυτή την καρτέλα, του δίνεται η δυνατότητα επίσης να κάνει και τις πρώτες του κινήσεις στο χώρο του SEO, ορίζοντας τον τίτλο, την περιγραφή και τα META Keywords κάθε σελίδας, αλλά και να παρέμβει στον κώδικα του Header και του Footer.

Μέσω της λειτουργίας **«Editors»**, έχει τη δυνατότητα να δηλώσει τα προνόμια πρόσβασης στη σελίδα του, το ποιος θα έχει δικαιώματα διαχειριστή, αλλά και το αν θα υπάρχουν άλλοι χρήστες και τι βαθμό πρόσβασης θα έχουν σε αυτή.

Τέλος, μέσω της λειτουργίας **«Settings»**, δίνονται στο χρήστη διάφορες επιλογές, όπως το να αλλάξει το όνομα της σελίδας, το να επεξεργαστεί το Header και το Footer, αν π.χ. θέλει να εγκαταστήσει το Google Analytics ή τα εργαλεία του Google Webmaster Tools. Από εδώ, μπορεί να κάνει επίσης αναβάθμιση στο Weebly Pro, το οποίο αναλύεται στη συνέχεια.

3.6.2 Το Weebly στην εκπαίδευση

Όσον αφορά τον τομέα της εκπαίδευσης, το Weebly αποτελεί μια δωρεάν υπηρεσία για τους εκπαιδευτικούς και τους μαθητές, το οποίο τους διευκολύνει στην εύκολη και γρήγορη δημιουργία ιστοσελίδων (χρησιμοποιείται από πάνω από 100.000 εκπαιδευτικούς και μαθητές).

Επίσης, το Weebly διακρίνεται από το απλό και έξυπνο περιβάλλον εργασίας, το οποίο είναι φιλικό στους εκπαιδευτικούς και στους μαθητές. Γι' αυτό το λόγο και έχει μπει δυναμικά και στο χώρο της εκπαίδευσης και υποστηρίζει πλέον σχολεία και πανεπιστήμια. Το weebly_for_education προσφέρει όλα τα εργαλεία που μπορεί να βρει κάποιος στο weebly αλλά προσφέρει και χαρακτηριστικά ειδικά για την τάξη.

Πιο συγκεκριμένα το Weebly προσφέρει στους εκπαιδευτικούς τα εξής:

1. Ο εκπαιδευτικός μπορεί να δημιουργήσει ξεχωριστό λογαριασμό για κάθε μαθητή, τον οποίο να παρακολουθεί και να διαχειρίζεται (ωστόσο η δωρεάν υπηρεσία προσφέρεται για 40 μαθητές).
2. Ο εκπαιδευτικός μπορεί να δημιουργήσει ισχυρές ιστοσελίδες στην τάξη (που να περιλαμβάνουν συλλογή από φωτογραφίες, βίντεο, ηχητικά αποσπάσματα, blogs, φόρμες επικοινωνίας κ.α.)
3. Να δώσει στους μαθητές ένα νέο και συναρπαστικό τρόπο για να εκφραστούν δημιουργικά.
4. Ο εκπαιδευτικός μπορεί να επιλέξει αν οι ιστοσελίδες των μαθητών θα είναι private ή public (οι private σελίδες δε φαίνονται στις μηχανές αναζήτησης).

Στη συγκεκριμένη περίπτωση, καλό είναι να αναφερθεί η σημαντική δυνατότητα που δίνει το weebly στους μαθητές:

- Χρησιμοποίηση του παραπάνω λογαριασμού για τη δημιουργία του δικού τους site κάνοντας login στο http://students.weebly.com.
- Κατασκευή ελκυστικών και πλούσιων σε ενημέρωση ιστοσελίδων.
- Εργασία μέσα σε ένα ελεγχόμενο και διασκεδαστικό περιβάλλον.

- Παρουσίαση της δουλειάς τους σε ένα αυτο-δημιούργητο e-portfolio.
- Δημιουργία εργασιών και e-portfolios.
- Μη ύπαρξη διαφημίσεων στις σελίδες που δημιουργούνται.

Στα πλαίσια της έρευνας που υλοποιήθηκε, χρησιμοποιήθηκε το Weebly διότι ικανοποιεί τα παρακάτω κριτήρια που αφορούν την εύκολη χρήση του.

Πίνακας 1: Κριτήρια για την προτίμηση στη χρήση του Weebly

ΚΡΙΤΗΡΙΑ	ΣΧΟΛΙΑ
Ευκολία στη χρήση	Οργάνωση και λειτουργία ιστοσελίδας σε ελάχιστο χρόνο.
Επιλογή προτύπου (flexibility) και ευελιξία	Τα σχέδια δεν είναι ιδιαίτερα συναρπαστικά αλλά προσφέρουν πρόσβαση στον πηγαίο κώδικα για προσαρμογή.
Δωρεάν Διαφήμιση	Μόνο στην Pro έκδοση. Η δωρεάν έκδοση έχει ένα μικρό διαφημιστικό σύνδεσμο στο υποσέλιδο.
Γλώσσες	Επί του παρόντος διατίθεται στα αγγλικά, γαλλικά, ισπανικά, γερμανικά, ιταλικά και κινέζικα. Διαθέσιμη υποστήριξη μόνο στην αγγλική γλώσσα. Δεν υπάρχει κάποιο ιδιαίτερο χαρακτηριστικό για τη δημιουργία πολυγλωσσικών sites.
Χαρακτηριστικά	
Κατάλληλο domain name	Μπορείτε να αγοράσετε ένα domain name από το Weebly, αλλά είναι αρκετά ακριβό και προσφέρει μόνο το .com, .net ή .org domains.
Βάθος πλοήγησης	Απεριόριστο. Ένα drop-down menu προστίθεται αυτόματα στην μπάρα πλοήγησης.
Widgets (μικρά εργαλεία για την προσθήκη επιπλέον λειτουργικότητας)	Γκαλερί φωτογραφιών, βίντεο, μουσικής κ.α.

Ηλεκτρονικό Εμπόριο	Απλό κατάστημα, αλλά δέχεται πληρωμές μόνο μέσω PayPal ή το Google Checkout.
Search-engine optimization (SEO)	Τίτλος, μετα-δεδομένα, περιγραφή tags είναι όλα προσαρμοσμένα σε επίπεδο σελίδας. Το URL κείμενο δημιουργείται πάντα από το αντίστοιχο menu.
Blog	Έχει όλες τις βασικές λειτουργίες e.g. comment moderation and trackbacks.
Στατιστικά επισκεψιμότητας	Το Weebly έχει το δικό του εργαλείο εντοπισμού του αλλά υπάρχει και η δυνατότητα χρήσης του Google Analytics.
Φόρμα επικοινωνίας	Χρησιμοποίηση του drag and drop για τη δημιουργία λεπτομερών φορμών επικοινωνίας ή έρευνες.
Προσθήκη HTML κώδικα	Δυνατότητα προσθήκης εξωτερικών widgets και άλλων εργαλείων.
Αποθηκευτικός χώρος	Ατομικά, τα αρχεία δεν μπορούν να υπερβαίνουν τα 5MB το καθένα για τη δωρεάν έκδοση ή τα 100MB το καθένα για την Pro έκδοση.
Φόρουμ	Άμεση ενσωμάτωση φόρουμ με Tal.ki.
Υποστήριξη	Υπάρχει αρμόδια τεχνική υποστήριξη που απαντάει γρήγορα στις ερωτήσεις των χρηστών.
Συνολική Βαθμολόγηση	Το Weebly αποτελεί έναν από τους καλύτερους τρόπους για τη δημιουργία ιστοσελίδων.

(Πηγή: http://www.websitetooltester.com/en/reviews/weebly-review/)

3.6.3 Κόστος και Προτερήματα Αναβάθμισης

Το Weebly κατά κύριο λόγο είναι δωρεάν, δηλαδή το βασικό πακέτο που προσφέρει είναι δωρεάν αλλά περιλαμβάνει μια μικρή διαφήμιση «Weebly» στο υποσέλιδο της ιστοσελίδας. Για επιπρόσθετες λειτουργίες υπάρχει και η έκδοση "Pro", στην αγορά της οποίας προβαίνουν οι εκπαιδευτικοί για να μπορέσουν να έχουν περισσότερες λειτουργίες. Το Weebly Pro κοστίζει $ 39.95/yr. Στην περίπτωση που ένας εκπαιδευτικός αναβαθμίσει την υπηρεσία του Weebly σε Pro, επίσης όλοι οι λογαριασμοί των φοιτητών που διαχειρίζεται ο εκπαιδευτικός αυτομάτως θα αναβαθμιστούν.

Από τα πολλά χαρακτηριστικά και τα πρόσθετα εργαλεία που προσφέρει το Weebly Pro, θα γίνει αναφορά μόνο σε πέντε που θεωρούνται τα πιο σημαντικά. Με το Weebly Pro:

1. Δίνεται η δυνατότητα για δημιουργία μέχρι 10 ιστοσελίδων στο λογαριασμό του χρήστη, ενώ με το δωρεάν λογαριασμό μπορεί να έχει μόνο δύο.
2. Μπορεί ο κάθε χρήστης να ανεβάσει αρχεία μεγέθους έως 100MB και μάλιστα όσα θέλει, ενώ με το δωρεάν λογαριασμό μπορεί να ανεβάσει μόνο αρχεία έως 5MB το καθένα.
3. Ως χρήστης Pro απολαμβάνει και Pro εξυπηρέτηση, αφού το τμήμα υποστήριξης επικοινωνεί μαζί του προνομιακά, σε σχέση με τους δωρεάν χρήστες.
4. Έχει τη δυνατότητα να αφαιρέσει το διαφημιστικό σύνδεσμο με το μήνυμα «Create a free website with Weebly», που βρίσκεται στο Footer, καθώς και να επεξεργαστεί το Footer και να γράψει τα δικά του μηνύματα.
5. Τέλος, ως χρήστης Pro, μπορεί να ενσωματώσει πολυμέσα και έγγραφα απ' ευθείας στο λογαριασμό του.

Το κόστος της υπηρεσίας είναι $4,58 το μήνα για εξάμηνη συνδρομή, $3,99 το μήνα για ετήσια συνδρομή και $2,99 το μήνα για διετή συνδρομή.

Αν, μάλιστα, αποφασίσει να χρησιμοποιήσει την Pro έκδοση, συμφέρει να κατοχυρώσει και διεύθυνση μέσω του Weebly, αφού η ετήσια συνδρομή συν το κόστος κατοχύρωσης κοστίζει $39,95, λιγότερο δηλαδή από την ετήσια μόνο συνδρομή, εφ' όσον πληρώνει μηνιαίως.(Greekaffiliates, 2011)

Στη συνέχεια παρουσιάζονται οι βασικές διαφορές μεταξύ των επιλογών του Weebly και του pro Weebly:

Πίνακας 2: Διαφορές μεταξύ του Weebly και του pro Weebly

	Λογαριασμός Εκπαιδευτή		Υπο-Λογαριασμοί Μαθητών	
	Δωρεάν Έκδοση	Έκδοση Pro	Δωρεάν Έκδοση	Έκδοση Pro
#ιστοσελίδες ανά λογαριασμό	2	10	1	10
# σελίδες στην ιστοσελίδα	Απεριόριστο	Απεριόριστο	5	Απεριόριστο
Στοιχείο Audio player	-	Ναι	-	Ναι
Στοιχείο Video player	-	Ναι	-	Ναι
Ενσωματωμένο στοιχείο εγγράφου	-	Ναι	-	Ναι
Οι κωδικοί πρόσβασης προστατεύουν τις ιστοσελίδες	-	Ναι	Ναι	Ναι
Ελεύθερο όριο (ανά αρχείο φόρτωσης)	5MB	100MB	5MB	100MB
Διαφημίσεις	Όχι_διαφημίσεις	Όχι_διαφημίσεις	Όχι_διαφημίσεις	Όχι_διαφημίσεις
Διαγραφή μηνύματος Weebly footer	-	Ναι	Οι ιστοσελίδες των μαθητών έχουν σύνδεση (log in).	

(Πηγή: http://ade2010digitalportfolios.wikispaces.com/file/view/Weebly+for+Education+-+Info.pdf)

3.7 Διαδικασία

Σε αυτό το κεφάλαιο παρουσιάζεται μια εκτενής ανάλυση του τρόπου με τον οποίο δομήθηκε η ιστοσελίδα BEsafe έτσι ώστε να ταιριάζει με τις ανάγκες της παρούσας έρευνας. Η δομή του περιεχομένου της ιστοσελίδας είναι ιδιαίτερα σημαντική έτσι ώστε οι επισκέπτες να πλοηγούνται στο περιεχόμενο εύκολα και γρήγορα.

3.7.1. Δημιουργία του BEsafe

Για τη δημιουργία της εν λόγω ιστοσελίδας, αρχικά, προτείνεται η χρήση σύνδεσης ADSL για την πρόσβαση και τη χρήση της υπηρεσίας. Βασική προϋπόθεση είναι η χρήση ενός λογαριασμού ηλεκτρονικού ταχυδρομείου του δημιουργού.

• **Γλώσσα χρήσης της υπηρεσίας.**

Το περιβάλλον χρήσης της υπηρεσίας είναι πολυγλωσσικό. Στις υποστηριζόμενες γλώσσες δεν υπάρχει η ελληνική. Η ευκολία που παρουσιάζει το περιβάλλον χρήσης της υπηρεσίας δε θα προβληματίσει ούτε το δημιουργό ούτε το κοινό στο οποίο απευθύνεται. Τα δεδομένα που εισάγονται μπορεί να είναι στην ελληνική γλώσσα χωρίς κανένα πρόβλημα.

• Περιβάλλον χρήσης της υπηρεσίας.

Ο δημιουργός κάνει μια εγγραφή χρησιμοποιώντας την προσωπική του διεύθυνση ηλεκτρονικού ταχυδρομείου. Με την είσοδό του στο σύστημα χρειάζεται να ρυθμίσει τα στοιχεία του στο λογαριασμό (Account Settings).

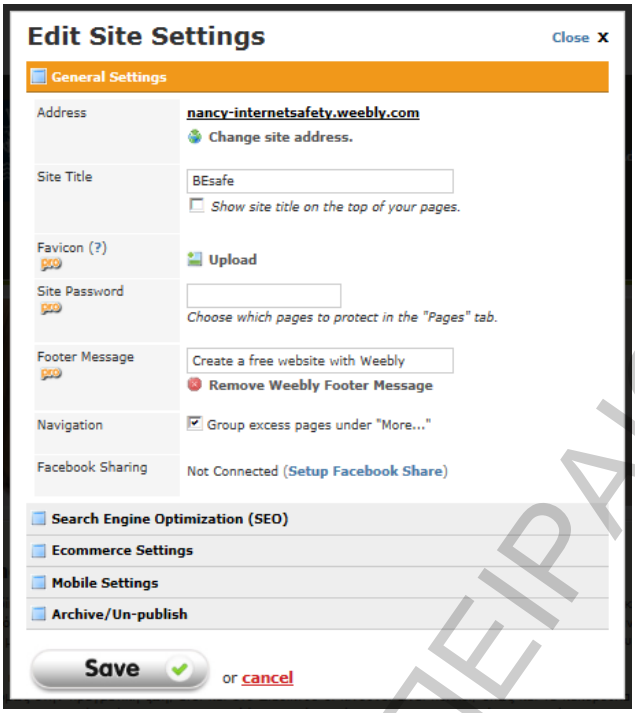
Μόλις ο χρήστης ολοκληρώσει την εγγραφή του, τότε είναι σε θέση να δημιουργήσει την ιστοσελίδα. Η ιστοσελίδα πρέπει να είναι δημόσια και να ανιχνεύεται από τις μηχανές αναζήτησης.

Τα βήματα που ακολουθήθηκαν για τη δημιουργία της BEsafe ιστοσελίδας είναι τα ακόλουθα:

1ο ΒΗΜΑ: Ορισμός ονόματος

Ορισμός ενός ονόματος ως διεύθυνση του χώρου, το οποίο όνομα μπορεί να είναι μια αγγλική λέξη ή μια ελληνική με λατινικούς χαρακτήρες.

Από την καρτέλα Settings γίνεται η καταχώρηση του επιθυμητού domain name της ιστοσελίδας, το οποίο στη συγκεκριμένη περίπτωση είναι http://nancy-internetsafety.weebly.com. Επίσης, δίνεται η δυνατότητα για λήψη ενός αρχείου zip με τα αρχεία της ιστοσελίδας εφόσον ο χρήστης επιθυμεί να επιλέξει κάποια άλλη υπηρεσία web hosting.



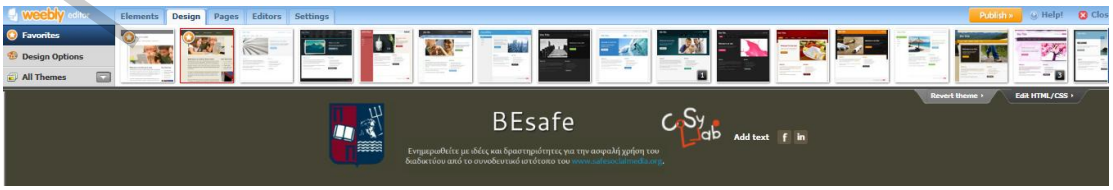
Εικόνα 1:1ο ΒΗΜΑ: Ορισμός Ονόματος - 2ο ΒΗΜΑ: Επιλογή ενός τίτλου για την ιστοσελίδα

2ο ΒΗΜΑ: Επιλογή ενός τίτλου για την ιστοσελίδα.

Στην προκειμένη περίπτωση θα χρησιμοποιηθεί το όνομα «BEsafe», όπως φαίνεται στην παραπάνω εικόνα. Η πληκτρολόγηση του τίτλου γίνεται από την καρτέλα Settings (Ρυθμίσεις).

3ο ΒΗΜΑ: Εμφάνιση της ιστοσελίδας.

Από την καρτέλα Design (σχεδιασμός) έγινε η επιλογή του κατάλληλου προτύπου (template). Υπάρχει δυνατότητα επέμβασης στην εμφάνιση του πρότυπου σε σημείο μάλιστα να γίνεται αγνώριστο. Η επιλογή Design Option προσφέρει δυνατότητα για άμεση αλλαγής γραμματοσειράς, μέγεθος και χρώματος σε κάθε περίπτωση (τίτλο, παράγραφο κ.α.). Όσοι εκπαιδευτικοί έχουν γνώσεις στην σχεδίαση ιστοσελίδων μπορούν να επέμβουν και στο HTML/CSS κώδικα. Οι εικόνες στο πρότυπο αλλάζουν άμεσα με ένα κλικ πάνω σε αυτές.



Εικόνα 2: 3ο ΒΗΜΑ: Εμφάνιση του ιστοτόπου BEsafe

4ο ΒΗΜΑ: Δημιουργία σελίδων ή ιστολογίων (blogs).

Πριν γίνει η εισαγωγή των αντικειμένων ο χρήστης πρέπει να δημιουργήσει τις σελίδες της ιστοσελίδας. Έχει τη δυνατότητα να επιλέξει απλές ιστοσελίδες ή ιστολόγια (blogs). Σε κάθε περίπτωση πρέπει να γράψει το όνομα, τον τίτλο και μια περιγραφή. Για τα δύο τελευταία χρειάζεται να επιλέξει το Advanced Settings για κάθε σελίδα. Έχει δηλαδή τη δυνατότητα:

1.Διαχείριση σελίδων (Pages).

2.Δημιουργία νέας σελίδας.

3.Δημιουργία νέου ιστολόγιου (Blog).

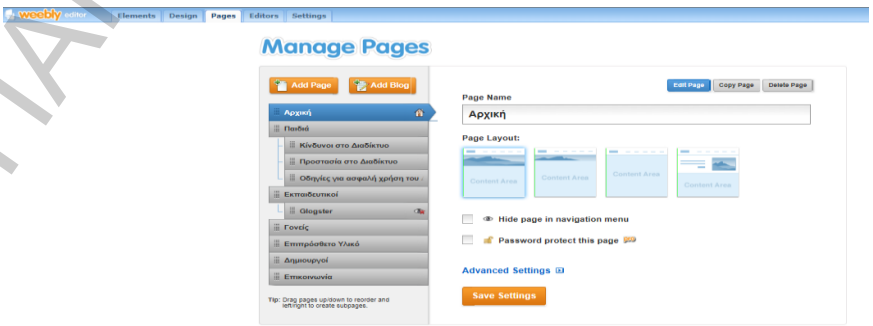
4.Εισαγωγή ονόματος στη σελίδα.

5.Καθορισμός εμφάνισης ή όχι στο menu της σελίδας.

6.Εισαγωγή στοιχείων σελίδας (τίτλος, περιγραφή, λέξεις κλειδιά, κώδικας).

Από την καρτέλα Pages (σελίδες) έγινε η δημιουργία των σελίδων και των υπο-σελίδων. Συγκεκριμένα, εδώ δημιουργήθηκαν επτά (7) σελίδες και τρεις (3) υπο-σελίδες με τα εξής ονόματα:

1) Αρχική
2) Παιδιά
    a. Κίνδυνοι στο Διαδίκτυο
    b. Προστασία στο Διαδίκτυο
    c. Οδηγίες για ασφαλή χρήση του Διαδικτύου
3) Εκπαιδευτικοί
4) Γονείς
5) Επιπρόσθετο Υλικό
6) Δημιουργοί
7) Επικοινωνία



Εικόνα 3: 4ο ΒΗΜΑ: Δημιουργία σελίδων ή ιστολογίων (blogs)

Εικόνα 4: Εμφάνιση Σελίδων - Υποσελίδων του ιστότοπου BEsafe

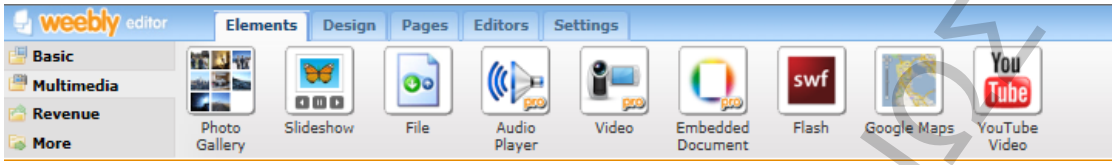
5ο ΒΗΜΑ: Προσθήκη αντικειμένων και περιεχομένου στις σελίδες.

Η προσθήκη των αντικειμένων γίνεται από την καρτέλα Elements με τον πιο εύκολο τρόπο που υπάρχει στο χώρο της σχεδίασης. Απλά χρειάζεται να συρθεί το αντικείμενο της καρτέλας Elements στο πεδίο της ιστοσελίδας (κάτω μέρος). Από εκείνη τη στιγμή κι έπειτα μπορούν να εισαχθούν τα δεδομένα από το δημιουργό. Τα αντικείμενα χωρίζονται σε διάφορες κατηγορίες (Βασικά, Πολυμέσα, Προϊόντα, Διάφορα).

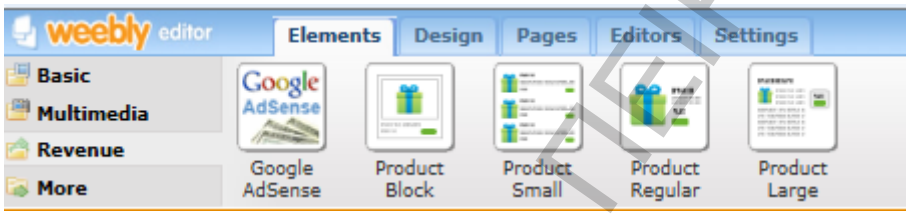
Τα πιο χρήσιμα αντικείμενα για τους εκπαιδευτικούς είναι:

1) Διπλή στήλη για την τοποθέτηση αντικειμένων (Two Column Layout).
2) Κείμενο με τίτλο, εικόνα και παράγραφο (Paragraph with Picture).
3) Φόρμα εισαγωγής στοιχείων. Όλα αποστέλλονται στο ηλεκτρονικό ταχυδρομείο του δημιουργού (Contact Form, RVP Form, Contact Form, Assignment Form).
4) Εικόνα/Φωτογραφία (Picture).
5) Gallery φωτογραφιών ή προβολή Slides (Photo Gallery, Slideshow).
6) Αποστολή αρχείου (File).
7) Flash αρχείο για προβολή εκπαιδευτικού υλικού ή παιχνιδιού (Flash).
8) Χάρτης της υπηρεσίας Google Maps για προσδιορισμό του τόπου που βρίσκεται η σχολική μονάδα του τμήματος.
9) Βίντεο της υπηρεσία Youtube για προβολή δραστηριοτήτων του τμήματος.
10) Ερωτηματολόγιο (Survey) με αποστολή δεδομένων στο ηλεκτρονικό ταχυδρομείο του δημιουργού.

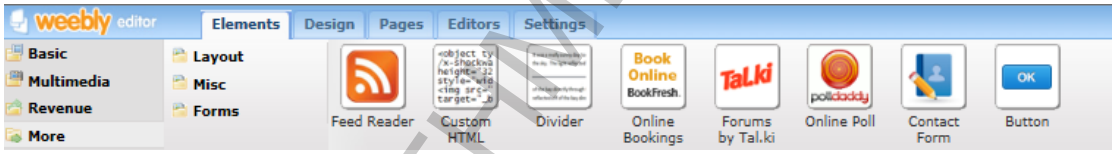
Εικόνα 5: 5ο ΒΗΜΑ: Προσθήκη κειμένων, εικόνων και στηλών στις σελίδες.



Εικόνα 6: 5ο ΒΗΜΑ: Προσθήκη Gallery φωτογραφιών, προβολή slides και βίντεο στις σελίδες.



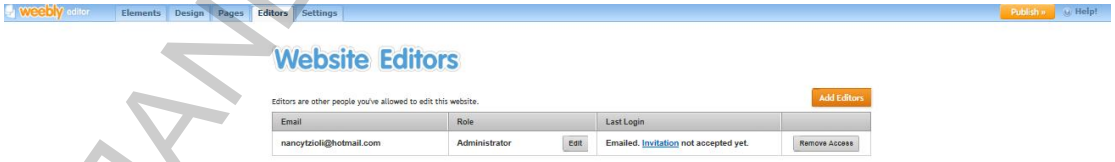
Εικόνα 7:5ο ΒΗΜΑ: Προσθήκη στατιστικών στοιχείων στις σελίδες.



Εικόνα 8: 5ο ΒΗΜΑ: Προσθήκη ψηφοφορίας και φόρμας επικοινωνίας στις σελίδες.

6ο ΒΗΜΑ: Διαχείριση ιστοσελίδας

Στην καρτέλα Editors ο δημιουργός μπορεί να ορίσει κι άλλα άτομα για τη διαχείριση της ιστοσελίδας.



Εικόνα 9: 6ο ΒΗΜΑ: Διαχείριση ιστοσελίδας

7ο ΒΗΜΑ: Δημοσίευση της ιστοσελίδας ώστε να γίνεται ορατή από όλους.

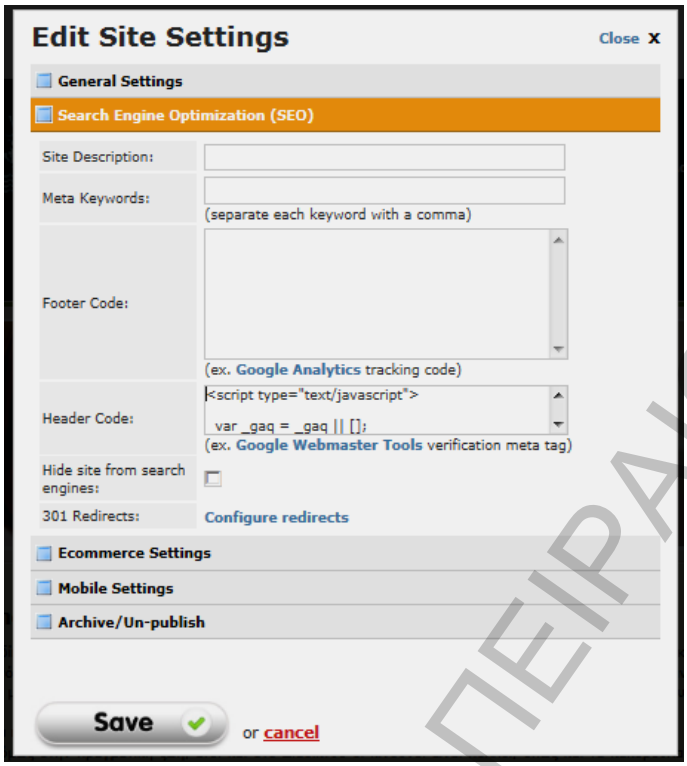
Ο δημιουργός-διαχειριστής δημοσιεύει την ιστοσελίδα κάνοντας κλικ στο πορτοκαλί πλήκτρο Publish (Δημοσίευση). Κάθε φορά που γίνεται κάποια αλλαγή

στην εμφάνιση και στο περιεχόμενο χρειάζεται η ανανέωση της δημοσίευσης. Η διεύθυνση της ιστοσελίδας μπορεί να αλλάξει οποιαδήποτε στιγμή. (Κανάς, 2010)

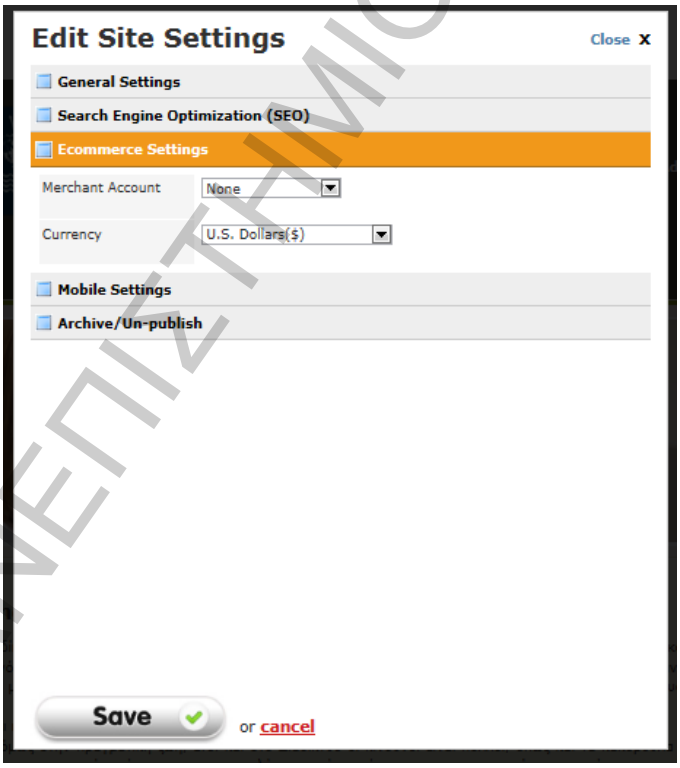
Εικόνα 10: 7ο ΒΗΜΑ: Δημοσίευση της ιστοσελίδας

Εικόνα 11: 7ο ΒΗΜΑ: Επίτευξη δημοσίευσης της ιστοσελίδας

Το πρώτο και το δεύτερο βήμα γίνεται από την καρτέλα Settings (ρυθμίσεις). Εκτός απ' αυτές υπάρχουν ρυθμίσεις που αφορούν την δημοσίευση –SEO- της ιστοσελίδας στις μηχανές αναζήτησης (Περιγραφή και προσθήκη κώδικα για καταγραφή στατιστικών).

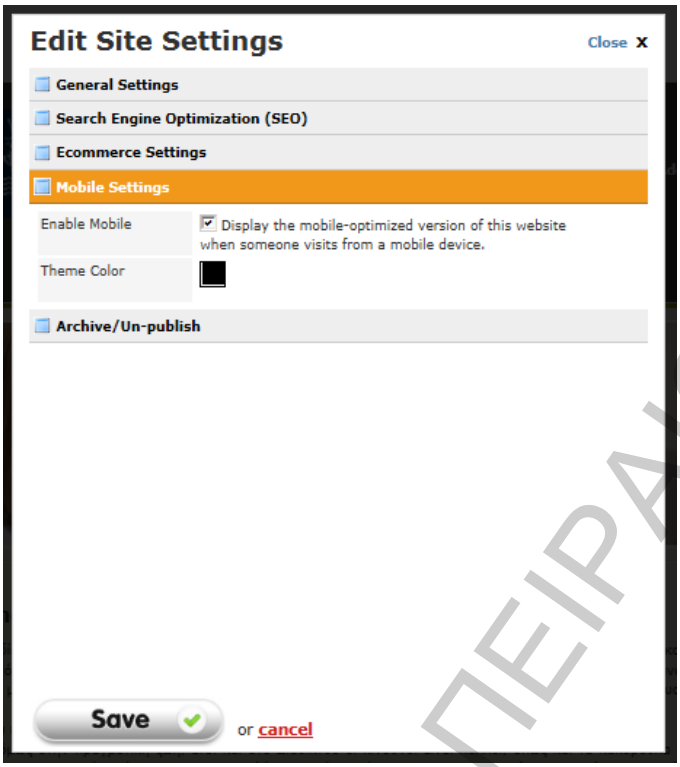


Εικόνα 12: Ρυθμίσεις SEO



Εικόνα 13: Ρυθμίσεις Ηλεκτρονικού Εμπορίου

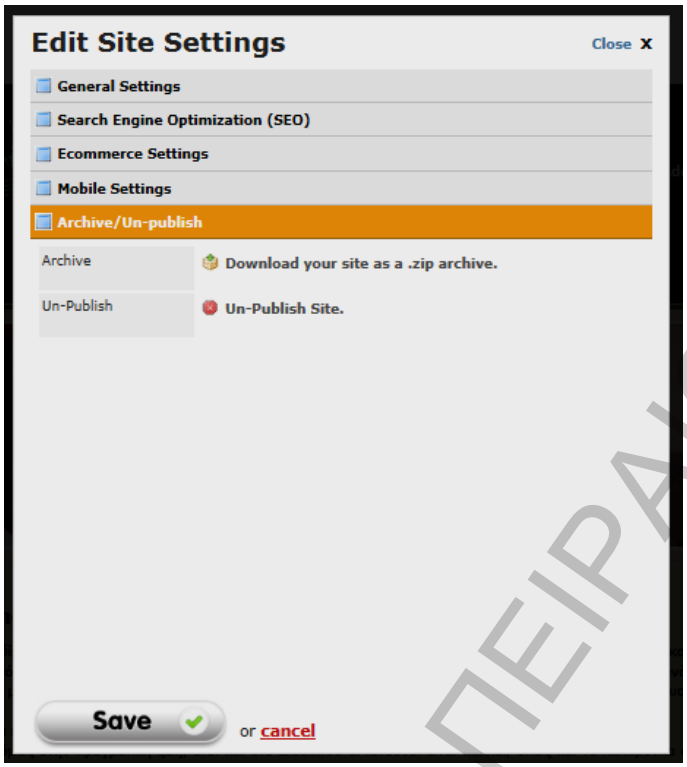
Επίσης, υπάρχουν και ρυθμίσεις για προβολή σε συσκευές κινητού τηλεφώνου (Mobile).



Εικόνα 14: Ρυθμίσεις για συσκευές κινητών

Σ' αυτήν την καρτέλα υπάρχει δυνατότητα αποθήκευσης όλου του διαδικτυακού χώρου στο σκληρό δίσκο για τη δημιουργία αντίγραφου ασφαλείας (backup).

Η τελευταία επιλογή της καρτέλας είναι η κατάργηση ή όχι της δημοσίευσης του συγκεκριμένου χώρου (Un-Publish Site).



Εικόνα 15: Δυνατότητα Un-publish

3.7.2 Περιγραφή περιεχομένου του BEsafe

3.7.2.1 Αρχική

Στον ιστότοπο BEsafe αναλύεται το ζήτημα «Ασφαλής Χρήση του Διαδικτύου» όπου και παρατίθεται αρχικά μια μικρή εισαγωγή. Στη συνέχεια, γίνεται αναφορά στο στόχο της δημιουργίας του συγκεκριμένου ιστοτόπου, όπως επίσης και στο στόχο του ιστοτόπου SafeSocialmedia, στον οποίο στηρίζεται και το σύνολο της έρευνας.

Εικόνα 16: "Αρχική Σελίδα" του ιστοτόπου BEsafe

3.7.2.2 Τα παιδιά

Στην ενότητα των παιδιών υπάρχουν πληροφορίες για οτιδήποτε σχετίζεται με το Διαδίκτυο και την ασφάλεια του. Επίσης, υπάρχουν χρήσιμες συμβουλές για τους κινδύνους στο Διαδίκτυο και πώς μπορεί το κάθε παιδί να προστατευτεί από αυτούς. Η συγκεκριμένη ενότητα χωρίζεται σε τρεις υπο-ενότητες:

1) Κίνδυνοι στο Διαδίκτυο
2) Προστασία στο Διαδίκτυο
3) Οδηγίες για ασφαλή χρήση του Διαδικτύου

Εικόνα 17: Σελίδα - Υποσελίδες "Παιδιά" του ιστοτόπου BEsafe

Εικόνα 18: Σελίδα "Παιδιά" του ιστοτόπου BEsafe

Στην κάθε μια ενότητα το παιδί έχει τη δυνατότητα να βρει ένα video και μια διαδραστική αφίσα έτσι ώστε να ενημερώνεται πλήρως. Στο τέλος υπάρχει και ένα quiz για το σωστό έλεγχο των γνώσεων που αποκόμισαν από τη συγκεκριμένη ενότητα.

Αναλυτικά το περιεχόμενο της κάθε ενότητας:

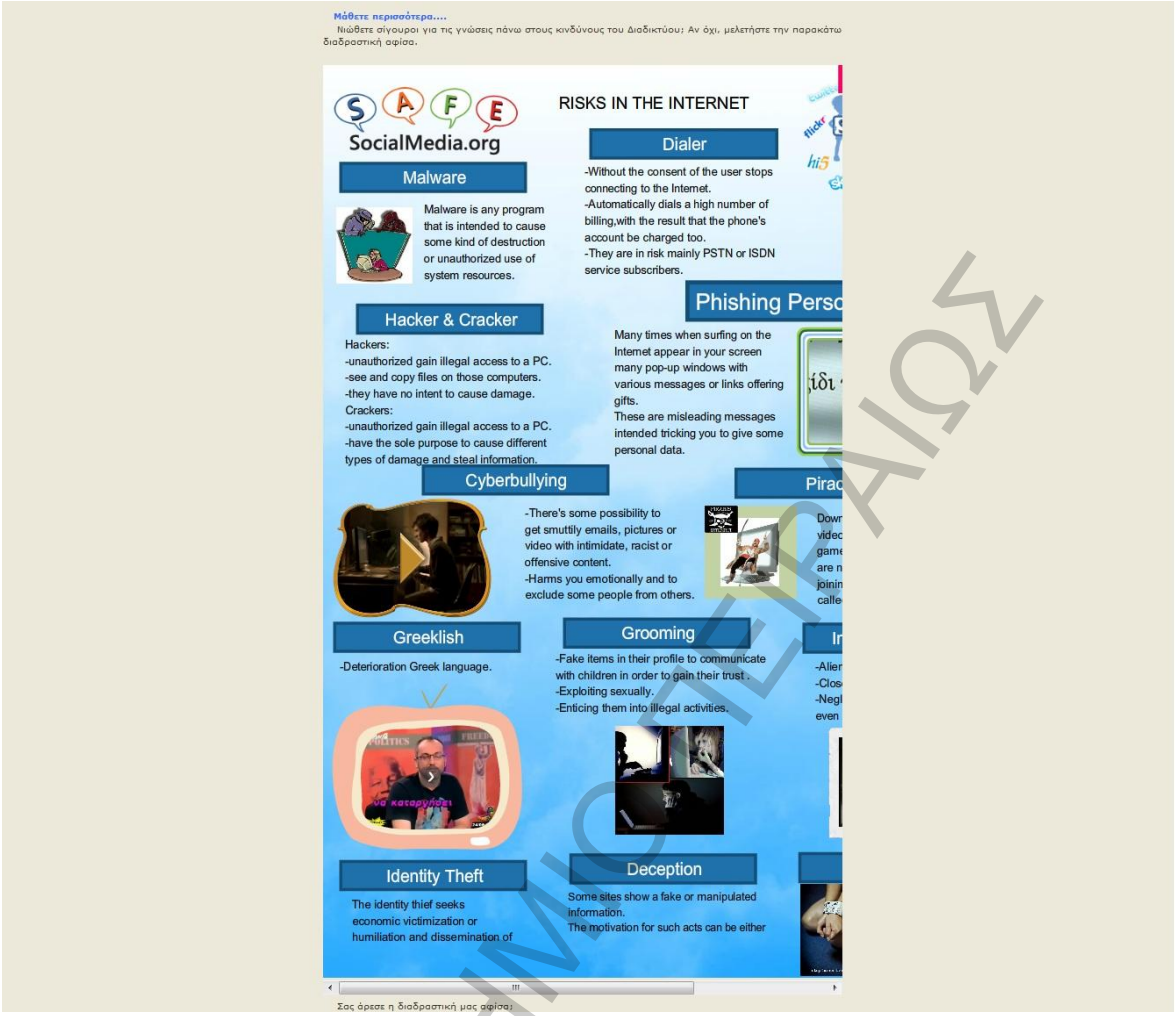
1) Κίνδυνοι στο Διαδίκτυο

Στο σημείο αυτό παρουσιάζονται οι βασικότεροι κίνδυνοι που παραμονεύουν στο Διαδίκτυο κατά τη διάρκεια της περιήγησης των παιδιών σε αυτό. Συγκεκριμένα, οι κίνδυνοι είναι οι παρακάτω:

1. Κακόβουλο Λογισμικό
2. Επιθέσεις Dialer
3. Επιθέσεις Χάκερ και Κράκερ
4. «Ψάρεμα» Προσωπικών Δεδομένων
5. Πειρατεία
6. Παραπλάνηση
7. Αποπλάνηση Ανηλίκων
8. Διαδικτυακός Εκφοβισμός
9. Κλοπή Ταυτότητας
10. Εθισμός στο Διαδίκτυο
11. Αλλοίωση της Γλώσσας (“Greeklish”)
12. Παράνομη Εμπορία Ανθρώπων

Αρχικά γίνεται μια μικρή περιγραφή των παραπάνω κινδύνων και στη συνέχεια παρουσιάζονται όλοι αυτοί οι κίνδυνοι συγκεντρωμένοι σε μια διαδραστική αφίσα έτσι ώστε τα παιδιά να τους κατανοήσουν πιο εύκολα και γρήγορα.

Εικόνα 19: Υποσελίδα "Κίνδυνοι στο Διαδίκτυο" του ιστοτόπου BEsafe

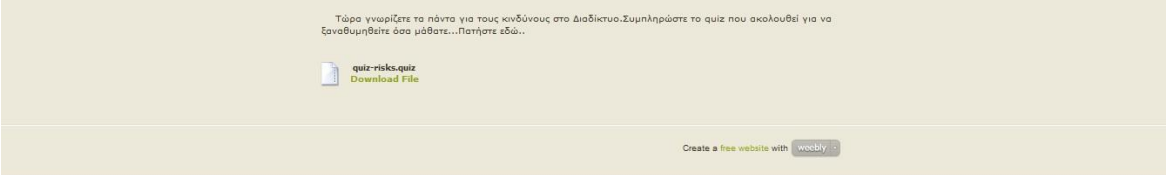


Εικόνα 20: Υποσελίδα "Κίνδυνοι στο Διαδίκτυο" του ιστοτόπου BEsafe - Glogster

Σε αυτό συμβάλλει βέβαια και το βίντεο που παρουσιάζεται στη συνέχεια της συγκεκριμένης ενότητας.

Εικόνα 21: Υποσελίδα "Κίνδυνοι στο Διαδίκτυο" του ιστοτόπου BEsafe – Video

Στο τέλος υπάρχει ένα quiz για τον έλεγχο των γνώσεων που αποκόμισαν από την ενότητα των «Κινδύνων στο Διαδίκτυο».



Εικόνα 22: Υποσελίδα "Κίνδυνοι στο Διαδίκτυο" του ιστοτόπου BEsafe - Quiz

2) Προστασία στο Διαδίκτυο

Στην ενότητα αυτή αναλύονται κάποιοι τρόποι προστασίας για την καλύτερη ασφάλεια των παιδιών στο Διαδίκτυο, τους οποίους πρέπει να ακολουθούν πιστά. Οι τρόποι αυτοί είναι οι ακόλουθοι:

- Προστασία από Κακόβουλο Λογισμικό
- Προστασία από Dialer
- Προστασία από Spam
- Προστασία από Κλοπή Ταυτότητας
- Προσωπική Προστασία

Εικόνα 23: Υποσελίδα "Προστασία στο Διαδίκτυο" του ιστοτόπου BEsafe

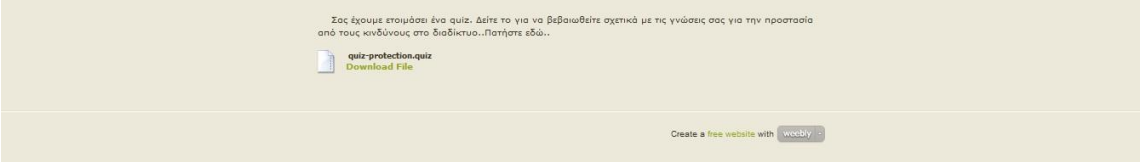
Αρχικά γίνεται μια μικρή περιγραφή των παραπάνω προτάσεων και στη συνέχεια παρουσιάζονται όλοι αυτοί οι τρόποι προστασίας συγκεντρωμένοι σε μια διαδραστική αφίσα έτσι ώστε τα παιδιά να κατανοήσουν πιο εύκολα και γρήγορα τους τρόπους προστασίας.

Εικόνα 24: Υποσελίδα "Προστασία στο Διαδίκτυο" του ιστοτόπου BEsafe - Glogster

Σε αυτό συμβάλλει βέβαια και το βίντεο που παρουσιάζεται στη συνέχεια της συγκεκριμένης ενότητας.

Εικόνα 25: Υποσελίδα "Προστασία στο Διαδίκτυο" του ιστοτόπου BEsafe - Video

Στο τέλος υπάρχει ένα quiz για τον έλεγχο των γνώσεων που αποκόμισαν από την ενότητα της «Προστασίας στο Διαδίκτυο».



Εικόνα 26: Υποσελίδα "Προστασία στο Διαδίκτυο" του ιστοτόπου BEsafe - Quiz

3) Οδηγίες για ασφαλή χρήση του Διαδικτύου

Στην τελευταία υπο-ενότητα παρουσιάζονται κάποιες οδηγίες για την ασφαλή χρήση του Διαδικτύου, οι οποίοι εμφανίζονται συγκεντρωμένοι και σε βίντεο.

Οι οδηγίες αυτές είναι οι παρακάτω:

- Χρησιμοποιούμε το Διαδίκτυο μόνο όταν ενήλικας είναι μαζί μας.
- Επισκεπτόμαστε μόνο ιστοσελίδες των οποίων το περιεχόμενο είναι ασφαλές και το οποίο γνωρίζουμε.
- Ψάχνουμε πληροφορίες στο Διαδίκτυο με τη βοήθεια ενός ενήλικα.
- Στέλνουμε και παραλαμβάνουμε email μαζί με κάποιον ενήλικα.
- Δε δίνουμε ποτέ προσωπικά στοιχεία (ονοματεπώνυμο, διεύθυνση, ηλικία, τηλέφωνο, φωτογραφίες κλπ.) σε υπηρεσίες όπως: δωμάτια συνομιλίας, διαδικτυακά παιχνίδια και ηλεκτρονικά μηνύματα.
- Δε συνομιλούμε ποτέ με άτομα που δε γνωρίζουμε και απορρίπτουμε μηνύματα ή αρχεία από αγνώστους.
- Προσέχουμε με ποια άτομα συνομιλούμε στο Διαδίκτυο. Σε περίπτωση που ο συνομιλητή μας μας κάνει να αισθανθούμε άβολα, διακόπτουμε απευθείας τη συνομιλία.
- Δεν επιδιώκουμε ποτέ συνάντηση με άγνωστα άτομα. Αν μας ζητήσει κάποιος άγνωστος να τον συναντήσουμε, αναφέρουμε το γεγονός σε ενήλικο άτομο της εμπιστοσύνης μας.

Στο τέλος υπάρχει ένα quiz για τον έλεγχο των γνώσεων που αποκόμισαν από την ενότητα των «Οδηγιών για ασφαλή χρήση του Διαδικτύου».

Εικόνα 27: Υποσελίδα "Οδηγίες για ασφαλή χρήση του Διαδικτύου" του ιστοτόπου BEsafe

3.7.2.3 Εκπαιδευτικοί

Στην ενότητα των «Εκπαιδευτικών» έχουν καταγραφεί κάποιες προτεινόμενες δραστηριότητες αξιοποίησης του εκπαιδευτικού υλικού, ούτως ώστε τα παιδιά χρησιμοποιώντας τις γνώσεις, δεξιότητες και στάσεις που αποκόμισαν από το υλικό να μπορούν να (συν)/δημιουργήσουν το δικό τους υλικό ανάλογα με το σενάριο χρήσης που θα τους δώσουν οι εκπαιδευτικοί.

Εικόνα 28: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe

Στη συνέχεια περιγράφονται αναλυτικά οι δραστηριότητες. Συγκεκριμένα γίνεται αναφορά στα βασικά χαρακτηριστικά τους και στο πώς μπορούν να συμβάλλουν στην παρότρυνση των μαθητών από την πλευρά του εκπαιδευτή.

3.7.2.3.1 Δραστηριότητες

Δραστηριότητα 1: Cmap (http://cmap.ihmc.us/)

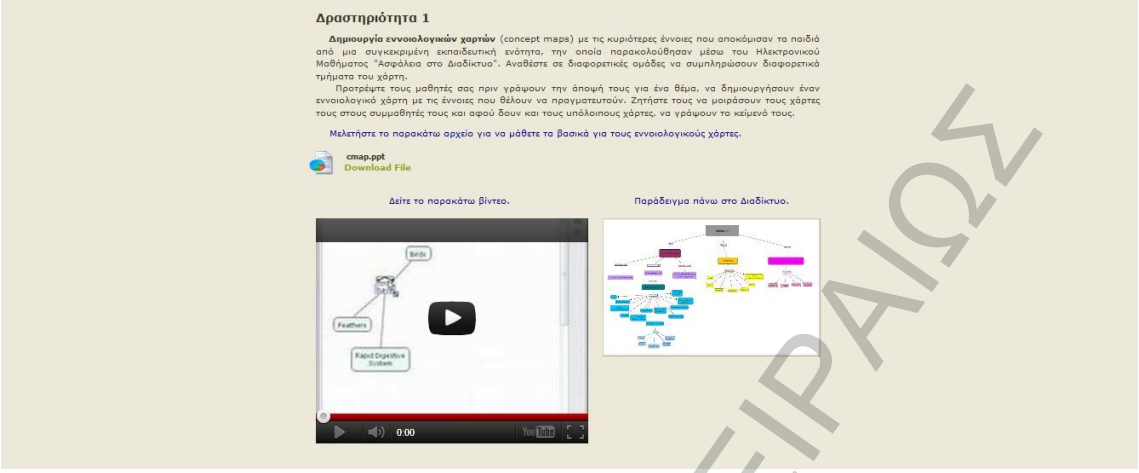
Ο εννοιολογικός χάρτης αναπτύχθηκε από τον J. Novak (Novak & Gowin 1984), ο οποίος βασίστηκε στη θεωρία της ουσιαστικής μάθησης (meaningful learning) του Ausubel (Ausubel et al. 1978) και αποτελεί μια από τις διδακτικές τεχνικές και στρατηγικές μάθησης που έχει ως σκοπό να ενισχύσει την εποικοδομητική και ουσιαστική μάθηση. Ένας εννοιολογικός χάρτης αποτελείται από *κόμβους* που αναπαριστούν τις έννοιες και *συνδέσμους* που προσδιορίζουν τις σχέσεις μεταξύ των εννοιών περιγράφοντας πώς μια έννοια συνδέεται με μια άλλη (Novak and Gowin 1984, McAleese 1998).

Σε ερευνητικές μελέτες, οι εννοιολογικοί χάρτες έχουν χρησιμοποιηθεί ως εργαλείο διερεύνησης της πρότερης γνώσης των μαθητών (Pearsall et al. 1997), ως εργαλείο διερεύνησης των αναπαραστάσεων των μαθητών σχετικά με το υπό εξέταση θέμα (Κόλλιας κ.ά. 2000), ως εργαλείο συνεργασίας (Basque and Lavoie 2006, Stoyanova and Kommers 2002, Komis et al. 2002, Kim et al. 2005), ως εργαλείο εννοιολογικής αλλαγής και αξιολόγησης (Mintzes et al. 2000, Liu 2004, Γρηγοριάδου κ.ά. 2003), ως εργαλείο επίλυσης προβλημάτων (Lee and Nelson 2005, Hsu 2004).

Στην εκπαιδευτική πράξη, ο εννοιολογικός χάρτης μπορεί να χρησιμοποιηθεί από το διδάσκοντα ως διδακτικό εργαλείο εμπλουτίζοντας τη διδακτική του προσέγγιση. Συγκεκριμένα, κατά τη διάρκεια της διδασκαλίας, ο εννοιολογικός χάρτης μπορεί να χρησιμοποιηθεί (i) για την παρουσίαση των εννοιών μιας ενότητας, (ii) ως οργανωτής προώθησης (advance organizer) συνεισφέροντας στην ενεργοποίηση της υπάρχουσας γνωστικής δομής των μαθητών και καθοδηγώντας την ενσωμάτωση εννοιών και γεγονότων καθώς και σχέσεων μεταξύ αυτών, εμπλουτίζοντας την υπάρχουσα γνωστική δομή των μαθητών, και (iii) ως επαναληπτικός χάρτης για τη σύνοψη των σημαντικότερων εννοιών της ενότητας.

Με τη βοήθεια του εννοιολογικού χάρτη οι εκπαιδευτικοί παροτρύνουν τους μαθητές να δημιουργήσουν τέτοιους χάρτες με τις κυριότερες έννοιες που αποκόμισαν τα παιδιά από μια συγκεκριμένη εκπαιδευτική ενότητα, την οποία

παρακολούθησαν μέσω του Ηλεκτρονικού Μαθήματος «Ασφάλεια στο Διαδίκτυο». Επίσης, μπορούν να τους αναθέσουν σε διαφορετικές ομάδες έτσι ώστε να συμπληρώσουν διαφορετικά τμήματα του χάρτη.



Εικόνα 29: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - Cmap

Δραστηριότητα 2: Glogster (www.glogster.com)

Το Glogster είναι ένας χώρος δημιουργικότητας όπου ο καθένας μπορεί, εύκολα, να κάνει μια ψηφιακή αφίσα (glog) μόνος του. Πρόκειται για μια διαδικτυακή ιστοσελίδα δημιουργίας διαδραστικής αφίσας με την εισαγωγή κειμένου, εικόνων, φωτογραφιών, ήχου (MP3), βίντεο, ειδικά εφέ και άλλα στοιχεία ώστε να δημιουργήσει κανείς online μία πολυμεσική (multimedia) αφίσα. Οι αφίσες μπορούν να μοιραστούν με άλλους χρήστες στην περιοχή, που είναι ενταγμένα στο πλαίσιο των εξωτερικών wikis και τα blogs, και σε ιστοσελίδες και από κοινού με πολλά κοινωνικά δίκτυα όπως το Facebook και το Twitter.

Το Glogster διαθέτει ένα πολύ απλό στη χρήση interface. Στα αρνητικά του είναι ότι δεν αναγνωρίζει ελληνικά καθώς και ότι η δωρεάν εκδοχή του είναι αρκετά λιτή μη περιλαμβάνοντας π.χ. δυνατότητα σχεδίασης. Αποτελεί έναν πολύ καλό τρόπο για να παρουσιάσουν οι μαθητές το τι έχουν αποκομίσει από τη μαθησιακή διαδικασία, ενώ μπορεί να χρησιμοποιηθεί σε διάφορα μαθήματα (στην ιστορία, τα μαθηματικά, τη γλώσσα, την πληροφορική, κ.α).

Με τη βοήθεια του Glogster υπάρχει η δυνατότητα δημιουργίας διαδραστικών σύμφωνα με ένα συγκεκριμένο θέμα (π.χ. Πώς συλλέγουν διάφορες ιστοσελίδες τα προσωπικά μας στοιχεία και ποιες επιλογές απορρήτου μπορούμε να ορίσουμε, για να αντιμετωπίσουμε τέτοια φαινόμενα;) είτε ατομικά είτε ομαδικά.

Εικόνα 30: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - Glogster

Δραστηριότητα 3: Prezi (www.prezi.com)

Το Prezi είναι ένα διαδικτυακό εργαλείο το οποίο δίνει τη δυνατότητα στο χρήστη να δημιουργήσει και να μοιραστεί μη γραμμικές παρουσιάσεις. Δίνει επίσης τη δυνατότητα δημιουργίας σχέσεων μεταξύ των περιεχόμενων της παρουσίασης αλλά και την δυνατότητα να κάνει zoom στις λεπτομέρειες.

Με το prezi δημιουργούνται θεαματικές, διαφορετικές από τις συνηθισμένες παρουσιάσεις στο MS Office Power Point και το Open Office Impress. Η παρουσίαση δεν αποτελείται από μια σειρά τυπικών σελίδων/διαφανειών αλλά από μια τεράστια επιφάνεια εργασίας πάνω στην οποία τοποθετείται το περιεχόμενο που θέλουμε να παρουσιάσουμε.

Βασικό εργαλείο μορφοποίησης του περιεχομένου του εργαλείου είναι το prezi zebra, που αποτελείται από τρεις κύκλους, τον ένα μέσα στον άλλον, με τους οποίους υπάρχει η δυνατότητα αλλαγής του μεγέθους του περιεχομένου/αντικειμένου, μετακίνησης και περιστροφής. Η σειρά με την οποία θα προβληθεί το περιεχόμενο αυτό θα εξαρτηθεί από τις επιλογές του χρήστη (σύνδεση των περιεχομένων με γραφικό τρόπο μεταξύ τους, ορίζοντας τη σειρά με την οποία θα προβληθούν).

Το Prezi παρουσιάζει κάποια θετικά σημεία, τα οποία αναφέρονται τη συνέχεια:

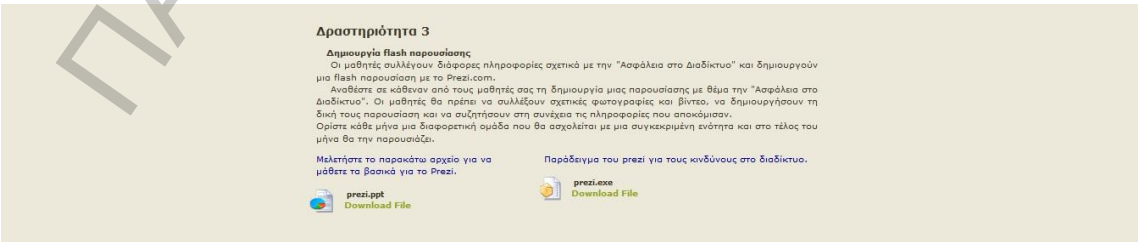
- Διαδικτυακό δωρεάν εργαλείο παρουσιάσεων που προσφέρει 100MBs αποθηκευτικού χώρου, κατόπιν εγγραφής.
- «Λήψη» (download) των παρουσιάσεων που δημιουργούμε. Με τον τρόπο αυτό μπορούμε να τις παρουσιάσουμε και εκτός δικτύου.
- Πρωτότυπο, εναλλακτικό, εργαλείο που δημιουργεί μη γραμμική/κλασική, σειριακή ροή παρουσίασης. Η παρουσίαση γίνεται περισσότερο διαδραστική επιτρέποντας την

πλοήγηση και την εστίαση (zoom) στο περιεχόμενο. (Η παρουσίαση μπορεί να έχει προκαθορισμένη από το δημιουργό της «αυτόματη» προβολή – για παρουσίαση π.χ. στην τάξη, ή να είναι διαδραστική, όπου ο χρήστης επιλέγει, χειροκίνητα, τα σημεία στα οποία θέλει να εστιάσει – χρησιμοποιώντας το ποντίκι του – π.χ. για προβολή σε χρόνο μεθύστερο από τον μαθητή.

- Ο δημιουργός της παρουσίασης μπορεί, αφού έχει εξοικειωθεί με το περιβάλλον, να προσθέτει εικόνες, βίντεο, σχήματα κ.α. διαλέγοντας με ποιον τρόπο και με ποια σειρά θα εμφανίζονται – μέσω της δημιουργίας ενός μονοπατιού που συνδέει το περιεχόμενο που έχουμε καταχωρήσει.
- Μη περιορισμός του χρήστη στην οριοθετημένη επιφάνεια μιας σελίδας, όπως στα κοινά προγράμματα, αλλά χρήση μιας, πρακτικά, ατέλειωτης επιφάνειας εργασίας, ενός μεγάλου καμβά πάνω στον οποίο ο δημιουργός της παρουσίασης εναποθέτει τα περιεχόμενα αυτής.
- Επιτρέπει τη συνεργασία μεταξύ χρηστών.
- Δυνατότητα δημιουργίας παρουσιάσεων prezi εκτός δικτύου – οι οποίες, όμως, δεν είναι στο δωρεάν πακέτο.
- Το περιεχόμενο που δημιουργούμε και αναρτούμε, άμεσα ή κατόπιν λήψης στη σελίδα του prezi, είναι συνέχεια διαθέσιμο – με την προϋπόθεση σύνδεσης στο διαδίκτυο.
- Εύκολο στην εκμάθηση και στη χρήση.

Στη συγκεκριμένη περίπτωση, το Prezi χρησιμοποιήθηκε για τη συλλογή διαφόρων πληροφοριών σχετικά με την «Ασφάλεια στο Διαδίκτυο» και για τη δημιουργία μιας flash παρουσίασης με το Prezi.com.

Ειδικότερα, προτείνεται η ανάθεση σε καθέναν από τους μαθητές η δημιουργία μιας παρουσίασης με θέμα την «Ασφάλεια στο Διαδίκτυο». Οι μαθητές θα πρέπει να συλλέξουν σχετικές φωτογραφίες και βίντεο, να δημιουργήσουν τη δική τους παρουσίαση και να συζητήσουν στη συνέχεια τις πληροφορίες που αποκόμισαν.



Εικόνα 31: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - Prezi

Δραστηριότητα4:ComicStripCreator (http://www.comicstripcreator.org/)

Τα κόμικς όπως και η γελοιογραφία ανήκουν στις γραφικές τέχνες. Τα πιο συνηθισμένα είδη είναι τα κόμικ στριπ (comic strip), που αφηγούνται μια ιστορία σε τρία ή τέσσερα καρέ και οι μεγαλύτερες ιστορίες σε περιοδικά ή βιβλία, γνωστές ως κόμικς ή βιβλία κόμικς. Πρόκειται για «ένα είδος φανταστικής ή και πραγματικής αφήγησης που γίνεται με εικόνες, λόγο ή και με ήχους και αποδίδεται με την παράθεση γραμμάτων» (Αντωνιάδης, 1995). Ο McCloud (1993) τα προσδιορίζει ως «γραφικά ή άλλες εικόνες σε αντιπαραβολή με μια προμελετημένη σειρά με σκοπό να μεταφέρουν πληροφορίες, και/ή να παράξουν μια αισθητική ανταπόκριση στον παρατηρητή». Ο Μαρτινίδης (1982) τα ονομάζει «εικονογραφήματα και ζωγραφιστή λογοτεχνία».

Η εισαγωγή τους στην εκπαιδευτική διαδικασία απετέλεσε αντικείμενο μελέτης σε πληθώρα από ερευνητικές εργασίες ήδη από τη δεκαετία του 1940 σε παγκόσμιο επίπεδο με ενθαρρυντικά αποτελέσματα.

Ειδικά μετά το 1992, όταν το βιβλίο κόμικς "Maus" με θέμα το Ολοκαύτωμα του Art Spiegelman κέρδισε βραβείο Pulitzer (Sturm, 2002), τα κόμικς άρχισαν σταθερά να βρίσκουν το δρόμο τους στον κόσμο της Εκπαίδευσης. Πληθώρα ερευνητικών προσπαθειών κυρίως στις ΗΠΑ, αλλά και στον ευρωπαϊκό χώρο, ήταν το έναυσμα για να αξιοποιήσουμε διδακτικά τα κόμικς και στην Ελλάδα, προχωρώντας ένα βήμα περαιτέρω, στη διδασκαλία με τη βοήθεια ψηφιακών κόμικς, έτσι ώστε να αξιοποιηθούν οι πολλαπλές εκπαιδευτικές δυνατότητές τους, αλλά και οι ΤΠΕ.

- **Εκπαιδευτικές Δυνατότητες**

Τα κόμικς μπορούν να αποτελέσουν ένα δυναμικό και πρωτότυπο εργαλείο μάθησης στα χέρια του εκπαιδευτικού με ποικίλες και αξιόλογες δυνατότητες, όπως:

- Κίνητρα: Παρακινούν τους μαθητές, ακόμη και τους απρόθυμους. Ο Alongi (1974) πιστοποιεί «τη μαγνητική έλξη που ασκούν στα παιδιά».
- Εποπτεία: Εικόνες και κείμενο επωμίζονται το φορτίο της ιστορίας από κοινού. Ο Versaci (2001) θεωρεί ότι μπορούν να βάλουν «ανθρώπινο πρόσωπο» σε ένα θέμα με συνέπεια μια οικεία, συναισθηματική σύνδεση μεταξύ μαθητών και χαρακτήρων μιας ιστορίας. Ο Sones (1944) διαπίστωσε ότι η οπτική τους ποιότητα προάγει την μάθηση.

- Μονιμότητα: Ο Williams (1995) αναφέρει το «μόνιμο, οπτικό συστατικό» των κόμικς ως έναν από τους λόγους χρήσης τους. Σε ταινίες ή σε μια παραδοσιακή διάλεξη η γλώσσα και οι πράξεις είναι «εφήμερες». Τα κείμενα από την άλλη έχουν το "οπτικό" και μόνιμο στοιχείο, αλλά όχι εικόνες. Η «οπτική μονιμότητα» επομένως είναι μοναδική στο κόμικς, όπου ο αναγνώστης ελέγχει το ρυθμό της εκπαίδευσης.
- Διαμεσολαβητικός ρόλος: Χρησιμεύουν ως ένα ενδιάμεσο βήμα προς δυσκολότερες και συνθετότερες έννοιες, ενώ η ίδια η πράξη δημιουργίας κόμικς είναι μια διεπιστημονική δραστηριότητα (Yang G., 2003).
- Δημοτικότητα: Τα παιδιά είναι εξοικειωμένα με τη λαϊκή κουλτούρα (popular culture). Ο Hutchinson (1949) πιστεύει ότι «πρέπει να υπάρξει αρμονία μεταξύ των δραστηριοτήτων ζωής του παιδιού και της εμπειρίας του στο σχολείο - η νέα μάθηση είναι πάντα συνέχεια ή επέκταση της μάθησης που ήδη κατέχει ο μαθητής». Εξάλλου τα κόμικς προάγουν την απόκτηση ικανοτήτων/γραμματισμού στα Μέσα Ενημέρωσης (media literacy).
- Καλλιέργεια κριτικής ικανότητας και αναλυτικής σκέψης: Σύμφωνα με το Versaci (2001) η απάντηση ερωτήσεων που αφορούν τη συνδυαστική χρήση εικόνας και κειμένου ωθεί τους μαθητές σε εξοικείωση με αυτά τα δύο μέσα έκφρασης, αποκαλύπτοντας βαθύτερα νοήματα και προσφέροντας τη δυνατότητα ενδοσκόπησης. (Βασιλικοπούλου, Αλτάνης, Μπολουδάκης, Γεωργιακάκης, Ρετάλης, 2009)

Όσον αφορά τα Κόμικς στη συγκεκριμένα έρευνα, δίνεται η δυνατότητα στους μαθητές να χρησιμοποιήσουν το ComicStrip Creator για να δημιουργήσουν ψηφιακά κόμικς ή ηλεκτρονικά βιβλία με τους διαλόγους που ετοίμασαν στο μάθημα και έτσι να οπτικοποιήσουν τα κείμενά τους. Μπορούν, επίσης, να σχεδιάσουν τις μικρές τους ιστορίες (κόμικς) στο χέρι και στη συνέχεια να τα ψηφιοποιήσουν και να τα αναρτήσουν στο blog του σχολείου ή στην ηλεκτρονική εφημερίδα της τάξης.

Εικόνα 32: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - ComicStripCreator

Δραστηριότητα 5: Storybird (http://storybird.com/)

Το Storybird αποτελεί ένα πολύ χρήσιμο εργαλείο για καθηγητές κάθε γλώσσας αλλά και γονείς. Μια δωρεάν ιστοσελίδα η οποία παρέχει εξαιρετική έτοιμη εικονογράφηση για τη δημιουργία διαφόρων ιστοριών από τους εκπαιδευτικούς και τους μαθητές. Το Storybird δίνει, επίσης, τη δυνατότητα δημιουργίας δωρεάν λογαριασμού για την κάθε τάξη και τον κάθε μαθητή ατομικά.

Η ιστοσελίδα είναι εξαιρετικά εύκολη στην χρήση ακόμα και για τους μαθητές. Δεν απαιτεί περίπλοκους χειρισμούς και έτσι οι μαθητές επικεντρώνουν μόνο στα ουσιαστικά θέματα. Δίνεται επίσης η δυνατότητα στους άλλους μαθητές να σχολιάσουν τη δουλειά των συμμαθητών τους.

Τέλος, το Storybird δίνει τη δυνατότητα αποστολής της δουλειάς των μαθητών στους γονείς μέσω email ή δημοσίευσης στην ιστοσελίδα ή το blog των εκπαιδευτικών.

Στη συγκεκριμένη ιστοσελίδα χρησιμοποιήθηκε για τη δημιουργία ενός e-book με μία ιστορία των μαθητών έχοντας ως έμπνευση κάποιες από τις εικόνες ή τα έργα τέχνης που φιλοξενούνται στο συγκεκριμένο διαδικτυακό χώρο.

Προτείνεται στους μαθητές να φτιάξουν εύκολα και γρήγορα μικρές ιστορίες, για να περιγράψουν διάφορα φαινόμενα ή ακόμα και δυσκολίες που μπορεί να αντιμετώπισαν.

Εικόνα 33: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - Storybird

Δραστηριότητα 6: Voki (www.voki.com)

Το Voki δημιουργήθηκε από ανθρώπους στο Oddcast, μια εταιρεία που έχει βάση τη Νέα Υόρκη, η οποία είχε δημιουργήσει χαρακτήρες να μιλάνε στο διαδίκτυο εδώ και πολλά χρόνια. Το Voki αποτελεί ένα Web 2.0 εργαλείο, το οποίο βασίζεται στην τεχνολογία Adobe Shockwave-Flash και είναι αποκλειστικά και μόνο για προσωπική, μη εμπορική χρήση.

Το Voki είναι ένα διαδικτυακό εργαλείο, με το οποίο μπορούμε να δημιουργήσουμε το ψηφιακό μας αντιπρόσωπο στο διαδίκτυο. Μπορούν δε να έχουν και το δικό τους ρόλο στην εκπαίδευση, τόσο σε μικτά (Blended Learning) όσο και σε καθαρά δικτυακά μαθήματα (Blended Online Learning). Το Voki είναι μια ψηφιακά δημιουργημένη εκδοχή του εαυτού μας. Ο πιο γενικός όρος για το Voki είναι ένας ομιλών αντιπρόσωπος, μια ψηφιακή αναπαράσταση ενός ανθρώπου στο διαδίκτυο. Οι εικονικοί αντιπρόσωποι μπορούν να έχουν το δικό τους ρόλο στην εκπαίδευση, σε μικτά καθώς και σε καθαρά δικτυακά μαθήματα. Για τους εκπαιδευτικούς, οι εικονικοί αντιπρόσωποι προσθέτουν ένα «ανθρώπινο» χαρακτηριστικό στο μάθημά τους (μέσα σε ένα blog, moodle…). Μπορεί να χρησιμοποιηθεί για την εισαγωγή στο θέμα του μαθήματος, ή για να βοηθήσει στις οδηγίες τους ακουστικούς/οπτικούς μαθητές. Τέλος, υπάρχει η δυνατότητα δημοσίευσης των Voki σε οποιοδήποτε blog, ιστοσελίδα ή διαδικτυακό προφίλ. Το Voki μας προσφέρει ένα διαφορετικό τρόπο επικοινωνίας.

Στην πληροφορική μπορεί να χρησιμοποιηθεί στην ενότητα των πολυμέσων καθώς και για την εξοικείωση των μαθητών με τα διαδικτυακά εργαλεία. Μπορεί, επίσης, να είναι και μια μικρή, διασκεδαστική και ευχάριστη δραστηριότητα (κυρίως λόγω της επιλογής και της διαμόρφωσης χαρακτήρα/ψηφιακού αντιπροσώπου που

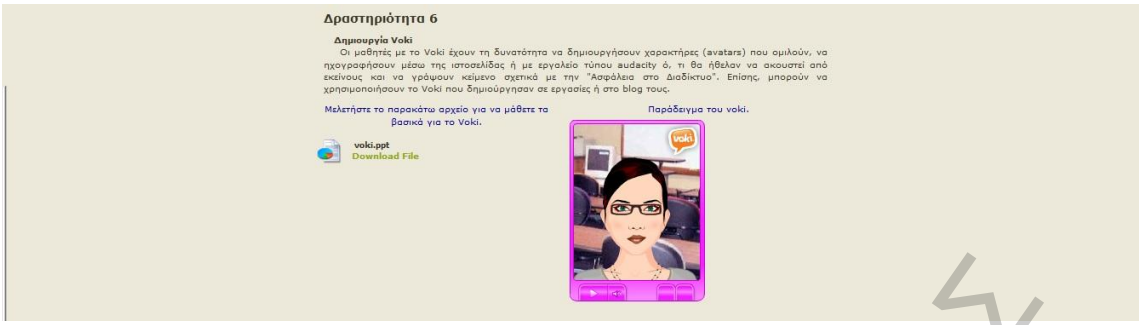
δεν περιορίζεται σε ανθρώπους) ενός διαθεματικού σχεδίου. Μια προφανής χρήση του είναι στα μαθήματα ξένων γλωσσών για την πρακτική ομιλίας των μαθητών – όπου θα καταγράψουν τη φωνή τους (δε θα χρησιμοποιήσουν την επιλογή «κείμενο σε ομιλία» (text to speech feature)). Μπορεί να χρησιμοποιηθεί ως «παγοθραύστης» (ice breaker) σε κοινά διαδικτυακά μαθήματα σχολείων, ζητώντας από τους μαθητές να δημιουργήσουν ένα voki που να τους ταιριάζει και στη συνέχεια, με τη βοήθεια αυτού, να περιγράψουν ή/και να παρουσιάσουν τον εαυτό τους (αντί του κλασικού τρόπου παρουσίασης σε μια ομάδα συζήτησης ή με τη χρήση κάποιων ice breakers).

Θα μπορούσε, ακόμα, να χρησιμοποιηθεί και για την καταγραφή των προφορικών απαντήσεών τους σε ερωτήσεις που τους έχουν τεθεί για το σπίτι.

- **Εφαρμογές στην Εκπαίδευση**

1. Οι μαθητές μπορούν να χρησιμοποιήσουν το Voki για να δημιουργήσουν μια παρουσίαση για την τάξη τους, να ηχογραφήσουν ένα μήνυμα και να δημιουργήσουν ένα avatar του εαυτού τους.
2. Οι μαθητές επικοινωνούν και συνεργάζονται με τους συμμαθητές τους ή/και με άλλους μαθητές σε άλλα σχολεία, με την ανταλλαγή των ηχογραφημένων μηνυμάτων.
3. Οι μαθητές ξενόγλωσσων μαθημάτων μπορούν να χρησιμοποιήσουν το Voki, για να «μιλήσουν» την ξένη γλώσσα σε δραστηριότητες παιξίματος ρόλων.
4. Ο καθένας μπορεί να τα χρησιμοποιήσει ως σύντομο «δελτίο ειδήσεων».
5. Μπορεί να χρησιμοποιηθεί ως εισαγωγή σε ηλεκτρονικά portfolia μαθητών.
6. Σα μια «αυθεντική» ξενόγλωσση εμπειρία, οι μαθητές γράφουν, διαβάζουν, διορθώνουν και μιλάνε σε κοινό.
7. Οι καθηγητές ξενόγλωσσων μαθημάτων μπορούν να ηχογραφήσουν την προφορά ή το λεξιλόγιο ως βοήθεια προς τους μαθητές τους.

Στη συγκεκριμένη περίπτωση, με το Voki δίνεται η δυνατότητα στους μαθητές να δημιουργήσουν χαρακτήρες (avatars) που ομιλούν, να ηχογραφήσουν μέσω της ιστοσελίδας ή με εργαλείο τύπου audacity ό, τι θα ήθελαν να ακουστεί από εκείνους και να γράψουν κείμενο σχετικά με την «Ασφάλεια στο Διαδίκτυο». Επίσης, μπορούν να χρησιμοποιήσουν το Voki που δημιούργησαν σε εργασίες ή στο blog τους.



Εικόνα 34: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe – Voki

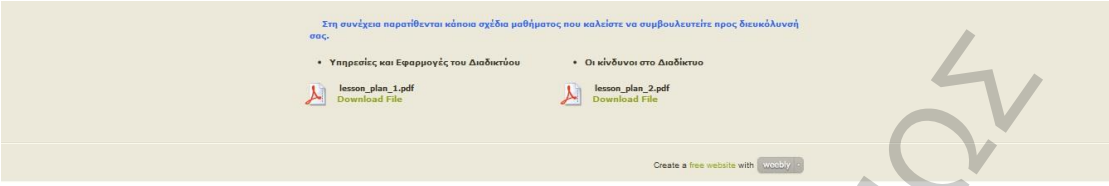
3.7.2.3.2 Σχέδια Μαθήματος

Στο τέλος της συγκεκριμένης ενότητας, δίνονται δυο παραδείγματα σχεδίων μαθήματος για δύο βασικές ενότητες της έρευνας, τις υπηρεσίες και τις εφαρμογές και για τους κινδύνους του διαδικτύου.

Το κάθε σχέδιο μαθήματος αποτελείται από τρία κυρίως μέρη: τους διδακτικούς στόχους, τη στρατηγική (δραστηριότητες) με την οποία θα επιδιωχθεί η επίτευξή τους και την αξιολόγηση (σενάρια για συζήτηση) με την οποία θα ελεγχθεί η επίτευξη των διδακτικών στόχων.

- Οι διδακτικοί στόχοι αναφέρονται ή πρέπει να αναφέρονται στον οδηγό διδασκαλίας. Διατυπώνονται με ρήματα και λέξεις οι οποίες καθιστούν σαφές το επιδιωκόμενο και κατά συνέπεια διευκολύνουν το σχεδιασμό και την ανάπτυξη του κριτηρίου αξιολόγησης.
- Η διδακτική στρατηγική είναι μια ακολουθία σταδίων των οποίων ο αριθμός μπορεί να αλλάζει και συνήθως είναι 3-7. Σε κάθε στάδιο επιτυγχάνεται ένας ενδιάμεσος στόχος και χρησιμοποιούνται διαφορετικοί χειρισμοί από τον εκπαιδευτή και διαφορετικά μαθησιακά έργα. Μαθησιακά έργα είναι πχ η απάντηση σε ερώτηση, η επίλυση προβλήματος, ο σχεδιασμός μιας πειραματικής διάταξης, η πραγματοποίηση ενός απλού πειράματος, η συζήτηση των μαθητών σε ομάδες, κλπ. Οι χειρισμοί μπορεί να είναι η διατύπωση μιας ερώτησης, η παροχή οδηγιών, η διαχείριση ενός διαλόγου μεταξύ μαθητών, η σύντομη ανάπτυξη ενός θέματος, η υποδειγματική σχεδίαση ενός μοντέλου, η εκτέλεση ενός πειράματος επίδειξης, κλπ.
- Η αξιολόγηση έχει ως αφετηρία τους διδακτικούς στόχους και ελέγχει το κατά πόσο αυτοί επιτεύχθηκαν. Είναι ένα τεστ σύντομης διάρκειας στο οποίο οι διαφόρων τύπων ερωτήσεις, οι ασκήσεις, κλπ ελέγχουν το κατά πόσο επιτεύχθηκαν οι στόχοι. Ανάλογα με το αποτέλεσμα ο εκπαιδευτής:

α)προχωράει στο σχεδιασμό της επόμενης διδασκαλίας, β) επανέρχεται στο ίδιο μάθημα για επιτευχθούν οι στόχοι που δεν επιτεύχθηκαν χρησιμοποιώντας διαφορετικά μαθησιακά έργα, γ) αναθεωρεί τη διδακτική στρατηγική που είχε ακολουθήσει εξαρχής.



Εικόνα 35: Σελίδα "Εκπαιδευτικοί" του ιστοτόπου BEsafe - Σχέδια Μαθήματος

3.7.2.4 Γονείς

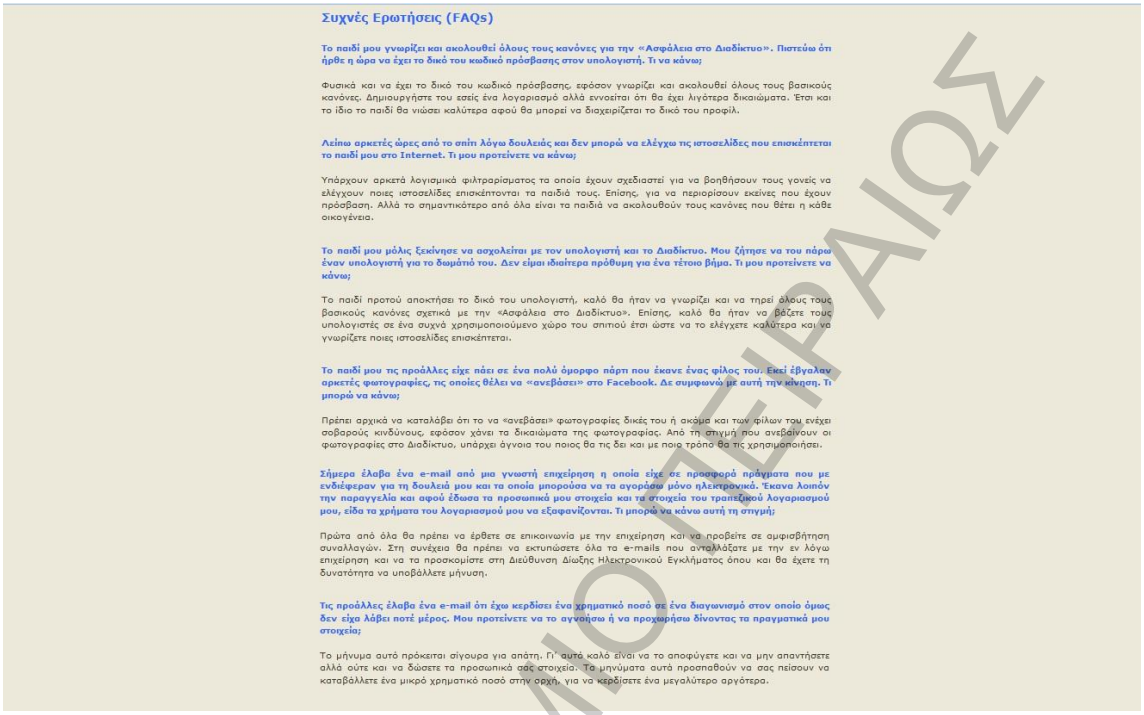
Στην ιστοσελίδα του BEsafe υπάρχει ακόμα μια ενδιαφέρουσα ενότητα η οποία απευθύνεται στους γονείς και η οποία έχει ως στόχο την πληροφόρηση των γονέων πάνω σε θέματα ασφάλειας του Διαδικτύου. Σε αυτό το σημείο παρουσιάζονται συμβουλές τις οποίες πρέπει να γνωρίζουν οι γονείς:

1) Να επιβλέπετε τα παιδιά σας κατά τη χρήση του διαδικτύου και να συνοδεύετε κυρίως τα μικρότερα παιδιά όταν συνδέονται στο Internet, ειδικά την πρώτη φορά.
2) Να δημιουργήσετε τη δική τους λίστα με τις προτεινόμενες παιδικές σελίδες και να συμπεριλάβετε μηχανές αναζήτησης φιλικές στη χρήση τους για παιδιά.
3) Να επιβλέπετε και να φιλτράρετε το περιεχόμενο του διαδικτύου ώστε να ελέγχετε ότι τα παιδιά σας δεν έχουν πρόσβαση σε περιεχόμενο που είναι επιβλαβές
4) Να δημιουργήσετε μια συμφωνία σε οικογενειακό επίπεδο για τη χρήση του Internet.
5) Να τους διδάξετε να μη δίνουν ποτέ τα προσωπικά τους στοιχεία και τις προσωπικές τους πληροφορίες.
6) Να ελέγχετε τα Αγαπημένα (bookmarks) και το Ιστορικό (History) του προγράμματος φυλλομετρητή ιστοσελίδων (browser) για να βλέπετε ποιες σελίδες έχουν επισκεφτεί τα παιδιά σας.
7) Να βάζετε τους υπολογιστές με σύνδεση στο Internet σε ένα συχνά χρησιμοποιούμενο χώρο του σπιτιού.

8) Για την καλύτερη προστασία των παιδιών σας μπορείτε να εγκαταστήσετε ειδικά προγράμματα τα οποία ελέγχουν την πρόσβαση στο διαδίκτυο, σύμφωνα με τις ρυθμίσεις τις οποίες μπορείτε να κάνετε εσείς.

Εικόνα 36: Σελίδα "Γονείς" του ιστοτόπου BEsafe

Στο συγκεκριμένο μέρος της ενότητας υπάρχουν οι σημαντικότερες συχνές ερωτήσεις (FAQs – Frequently Asked Questions) με τις αντίστοιχες απαντήσεις τους που μπορεί να δημιουργηθούν από τους γονείς.



Συχνές Ερωτήσεις (FAQs)

Το παιδί μου γνωρίζει και ακολουθεί όλους τους κανόνες για την «Ασφάλεια στο Διαδίκτυο». Πιστεύω ότι ήρθε η ώρα να έχει το δικό του κωδικό πρόσβασης στον υπολογιστή. Τι να κάνω;

Φυσικά και να έχει το δικό του κωδικό πρόσβασης, εφόσον γνωρίζει και ακολουθεί όλους τους βασικούς κανόνες. Δημιουργήστε του εσείς ένα λογαριασμό αλλά εννοείται ότι θα έχει λιγότερα δικαιώματα. Έτσι και το ίδιο το παιδί θα νιώσει καλύτερα αφού θα μπορεί να διαχειρίζεται το δικό του προφίλ.

Λείπω αρκετές ώρες από το σπίτι λόγω δουλειάς και δεν μπορώ να ελέγχω τις ιστοσελίδες που επισκέπτεται το παιδί μου στο Internet. Τι μου προτείνετε να κάνω;

Υπάρχουν αρκετά λογισμικά φιλτραρίσματος τα οποία έχουν σχεδιαστεί για να βοηθήσουν τους γονείς να ελέγχουν ποιες ιστοσελίδες επισκέπτονται τα παιδιά τους. Επίσης, για να περιορίσουν εκείνες που έχουν πρόσβαση. Αλλά το σημαντικότερο από όλα είναι τα παιδιά να ακολουθούν τους κανόνες που θέτει η κάθε οικογένεια.

Το παιδί μου μόλις ξεκίνησε να ασχολείται με τον υπολογιστή και το Διαδίκτυο. Μου ζήτησε να του πάρω έναν υπολογιστή για το δωμάτιό του. Δεν είμαι ιδιαίτερα πρόθυμη για ένα τέτοιο βήμα. Τι μου προτείνετε να κάνω;

Το παιδί προτού αποκτήσει το δικό του υπολογιστή, καλό θα ήταν να γνωρίζει και να τηρεί όλους τους βασικούς κανόνες σχετικά με την «Ασφάλεια στο Διαδίκτυο». Επίσης, καλό θα ήταν να βάζετε τους υπολογιστές σε ένα συχνά χρησιμοποιούμενο χώρο του σπιτιού έτσι ώστε να το ελέγχετε καλύτερα και να γνωρίζετε ποιες ιστοσελίδες επισκέπτεται.

Το παιδί μου τις προάλλες είχε πάει σε ένα πολύ όμορφο πάρτι που έκανε ένας φίλος του. Εκεί έβγαλαν αρκετές φωτογραφίες, τις οποίες θέλει να «ανεβάσει» στο Facebook. Δε συμφωνώ με αυτή την κίνηση. Τι μπορώ να κάνω;

Πρέπει αρχικά να καταλάβει ότι το να «ανεβάσει» φωτογραφίες δικές του ή ακόμα και των φίλων του ενέχει σοβαρούς κινδύνους, εφόσον χάνει τα δικαιώματα της φωτογραφίας. Από τη στιγμή που ανεβαίνουν οι φωτογραφίες στο Διαδίκτυο, υπάρχει άγνοια του ποιος θα τις δει και με ποιο τρόπο θα τις χρησιμοποιήσει.

Σήμερα έλαβα ένα e-mail από μια γνωστή επιχείρηση η οποία είχε σε προσφορά πράγματα που με ενδιέφεραν για τη δουλειά μου και τα οποία μπορούσα να τα αγοράσω μόνο ηλεκτρονικά. Έκανα λοιπόν την παραγγελία και αφού έδωσα τα προσωπικά μου στοιχεία και τα στοιχεία του τραπεζικού λογαριασμού μου, είδα τα χρήματα του λογαριασμού μου να εξαφανίζονται. Τι μπορώ να κάνω αυτή τη στιγμή;

Πρώτα από όλα θα πρέπει να έρθετε σε επικοινωνία με την επιχείρηση και να προβείτε σε αμφισβήτηση συναλλαγών. Στη συνέχεια θα πρέπει να εκτυπώσετε όλα τα e-mails που ανταλλάξατε με την εν λόγω επιχείρηση και να τα προσκομίσετε στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος όπου και θα έχετε τη δυνατότητα να υποβάλλετε μήνυση.

Τις προάλλες έλαβα ένα e-mail ότι έχω κερδίσει ένα χρηματικό ποσό σε ένα διαγωνισμό στον οποίο όμως δεν είχα λάβει ποτέ μέρος. Μου προτείνετε να το αγνοήσω ή να προχωρήσω δίνοντας τα πραγματικά μου στοιχεία;

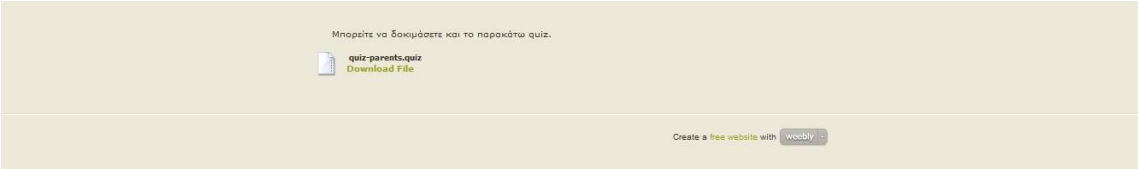
Το μήνυμα αυτό πρόκειται σίγουρα για απάτη. Γι' αυτό καλό είναι να το αποφύγετε και να μην απαντήσετε αλλά ούτε και να δώσετε τα προσωπικά σας στοιχεία. Τα μηνύματα αυτά προσπαθούν να σας πείσουν να καταβάλλετε ένα μικρό χρηματικό ποσό στην αρχή, για να κερδίσετε ένα μεγαλύτερο αργότερα.

Εικόνα 37: Σελίδα "Γονείς" του ιστοτόπου BEsafe - FAQ's

Επίσης, στη συγκεκριμένη ενότητα παρουσιάζονται συγκεντρωμένοι οι σημαντικότεροι κανόνες προς τους γονείς μέσα από ένα βίντεο.

Εικόνα 38: Σελίδα "Γονείς" του ιστοτόπου BEsafe – Video

Στο τέλος υπάρχει ένα quiz για τον έλεγχο των γνώσεων που αποκόμισαν οι εκπαιδευτικοί από τη συγκεκριμένη ενότητα.



Εικόνα 39: Σελίδα "Γονείς" του ιστοτόπου BEsafe - Quiz

3.7.2.5 Επιπρόσθετο Υλικό

Επίσης, υπάρχει και μια ενδιαφέρουσα ενότητα στην ιστοσελίδα, η οποία καλείται «Επιπρόσθετο Υλικό» και στην οποία είναι συγκεντρωμένα άρθρα και βιβλία για επιπλέον ενημέρωση του κοινού πάνω στο θέμα της «Ασφαλούς χρήσης του Διαδικτύου».

Εικόνα 40: Σελίδα "Επιπρόσθετο Υλικό" του ιστοτόπου BEsafe

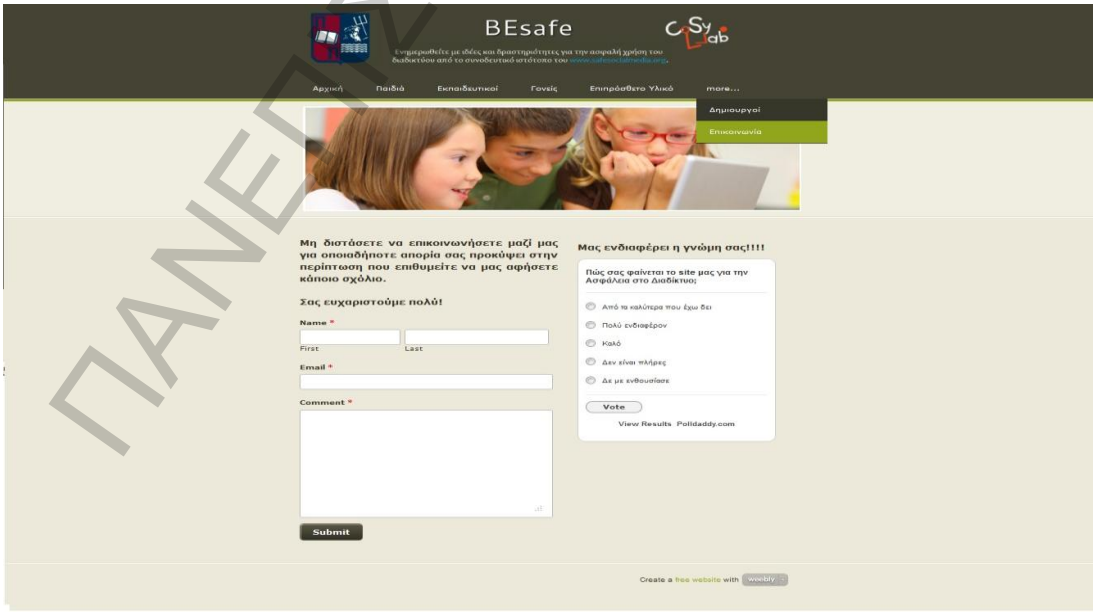
3.7.2.6 Δημιουργοί

Στη συνέχεια του ιστοτόπου, γίνεται σύντομη αναφορά των δημιουργών της ιστοσελίδας στην αντίστοιχη ενότητα «Δημιουργοί».

Εικόνα 41: Σελίδα "Δημιουργοί" του ιστοτόπου BEsafe

3.7.2.7 Επικοινωνία

Τέλος, ο ιστότοπος ολοκληρώνεται με την ενότητα της «Επικοινωνίας», όπου το κοινό που την επισκέπτεται έχει τη δυνατότητα να θέσει οποιαδήποτε απορία ή παρατήρηση έχει. Επίσης, στη συγκεκριμένη ενότητα υπάρχει και μια μικρή ψηφοφορία σχετικά με το πώς φαίνεται ο ιστότοπος και το θέμα που πραγματεύεται.



Εικόνα 42: Σελίδα "Επικοινωνία" του ιστοτόπου BEsafe

3.7.2.8 Διαμορφώνοντας τον ιστότοπο BEsafe στο Weebly

Ο σχεδιασμός της ιστοσελίδας καθορίζει την εμφάνιση των σελίδων και τη διάταξη των διαφόρων στοιχείων σε αυτές. Παρακάτω παρατίθεται ένας συγκεντρωτικός πίνακας, στον οποίο γίνεται αναλυτική περιγραφή όλης της ιστοσελίδας BEsafe.

Πίνακας 3: Αναλυτική Περιγραφή των σελίδων του BEsafe

ΣΕΛΙΔΕΣ	ΠΕΡΙΓΡΑΦΗ
Αρχική	Αναλύεται ο κύριος στόχος της δημιουργίας της ιστοσελίδας BEsafe. Αναφορά στο βασικό ιστότοπο στον οποίο στηρίζεται όλη η έρευνα, δηλαδή στο Safesocialmedia.
Παιδιά	Στο συγκεκριμένο σημείο τα παιδιά έχουν τη δυνατότητα να βρουν πληροφορίες για οτιδήποτε τους απασχολεί σχετικά με το Διαδίκτυο και την ασφάλεια του. Επίσης, μπορούν να μελετήσουν χρήσιμες συμβουλές για τους κινδύνους στο Διαδίκτυο και πώς μπορούν να προστατευτούν από αυτούς. • Κίνδυνοι στο Διαδίκτυο Εδώ τα παιδιά έχουν τη δυνατότητα να γνωρίσουν τους κινδύνους τους Διαδικτύου καθώς και να τους μελετήσουν διεξοδικά τον κάθε έναν ξεχωριστά. • Προστασία στο Διαδίκτυο Στο Διαδίκτυο παραμονεύουν πάρα πολλοί κίνδυνοι, τους οποίους τα παιδιά γνώρισαν στην προηγούμενη σελίδα. Εδώ τους δίνεται η δυνατότητα να γνωρίσουν αναλυτικά τους τρόπους με τους οποίους μπορούν να προστατευτούν από αυτούς τους κινδύνους. • Οδηγίες για ασφαλή χρήση του Διαδικτύου Στο συγκεκριμένο μέρος παρουσιάζονται στα παιδιά οι οδηγίες που πρέπει να ακολουθούν για την ασφαλή χρήση του Διαδικτύου.
Εκπαιδευτικοί	Στην παρούσα ενότητα έχουν καταγραφεί κάποιες προτεινόμενες δραστηριότητες αξιοποίησης του εκπαιδευτικού υλικού, ούτως ώστε τα παιδιά χρησιμοποιώντας τις γνώσεις, δεξιότητες και στάσεις που αποκόμισαν από το υλικό να μπορούν να (συν)/δημιουργήσουν το δικό τους υλικό ανάλογα με το σενάριο

	χρήσης που θα τους δώσουν οι εκπαιδευτικοί.
Γονείς	Στην ενότητα αυτή φιλοξενείται το κατάλληλο υλικό που έχει ως στόχο την πληροφόρηση των γονέων και άλλων ενδιαφερομένων πάνω σε θέματα ασφάλειας του Διαδικτύου.
Επιπρόσθετο Υλικό	Η σελίδα αυτή περιέχει συνδέσεις σε ιστοσελίδες, από τις οποίες δίνεται η δυνατότητα στους επισκέπτες- χρήστες να βρουν επιπλέον πληροφορίες.
Δημιουργοί	Η συγκεκριμένη σελίδα περιλαμβάνει πληροφορίες για τους δημιουργούς της ιστοσελίδας "BEsafe". Επίσης, γίνεται αναφορά σχετικά με το πλαίσιο στο οποίο έχει κατασκευαστεί.
Επικοινωνία	• Επικοινωνία Δίνεται η δυνατότητα στους επισκέπτες - χρήστες της ιστοσελίδας να αφήσουν σχόλια και να θέσουν ερωτήσεις σχετικά με το περιεχόμενο της συγκεκριμένης ιστοσελίδας. • Ψηφοφορία Δίνεται η δυνατότητα στους επισκέπτες - χρήστες της ιστοσελίδας να πάρουν μέρος στην ψηφοφορία έτσι ώστε να βελτιωθεί το περιεχόμενο της.

ΚΕΦΑΛΑΙΟ 4. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

4.1 Εισαγωγή

Μετά τη συγκέντρωση των ερωτηματολογίων το επόμενο βήμα ήταν η επεξεργασία των στοιχείων. Για την ανάλυση αυτή χρησιμοποιήθηκε το στατιστικό πρόγραμμα ανάλυσης δεδομένων SPSS (Statistical Package for Social Sciences) έκδ. 20, ένα από τα πιο δημοφιλή, ευέλικτα και εύχρηστα στατιστικά πακέτα για την ανάλυση και πραγματοποίηση ποσοτικών ερευνών.

Το στατιστικό αυτό πακέτο προσφέρει πολλές δυνατότητες στους ερευνητές μόνο όμως για τις ποσοτικές ερωτήσεις (κλειστού τύπου). Αντίθετα για τις ποιοτικές (ανοιχτού τύπου ερωτήσεις) ακολουθήθηκε η χειρόγραφη καταγραφή των δεδομένων.

4.2 Αποτελέσματα

Ο ερευνητής πρέπει να γνωρίζει τη σημασία που έχει για μια έγκυρη έρευνα: η εκτενής βιβλιογραφική ανασκόπηση, ένα αντιπροσωπευτικό δείγμα, ένα σωστά σχεδιασμένο και συμπληρωμένο ερωτηματολόγιο και τέλος η ερμηνεία των αποτελεσμάτων και η εξαγωγή γενικεύσιμων συμπερασμάτων.

4.2.1 Έλεγχος Αξιοπιστίας

Για να διασφαλιστεί η αξιοπιστία των δεδομένων πραγματοποιήθηκε έλεγχος αξιοπιστίας χρησιμοποιώντας το συντελεστή αξιοπιστίας Cronbach α. Η τιμή του συντελεστή Cronbach α, όπως φαίνεται στον πίνακα είναι 0,819. Το "alpha" είναι πολύ υψηλό και συμπεραίνεται ότι η αξιοπιστία της κλίμακας είναι πολύ υψηλή. Γενικά, κλίμακες των οποίων το Cronbach α ξεπερνά ή πλησιάζει το 0,70 θεωρούνται αξιόπιστες (Σιώμκος, Βασιλακοπούλου, 2005).

Πίνακας 4: Έλεγχος Αξιοπιστίας Ερωτηματολογίου – Cronbach α

Reliability Statistics

Cronbach's Alpha	N of Items
,819	9

4.2.2 Περιγραφική Ανάλυση Δεδομένων

Συγκεκριμένα, οι ερωτήσεις (μεταβλητές) 1-9 πραγματεύονται την παρουσίαση των δύο ιστοτόπων και των δραστηριοτήτων που δημιουργήθηκαν και μετρώνται με κλίμακα Likert (1=Διαφωνώ απόλυτα σε 5=Συμφωνώ απόλυτα) όπου οι ερωτηθέντες δήλωσαν το βαθμό συμφωνίας ή διαφωνίας τους. Στην ερώτηση 10 παρουσιάζονται οι παρατηρήσεις και τα σχόλια των ερωτηθέντων σχετικά με το «BEsafe» και το «Safesocialmedia», στην οποία οι ερωτηθέντες μπορούν να εκφράσουν τη γνώμη τους ελεύθερα και χωρίς περιορισμούς.

Προτού, όμως, ξεκινήσει η έρευνα του πεδίου (συμπλήρωση των ερωτηματολογίων), το συγκεκριμένο ερωτηματολόγιο ελέγχθηκε για τη λειτουργικότητά του με πιλοτικό τεστ από πέντε φίλους - εκπαιδευτικούς, με τη βοήθεια του οποίου εξακριβώθηκε εάν:

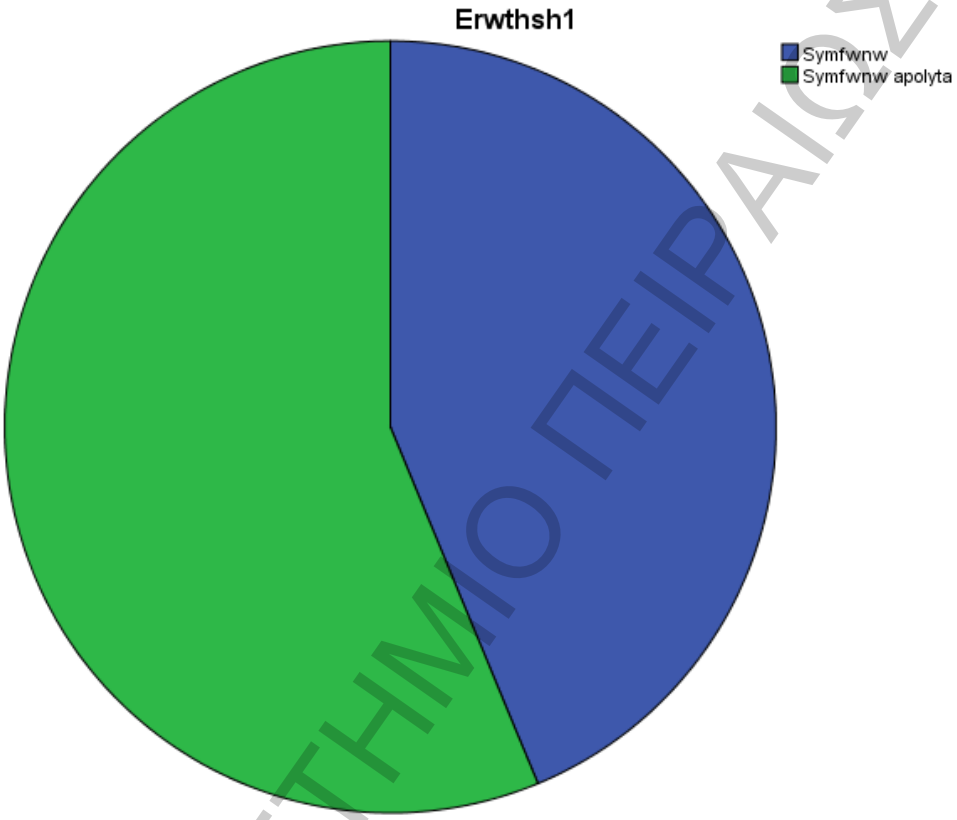
- Οι χρησιμοποιούμενοι όροι γίνονται εύκολα αντιληπτοί.
- Η σειρά των ερωτήσεων δεν προκαλεί τάσεις πιθανής διαστρέβλωσης.
- Ο τρόπος της διατύπωσης των ερωτήσεων επιτρέπει τη συλλογή των επιθυμητών στοιχείων.

Επίσης για τη διευκόλυνση των ερωτηθέντων στην κατανόηση του σκοπού της έρευνας καθώς και την εξασφάλιση της προστασίας των προσωπικών δεδομένων των ερωτηθέντων, υπήρξε εισαγωγικό σημείωμα στο οποίο διατυπώθηκε ο στόχος και το αντικείμενο της έρευνας καθώς και η βεβαίωση ότι τα προσωπικά δεδομένα είναι εμπιστευτικά και θα χρησιμοποιηθούν αποκλειστικά και μόνο για τη στατιστική ανάλυση και την εξαγωγή συμπερασμάτων για την παρούσα έρευνα.

Από τη στιγμή που το ερωτηματολόγιο έχει σχεδιασθεί σωστά, το δείγμα είναι αντιπροσωπευτικό, οι ορισμοί έχουν γίνει κατανοητοί από τους ερωτώμενους και το ερωτηματολόγιο έχει συμπληρωθεί σωστά, τότε τα αποτελέσματα της έρευνας θεωρούνται έγκυρα και αντιπροσωπευτικά της ομάδας που το μελέτησε.

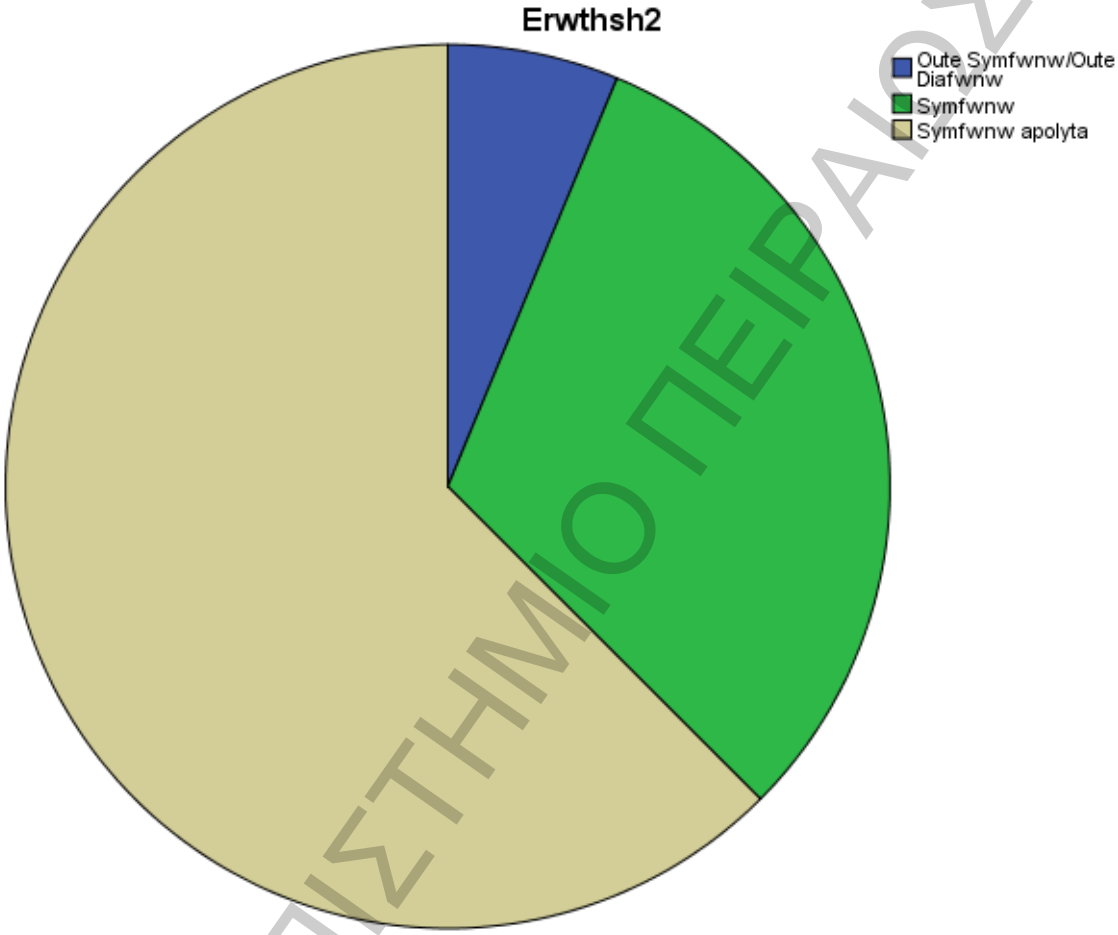
Με βάση τα αποτελέσματα αυτά μπορεί τότε ο ερευνητής να προχωρήσει στην ερμηνεία του κοινωνικού φαινομένου καθώς και στην εξαγωγή γενικεύσιμων συμπερασμάτων. Επίσης, πρέπει πάντοτε να γνωρίζει ότι μια έρευνα δεν επαρκεί για μια ολοκληρωμένη διερεύνηση ενός κοινωνικού φαινομένου αλλά απλά ρίχνει φως σε ορισμένες πτυχές του (Κυριαζή, 2002). Για αυτό το λόγο είναι σημαντική η βιβλιογραφική επισκόπηση, ώστε να γνωρίζει τι έχει ήδη μελετηθεί και τι φαίνεται ότι υπάρχει ενδιαφέρον να διερευνηθεί στη συνέχεια.

Έτσι, λοιπόν, για τις εννέα πρώτες ερωτήσεις κλειστού τύπου χρησιμοποιήθηκε περιγραφική ανάλυση. Ειδικότερα, στην ερώτηση 1 όπου οι εκπαιδευτικοί ρωτήθηκαν αν ο ιστότοπος BEsafe τους προετοιμάζει κατάλληλα για την κατανόηση του περιεχομένου του ιστότοπου Safesocialmedia, οι 14 απάντησαν «Συμφωνώ» και οι 18 απάντησαν «Συμφωνώ απόλυτα».



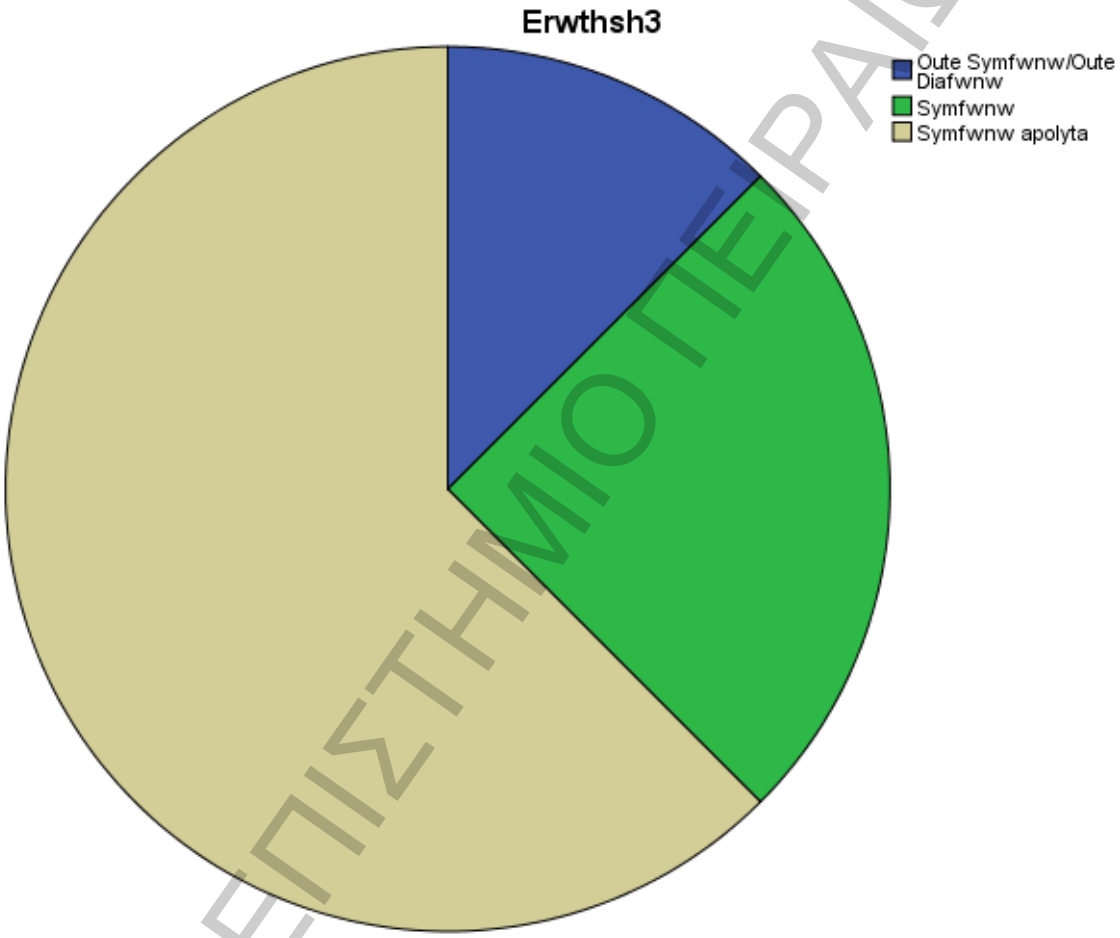
Εικόνα 43: Στατιστικά στοιχεία για την Ερώτηση 1 Ερωτηματολογίου

Στην ερώτηση 2 όπου οι εκπαιδευτικοί ρωτήθηκαν αν οι ιστότοποι BEsafe και Safesocialmedia τους ενημερώνουν πλήρων για την ασφαλή χρήση του Διαδικτύου, οι 2 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 10 απάντησαν «Συμφωνώ» και οι 20 απάντησαν «Συμφωνώ απόλυτα».



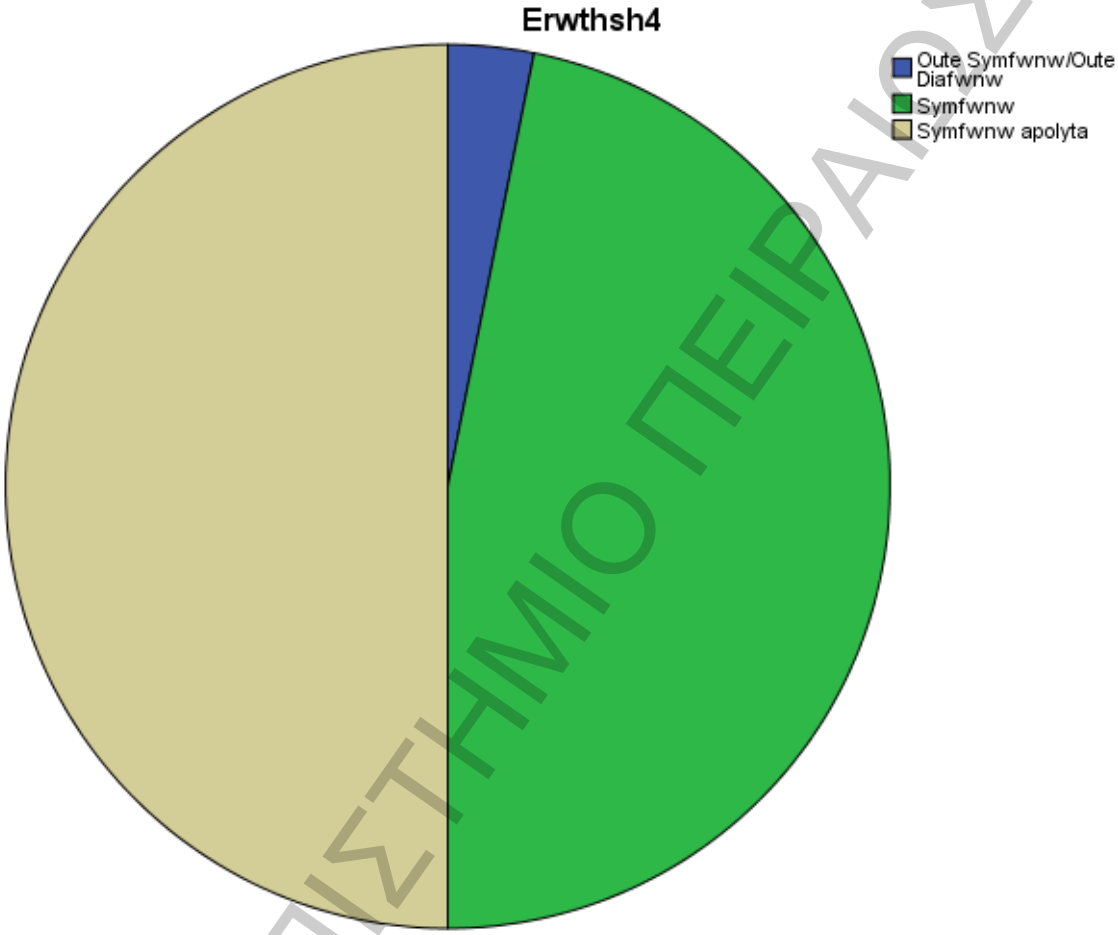
Εικόνα 44: Στατιστικά στοιχεία για την Ερώτηση 2 Ερωτηματολογίου

Στην ερώτηση 3 όπου οι εκπαιδευτικοί ρωτήθηκαν αν οι ιστότοποι είναι ελκυστικοί και λειτουργικοί τυπογραφικά, δηλαδή ως προς τα στοιχεία που χρησιμοποιούνται για τη διευκόλυνση της ενημέρωσης μου (υπογραμμίσεις, επισημάνσεις, χρήση κεφαλαίων, πλαγίων και έντονων γραμμάτων, χρωματικές κωδικοποιήσεις), οι 4 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 8 απάντησαν «Συμφωνώ» και οι 20 απάντησαν «Συμφωνώ απόλυτα».



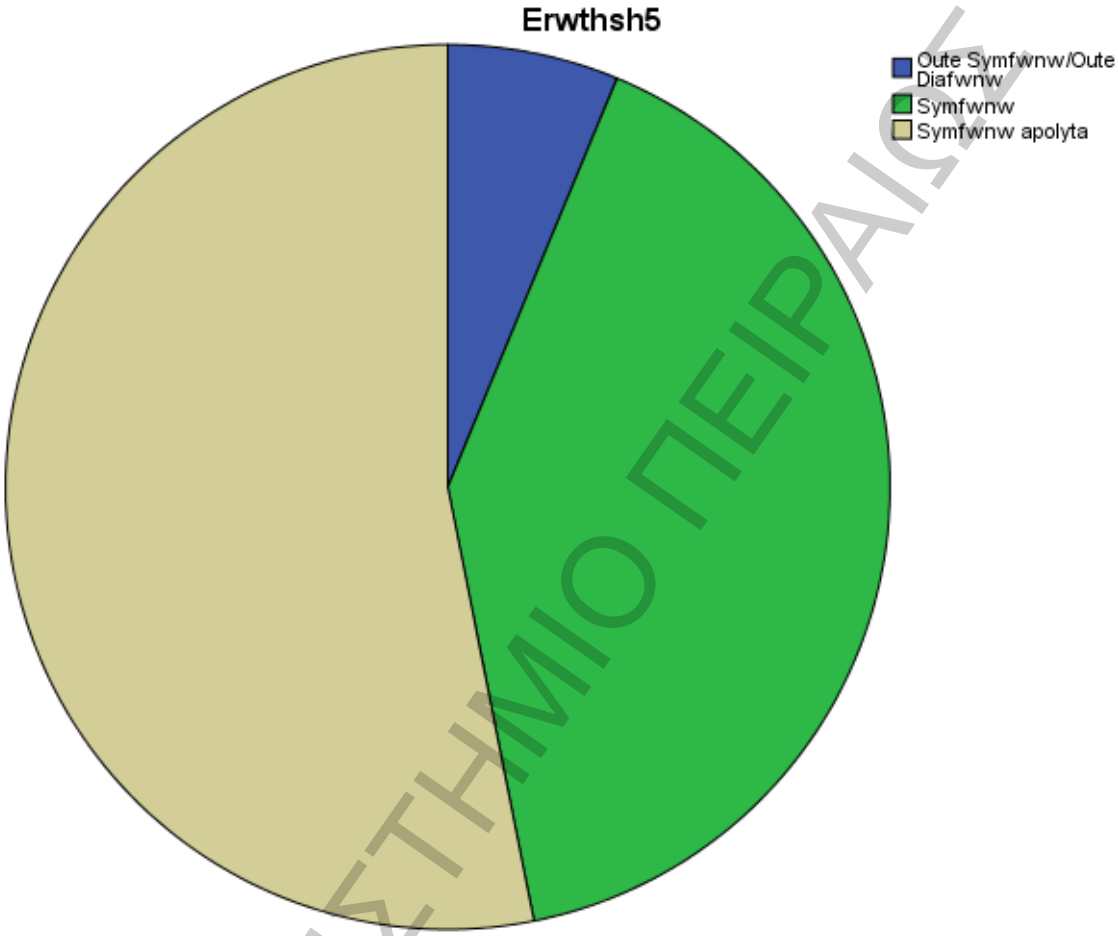
Εικόνα 45: Στατιστικά στοιχεία για την Ερώτηση 3 Ερωτηματολογίου

Στην ερώτηση 4 όπου οι εκπαιδευτικοί ρωτήθηκαν αν μπορούν να κατανοήσουν με ευκολία τα κείμενα και τις δραστηριότητες που περιγράφονται στους ιστοτόπους, ο 1 απάντησε «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 15 απάντησαν «Συμφωνώ» και οι 16 απάντησαν «Συμφωνώ απόλυτα».



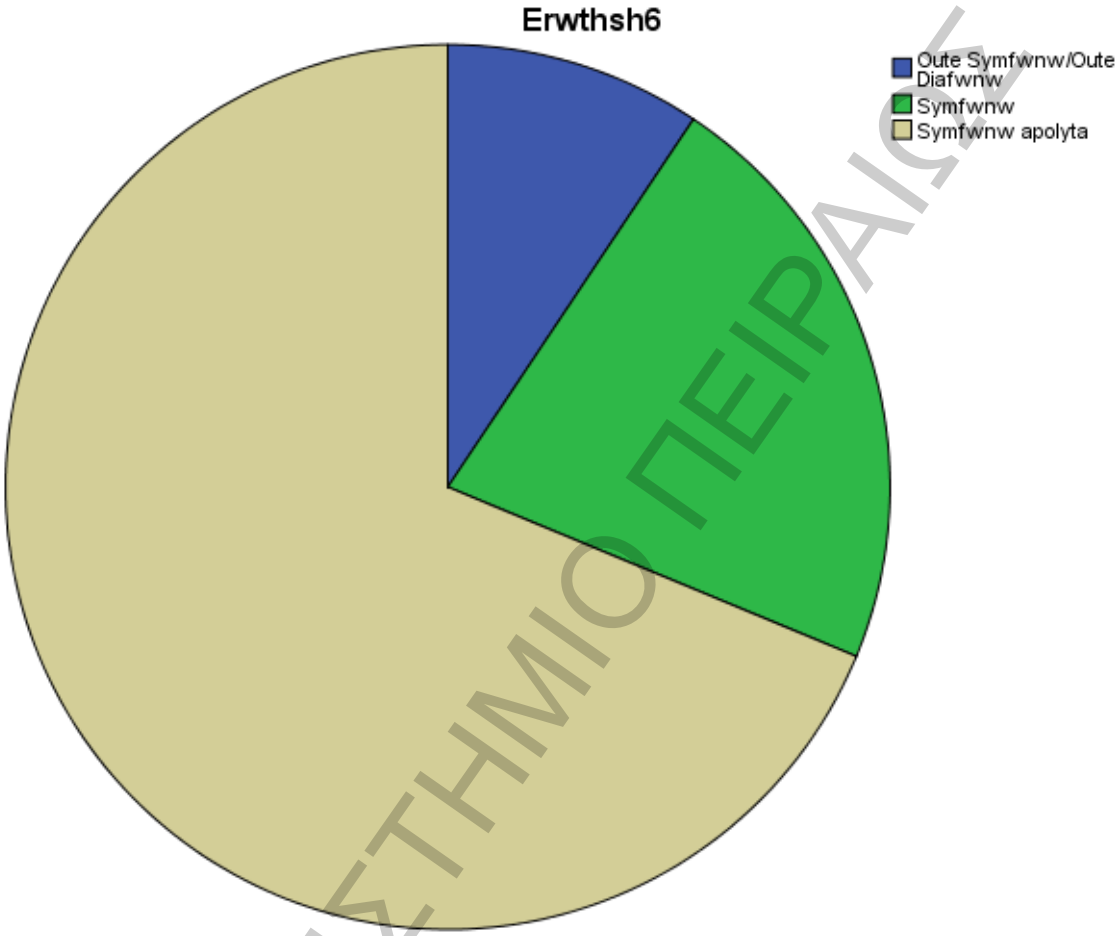
Εικόνα 46: Στατιστικά στοιχεία για την Ερώτηση 4 Ερωτηματολογίου

Στην ερώτηση 5 όπου οι εκπαιδευτικοί ρωτήθηκαν αν τα βίντεο που παρουσιάζονται στους ιστοτόπους συμβάλλουν στη διέγερση του ενδιαφέροντός τους, οι 2 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 13 απάντησαν «Συμφωνώ» και οι 17 απάντησαν «Συμφωνώ απόλυτα».



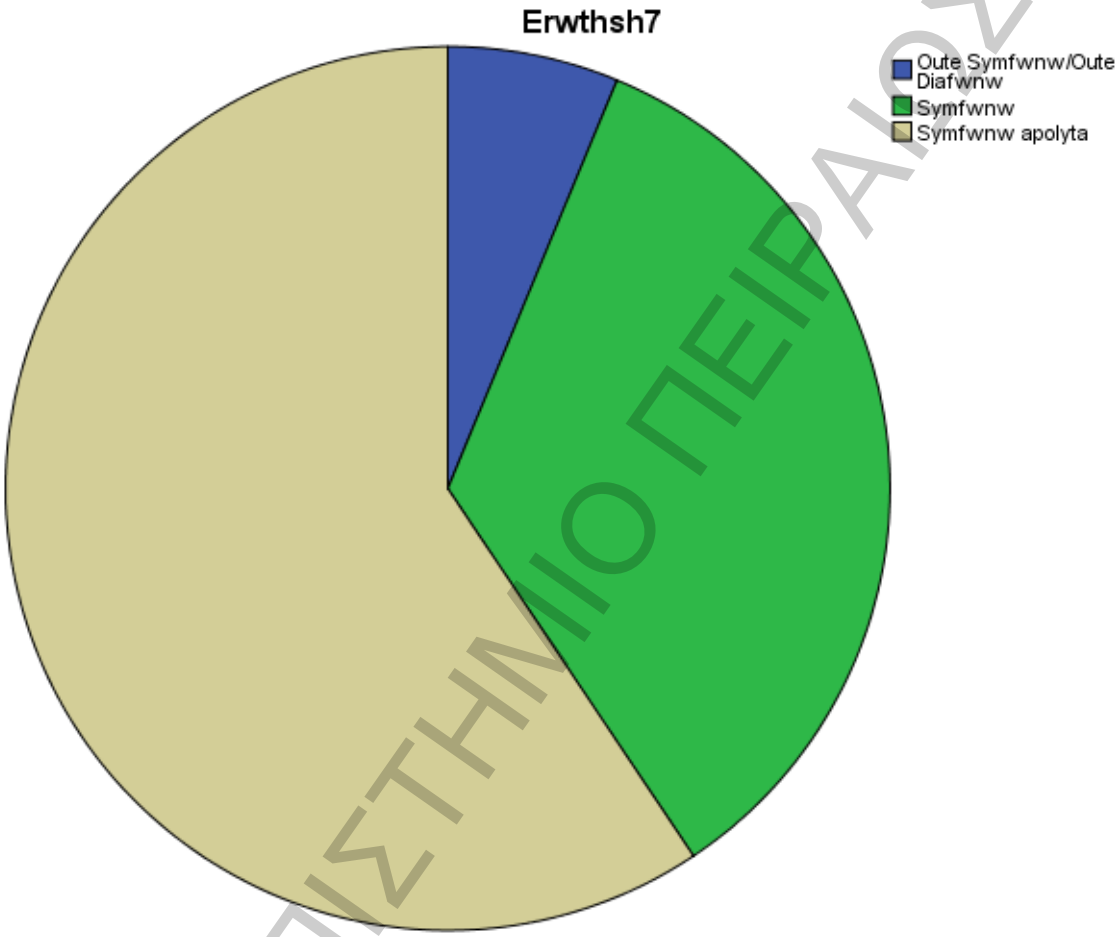
Εικόνα 47: Στατιστικά στοιχεία για την Ερώτηση 5 Ερωτηματολογίου

Στην ερώτηση 6 όπου οι εκπαιδευτικοί ρωτήθηκαν αν οι διαδραστικές αφίσες είναι κατατοπιστικές για κάθε ενότητα ώστε να διευκολύνουν τη διαδικασία της ενημέρωσης - μάθησης, οι 3 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 7 απάντησαν «Συμφωνώ» και οι 22 απάντησαν «Συμφωνώ απόλυτα».



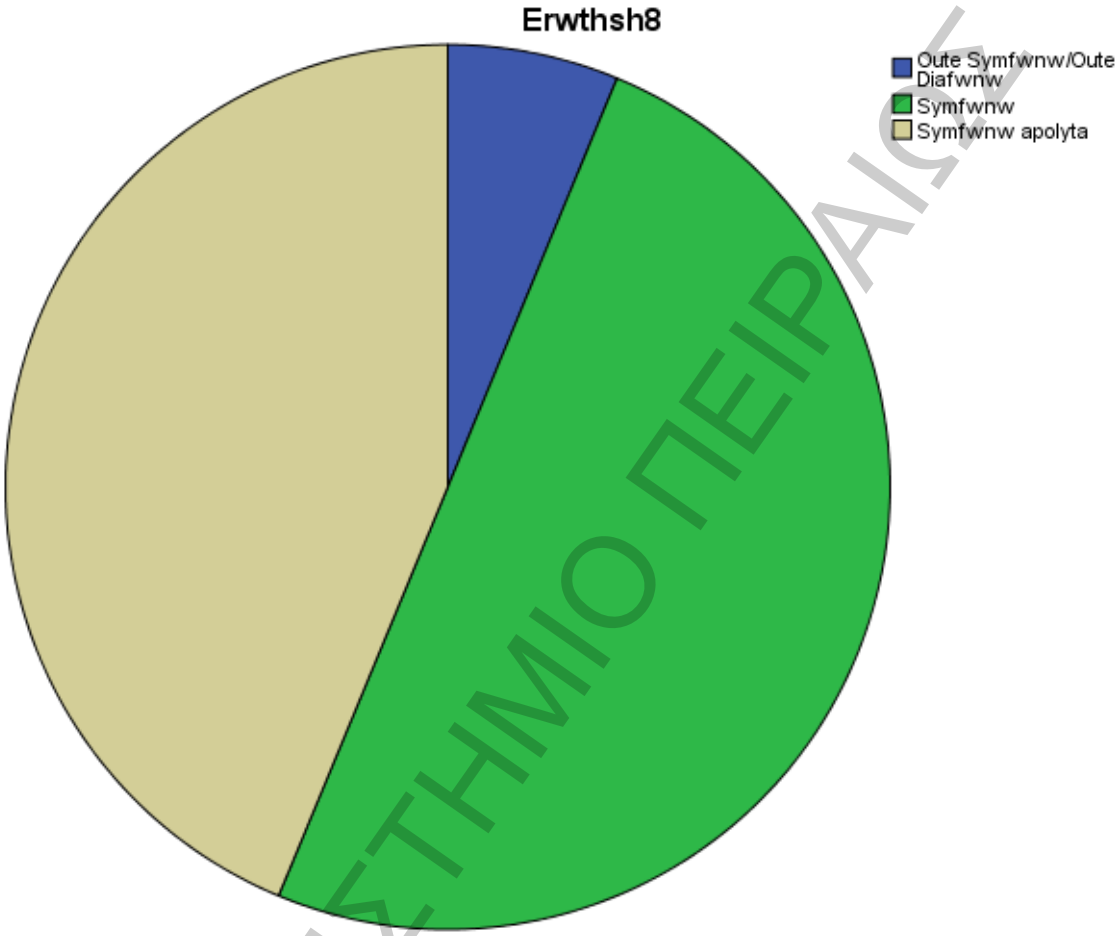
Εικόνα 48: Στατιστικά στοιχεία για την Ερώτηση 6 Ερωτηματολογίου

Στην ερώτηση 7 όπου οι εκπαιδευτικοί ρωτήθηκαν αν οι δραστηριότητες (cmap, glogster, prezi, comicstripcreator, storybird, voki) που περιγράφηκαν στην ενότητα των εκπαιδευτικών είναι ιδιαίτερα χρήσιμες, οι 2 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 11 απάντησαν «Συμφωνώ» και οι 19 απάντησαν «Συμφωνώ απόλυτα».



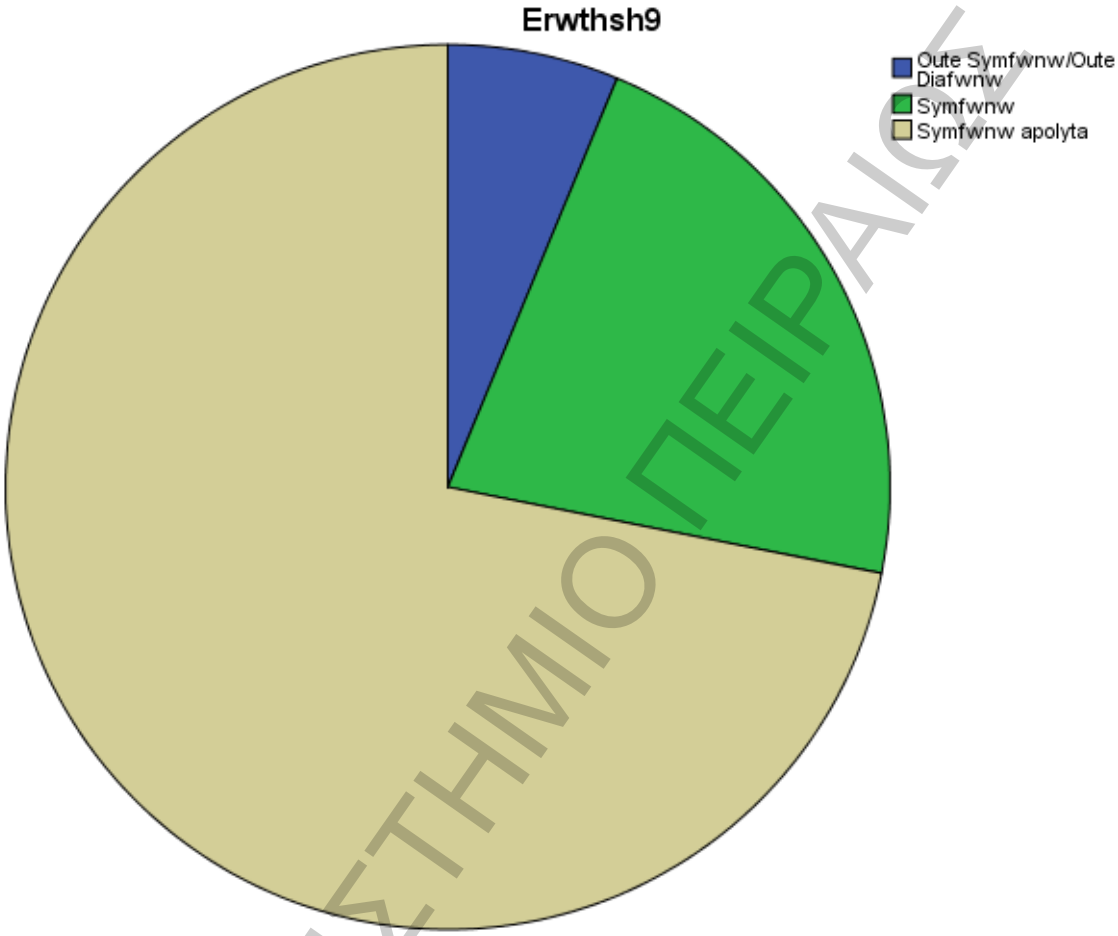
Εικόνα 49: Στατιστικά στοιχεία για την Ερώτηση 7 Ερωτηματολογίου

Στην ερώτηση 8 όπου οι εκπαιδευτικοί ρωτήθηκαν αν τα σχέδια μαθήματος βοηθούν στην καλύτερη κατανόηση του θέματος (Ασφαλή χρήση του Διαδικτύου), οι 2 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 16 απάντησαν «Συμφωνώ» και οι 14 απάντησαν «Συμφωνώ απόλυτα».



Εικόνα 50: Στατιστικά στοιχεία για την Ερώτηση 8 Ερωτηματολογίου

Στην ερώτηση 9 όπου οι εκπαιδευτικοί ρωτήθηκαν αν θα συνέστηναν ανεπιφύλακτα τους συγκεκριμένους ιστότοπους σε συναδέλφους και γονείς σα χρήσιμους και ενδιαφέροντες, οι 2 απάντησαν «Ούτε Συμφωνώ/ Ούτε Διαφωνώ», οι 7 απάντησαν «Συμφωνώ» και οι 23 απάντησαν «Συμφωνώ απόλυτα».



Εικόνα 51: Στατιστικά στοιχεία για την Ερώτηση 9 Ερωτηματολογίου

Όσον αφορά, όμως, την ποιοτική ανάλυση, δηλαδή την ανοικτού τύπου ερώτηση 10, στην οποία ζητήθηκε από τους εκπαιδευτικούς να παραθέσουν οποιαδήποτε παρατήρηση ή σχόλιο που θα μπορούσε να βοηθήσει στη βελτίωση των ιστοτόπων του BEsafe και του Safesocialmedia, τα αποτελέσματα που πήραμε ήταν τα ακόλουθα. Στη συγκεκριμένη ερώτηση απάντησαν οι 10 από τους 32 εκπαιδευτικούς που ανταποκρίθηκαν στη συμπλήρωση του ερωτηματολογίου.

Αναλυτικότερα, οι παρατηρήσεις - σχόλια που ελήφθησαν ήταν οι ακόλουθες:

1. Πολύ χρήσιμα sites για την παρουσίαση του θέματος ασφαλούς χρήσης του Internet στα παιδιά.
2. Οι ιστότοποι BEsafe και Safesocialmedia αποτελούν εξαιρετική βοήθεια για οποιονδήποτε (εκπαιδευτικό, μαθητή, γονέα) ενδιαφέρεται να λάβει πληροφορίες σχετικά με την ασφαλή πλοήγηση στο Διαδίκτυο. Όντας εκπαιδευτικός, η πλοήγηση μου στους εν λόγω ιστότοπους με έχει εκπλήξει ευχάριστα και θεωρώ πως θα μπορούσε να αποτελέσει πανίσχυρο παιδαγωγικό εργαλείο στην προσπάθεια ενημέρωσης για τους κινδύνους που ενέχει το διαδίκτυο!!! Είναι ελκυστικοί, κατανοητοί, άρτια δομημένοι και το πλούσιο περιεχόμενο τους θα μπορούσε να ωφελήσει τα μέγιστα τόσο το εκπαιδευτικό έργο όσο και να αποτελέσουν αρωγό στην προσπάθεια των γονέων να προστατέψουν τα παιδιά τους από τους κινδύνους στο Διαδίκτυο από τους οποίους βάλλονται σε καθημερινή βάση.
3. Θεωρώ ότι οι δυο ιστότοποι προετοιμάζουν κατάλληλα το κοινό σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο και το ενημερώνει πλήρως σχετικά με τους κινδύνους που υπάρχουν. Είναι πλήρεις, κατανοητοί και ιδιαίτερα εύχρηστοι.
4. Πολύ καλή προσπάθεια, και με καλό σκοπό.
5. Ο ιστότοπος BEsafe στην ολοκληρωμένη λειτουργία του, θα μπορούσε να υποστηριχτεί περισσότερο γραφικά. Ο ιστότοπος Safesocialmedia χρειάζεται εμπλουτισμό ως προς το περιεχόμενο του και τη στοχοθέτηση του θέματος λειτουργίας (socialmedia). “Yesterday I was clever, so I wanted to change the world. Today I am wise, so I am changing myself.” Rumi Συνεχίστε την καλή δουλειά
6. Όσον αφορά το BEsafe, θα έδινα περισσότερη έμφαση στο "αισθητικό" κομμάτι του site, φροντίζοντας για τη διαμόρφωση των κειμένων και του

υλικού στο σύνολό του. Πολύ καλή δουλειά! Μπράβο στην ομάδα. Ελπίζω να έχετε θετικά αποτελέσματα από την έρευνά σας!

7. Αξιόλογη και προσεγμένη ενημέρωση σχετικά με τους κινδύνους που παραμονεύουν στο διαδίκτυο. Θεωρώ πως τόσο οι συνάδελφοι μου όσο και οι γονείς θα μπορούσαν να ωφεληθούν ιδιαίτερα από τις πληροφορίες που περιέχονται στους δύο ιστοτόπους. Θα τους συνέστηνα ανεπιφύλακτα!
8. Το περιεχόμενο και των δύο ιστοτόπων άπτεται των ενδιαφερόντων των εκπαιδευτικών και γονέων της ψηφιακής εποχής...μια πολύ καλή προσπάθεια! Συνεχίστε έτσι!!
9. Θεωρώ πως με τη συνδρομή των δύο αυτών ιστοτόπων επιτυγχάνεται η αξιόπιστη και επικαιροποιημένη ενημέρωση εκπαιδευτικών, μαθητών καθώς και των γονιών και κηδεμόνων τους, για ασφαλέστερη χρήση του Διαδικτύου. Μια ιδιαίτερα εποικοδομητική πρόταση.
10. Κίνηση που πιστεύω πως θα συντελέσει στη δημιουργία ενός Ασφαλούς Διαδικτύου για όλους. Θα παρακολουθήσω στενά την πορεία των δύο ιστοτόπων ελπίζοντας να αποκομίσω ακόμη περισσότερη γνώση και πληροφορίες σχετικά με την ασφαλή χρήση του διαδικτύου.

ΚΕΦΑΛΑΙΟ 5. ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Επισκόπηση Αποτελεσμάτων

Με βάση τα αποτελέσματα που αναφέρθηκαν στο προηγούμενο κεφάλαιο, φαίνεται ότι οι συμμετέχοντες είναι, σε γενικές γραμμές, ευχαριστημένοι και με τους δυο ιστοτόπους όσον αφορά το περιεχόμενο τους σχετικά με την «Ασφαλή Χρήση του Διαδικτύου», όπως φαίνεται και από τις απαντήσεις που έδωσαν οι περισσότεροι στην τελευταία ανοικτού τύπου ερώτηση. Επιπρόσθετα, όσον αφορά τις πρώτες εννέα ερωτήσεις, οι συμμετέχοντες επέλεξαν κατά κύριο λόγο την επιλογή «Συμφωνώ Απόλυτα» υποδεικνύοντας με αυτόν τον τρόπο μια γενικότερη ικανοποίηση ως προς τη σωστή και πλήρη ενημέρωση του κοινού από τους συγκεκριμένους ιστοτόπους.

5.2 Συζήτηση

Η συζήτηση αυτή, βασίζεται κυρίως στα αποτελέσματα που πάρθηκαν από την τελευταία ανοιχτού τύπου ερώτηση, συμπληρώνεται από μια σειρά από παρατηρήσεις που υποβλήθηκαν από τους συμμετέχοντες, όσον αφορά τη συνολική εικόνα του «BEsafe» και του «SafeSocialmedia».

Αφού οι συμμετέχοντες απάντησαν τις εννέα πρώτες ερωτήσεις κλειστού τύπου, έπρεπε να συμπληρώσουν και την τελευταία. Κατά κύριο λόγο, έμειναν απόλυτα ευχαριστημένοι από τον τρόπο γραφής και τα στοιχεία που χρησιμοποιήθηκαν έτσι ώστε να είναι όσο γίνεται περισσότερο κατανοητοί από όλους, όπως επίσης και από τις δραστηριότητες που χρησιμοποιήθηκαν για να είναι πιο προσιτοί κυρίως στις μικρότερες ηλικίες.

Συγκεκριμένα, όπως δήλωσε ένας από αυτούς, «Πολύ χρήσιμα sites για την παρουσίαση του θέματος ασφαλούς χρήσης του Internet στα παιδιά.» Στη συνέχεια ήρθε να προσθέσει ένας ακόμα πολύ αναλυτικά λέγοντας ότι: «Οι ιστότοποι BEsafe και Safesocialmedia αποτελούν εξαιρετική βοήθεια για οποιονδήποτε (εκπαιδευτικό, μαθητή, γονέα) ενδιαφέρεται να λάβει πληροφορίες σχετικά με την ασφαλή πλοήγηση στο Διαδίκτυο. Όντας εκπαιδευτικός, η πλοήγηση μου στους εν λόγω ιστότοπους με έχει εκπλήξει ευχάριστα και θεωρώ πως θα μπορούσε να αποτελέσει πανίσχυρο παιδαγωγικό εργαλείο στην προσπάθεια ενημέρωσης για τους κινδύνους που ενέχει το διαδίκτυο!!! Είναι ελκυστικοί, κατανοητοί, άρτια δομημένοι και το

πλούσιο περιεχόμενο τους θα μπορούσε να ωφελήσει τα μέγιστα τόσο το εκπαιδευτικό έργο όσο και να αποτελέσουν αρωγό στην προσπάθεια των γονέων να προστατέψουν τα παιδιά τους από τους κινδύνους στο Διαδίκτυο από τους οποίους βάλλονται σε καθημερινή βάση.»

Οι συμμετέχοντες επίσης εντόπισαν κάποια πράγματα που ο δημιουργός θα μπορούσε να λάβει υπόψη έτσι ώστε να γίνει «αισθητικά πιο όμορφο». Συγκεκριμένα αναφέρει «Όσον αφορά το BEsafe, θα έδινα περισσότερη έμφαση στο "αισθητικό" κομμάτι του site, φροντίζοντας για τη διαμόρφωση των κειμένων και του υλικού στο σύνολό του. Πολύ καλή δουλειά! Μπράβο στην ομάδα. Ελπίζω να έχετε θετικά αποτελέσματα από την έρευνά σας!».

Συμπερασματικά, φυσικά μπορεί και να απαιτούνται κάποιες μικρές προσαρμογές και διορθώσεις στους ιστοτόπους αλλά οι ιστότοποι στο σύνολό τους είναι πλήρεις και αποτελεσματικοί για το σκοπό για τον οποίο δημιουργήθηκαν, σύμφωνα με τις απόψεις των τριάντα-δύο συμμετεχόντων που απάντησαν το ερωτηματολόγιο.

5.3 Μελλοντική Έρευνα

Η παρούσα έρευνα έγινε με στόχο την ενημέρωση των εκπαιδευτικών για την ασφάλεια στο διαδίκτυο με τη συνδρομή πολυμεσικού υποστηρικτικού υλικού η οποία διευκολύνεται μέσα από μια ιστοσελίδα, την BEsafe, η οποία αποτελεί συνοδευτικό ιστότοπο του SafeSocialmedia, όπου (στη BEsafe) παρουσιάζονται ιδέες για δραστηριότητες τόσο σε εκπαιδευτικούς όσο και σε γονείς ώστε να βοηθήσουν τους μαθητές να κατανοήσουν και να οχυρωθούν απέναντι στους κινδύνους που ενέχει το διαδίκτυο.

Σε μελλοντική έρευνα, θα μπορούσε να γίνει επίσκεψη στα σχολεία και να παρουσιαστούν οι ιστότοποι αρχικά στους εκπαιδευτικούς και εν συνεχεία στους γονείς και στα παιδιά. Αφού το μελετήσουν αναλυτικά όλοι οι παραπάνω, θα χρειαστεί να απαντήσουν σε ένα αντίστοιχο ερωτηματολόγιο, έτσι ώστε μέσα από τα αποτελέσματα που θα ληφθούν, οι ιστότοποι να προβούν στις απαραίτητες αλλαγές και βελτιώσεις, εφόσον υπάρχουν προβλήματα ή δυσνόητα μέρη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Adomaitis, M., *Kids Safety on the Internet*, 2006 (http://safety.lovetoknow.com/Kids_Safety_on_the_Internet).

Alongi, C., "Response to Kay Haugaard: Comic Books Revisited", *Reading Teacher*, vol.27, pp.801-803, 1974.

Ausubel D., Novak J. and Hanesian H., *Educational Psychology: A Cognitive View*, New York: Holt, Rinehart and Winston (2nd ed.), 1978.

Basque, J. and Lavoie, M-C., "Collaborative Concept Mapping in Education: Major Research Trends, in A. Cañas and J. Novak (eds.)", *Concept Maps: Theory, Methodology, Technology, Proceedings of the Second International Conference on Concept Mapping*, vol. 1, pp.79-86, San José, Costa Rica, 2006.

Berson, M., "The Computer Cannot See You Blush" *Pi Delta Kappa Record*, vol.36(4), pp.158-162, 2000.

Greekaffiliates, *Weebly*, 2011 (http://greekaffiliates.gr/weebly/).

Hutchinson, K., "An Experiment in the Use of Comics as Instructional Material", *Journal of Educational Sociology*, vol.23, pp.236-245, 1949.

Hsu, L-L., "Developing Concept Maps from Problem-Based Learning Scenario Discussions", *Journal of Advanced Nursing*, vol.48(5), pp.510-518, 2004.

Kim, B., Yang, C. and Tsai, I., "Review of Computer-Mediated Collaborative Concept Mapping: Implication for Future Research", in T. Koschmann, D. Suthers and T. W. Chan (eds.), *Proceedings of the 2005 Conference on Computer Support for Collaborative Learning (CSCL): The next 10 years*, pp.291-295,Taipei, Taiwan, 2005.

Komis, V., Avouris, N. and Fidas, C., "Computer-Supported Collaborative Concept Mapping: Study of Synchronous Peer Interaction", *Education and Information Technologies*, vol.7(2), pp.169-188, 2002.

Lee, Y., and Nelson, D., "Viewing or Visualizing – Which Concept Map Strategy Works Best on Problem-Solving Performance?", *British Journal of Educational Technology*, vol.36(2), pp.193-203, 2005.

Liu, X., "Using Concept Mapping for Assessing and Promoting Relational Conceptual Change in Science", *Science Education*, vol.88(3), pp.373-396, 2004.

McAleese, R., "The Knowledge Arena as an Extension to the Concept Map: Reflection in Action", *Interactive Learning Environments*, vol.6, pp.1-22, 1998.

McCloud Scott, *Understanding comics*, Northampton MA Kitchen Sink Press Inc p.9, pp.64-69, 1993.

Media Awareness Network, *Canada's Children in a Wired World: The Parents' View – Final Report.* Ottawa: Media Awareness Network, 2001.

Mintzes, J., Wandersee, J. and Novak, J., *Assessing Science Understanding: A Human Constructivist View*, Educational Psychology Series, London: Academic Press, 2000.

NCTE, *Dot.Safe Project*. Dublin: NCTE, Dublin City University, National Centre for Technology in Education, 2001.

Novak, J. and Gowin, D., *Learning How to Learn*, New York: Cambridge University Press, 1984.

Pearsall, N. R., Skipper, J. and Mintzes, J., "Knowledge Restructuring in the Life Sciences: a Longitudinal Study of Conceptual Change in Biology", *Science Education*, vol.81(2), pp.193-215, 1997.

Redding, V., "Information Society Commisioner", *Position in Teachers Told to Protect Children from Online Risks*, 2008. (http://www.euractiv.com/en/infosociety/teachers-told-protectchildren-online-risks/article-171879)

Sones, W., "The Comics and Instructional Method", *Journal of Educational Sociology*, vol.18, pp.232-240, 1944.

Stoyanova, N. and Kommers, P., "Concept Mapping as a Medium of Shared Cognition in Computer Supported Collaborative Problem Solving", *Journal of Interactive Learning Research*, vol.13(1/2), pp.111-133, 2002.

Sturm, James., "Comics in the Classroom", *The Chronicle of Higher Education*, pp. B14-5, April 5, 2002.

Tynes, B.M., "Internet Safety Gone Wild?", *Journal of Adolescent Research* vol.22(6), pp.575-584, 2007.

Valcke, M., Schellens, T., Van Keer, H., Gerarts, M., "Primary School Children's Safe and Unsafe Use of the Internet at Home and at School: An Exploratory Study", *Computers in Human Behavior* 23, pp.2838-2850, 2007.

Versaci, R., "How Comic Books Can Change the Way Our Students See Literature", *Teacher's Perspective English Journal*, vol.91(2), pp.61-67, 2001.

Williams, N., "The Comic Book as Course Book: Why and How", *Annual Meeting of the Teachers of English to Speakers of Other Languages*, CA, 1995.

Yang, G., "Comics in Education", *Masters of Education degree thesis*, California State University at Hayward, 2003.

Αντωνιάδης, Λ., *Διδακτική της Ιστορίας*, pp.155-157, Εκδόσεις Πατάκη, Αθήνα, 1995.

Βασιλικοπούλου Μ., Αλτάνης Ι., Μπολουδάκης Μ., Γεωργιακάκης Π., Ρετάλης Σ., "Πιλοτικό Εργαστήριο Χρήσης Εκπαιδευτικών Ψηφιακών Κόμικς σε Μαθητές Δευτεροβάθμιας Εκπαίδευσης με Θέμα την Ισότητα των Δύο Φύλων, Πρακτικά 1ου Εκπαιδευτικού Συνεδρίου", *Ένταξη και Χρήση των ΤΠΕ στην Εκπαιδευτική Διαδικασία*, 2009, (http://www.etpe.gr/files/proceedings/24/1244808037_%D0%E9%EB%EF%F4%E9%EA%FC%20%C5%F1%E3%E1%F3%F4%DE%F1%E9%EF%20%D7%F1%DE%F3%E7%F2%20%C5%EA%F0%E1%E9%E4%E5%F5%F4%E9%EA%FE%ED%20%D8%E7%F6%E9%E1%EA%FE%ED%20%CA%FC%EC%E9%EA%F2.pdf**).**

Γρηγοριάδου, Μ, Γουλή, Ε. και Γόγουλου, Α., *Ο Εννοιολογικός Χάρτης στη Μαθησιακή Διεργασία της Εκπαίδευσης από Απόσταση*, στο Α. Λιοναράκης (επιμ.), Πρακτικά Εισηγήσεων 2ου Συνεδρίου για την Ανοικτή και εξ Αποστάσεως Εκπαίδευση, σελ.371-381, Πάτρα, 2003.

Δίκτυο Υπεύθυνων Οργανισμών & Ενεργών Πολιτών, *Η Ασφάλεια στο Διαδίκτυο,* 2011 (http://www.qualitynet.gr/displayITM1.asp?ITMID=67464&LANG=GR).

Κανάς Δ., *Μαθητικές Ιστοσελίδες*, 2010 (http://www.labschool.eu/web-service/research-education/weebly-for-education-greek-school.html?page=3#ixzz27WaZcMGW)

Κόλλιας, Α., Μαργετουσάκη, Α., Κόμης, Β. και Γουμενάκης, Γ., *Αναπαραστάσεις Μαθητών του Δημοτικού για τις Νέες Τεχνολογίες από τη Χρήση Εννοιολογικών Χαρτών και Κειμένων*, στο Β. Κόμης (επιμ.), Πρακτικά 2ου Πανελλήνιου Συνεδρίου «Οι Τεχνολογίες της Πληροφορίας και της Επικοινωνίας στην Εκπαίδευση», σελ.551-562, Πάτρα, 2000.

Κορμάς, Γ., "Διαδίκτυο και εξάρτηση", *Ημερίδα Ημέρα Γνώσης: Εκπαίδευση Εκπαιδευτικών στο Ασφαλές Διαδίκτυο*, Ηράκλειο, Ιούνιος, 2009 (http://plirancrete.sch.gr/files/EkdilwseisSeminaria/Eisigiseis_asfales_diadiktyo%202009.zip).

Κυριαζή Ν., *Η Κοινωνιολογική Έρευνα, Κριτική Επισκόπηση των Μεθόδων και των Τεχνικών*, Ελληνικά Γράμματα, Αθήνα, 2002.

Κωστάκη Μ., *Ασφάλεια στο Διαδίκτυο*, χ.η. (http://www.cpe.gr/periodiko/asfaleia_sto_diadiktio.pdf).

Μακροβασίλης, Α., *Αθέμιτο και Παράνομο Περιεχόμενο στο Διαδίκτυο: Τεχνικά και Νομικά Ζητήματα. Μελέτη Περίπτωσης Πανελλήνιου Σχολικού Δικτύου*, 2007.

Μαρτινίδης Π., *Συνηγορία της Παραλογοτεχνίας*, Εκδόσεις Πολύτυπο, Αθήνα, 1982.

Μυλωνάς, Π., *Διαδίκτυο και Εξάρτηση*, 2009 (http://dspace.lib.uom.gr/bitstream/2159/13839/1/Milonas_Msc2010.pdf).

Πανελλήνιο Σχολικό Δίκτυο, *Ασφάλεια στο Διαδίκτυο*, 2010 (http://www.sch.gr/2010-04-07-09-22-34/2010-04-07-10-31-40?lang=el&showall=1).

Πανούτσου, *Ασφάλεια και Διαδίκτυο*, 2010 (http://gym-demen.ach.sch.gr/index.php/ergasies/34-2010-04-04-22-02-50/34-2010-04-04-21-37-02).

Παρασκευόπουλος, Ι., *Μεθοδολογία Επιστημονικής Έρευνας*, τόμ. Α΄ και Β΄, Αθήνα, 1993.

Σιώμκος Γ., Βασιλακοπούλου Αικατερίνη, *Εφαρμογή Μεθόδων Ανάλυσης στην Έρευνα Αγοράς*, Εκδόσεις Σταμούλης, Αθήνα, 2005.

Σταθακόπουλος Β., *Μέθοδοι Έρευνας Αγοράς*, Εκδόσεις Σταμούλης, Αθήνα, 2005.

ΠΑΡΑΡΤΗΜΑ 1

QUIZ ΓΙΑ ΤΗΝ ΥΠΟΣΕΛΙΔΑ «ΚΙΝΔΥΝΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

1) Εάν μια επαφή στο chat room σε ενοχλεί ή σε εκφοβίζει, τι κάνεις;

Α) Την αγνοείς και την μπλοκάρεις.

Β) Ενημερώνεις τους γονείς σου.

Γ) Ενημερώνεις τον πάροχο ή το διαχειριστή του chatroom.

Δ) Όλα τα παραπάνω.

Επεξήγηση: Αν κάποιος σε ενοχλεί ή σε εκφοβίζει μπλόκαρέ τον, αποθήκευσε τη συνομιλία και ενημέρωσε τον πάροχο ή το διαχειριστή του chatroom.

2) Μπορώ να δώσω σε κάποιον που συνομιλώ διαδικτυακά το πραγματικό μου όνομα και τη διεύθυνσή μου, εάν:

Α) Μιλάμε πολύ συχνά τους τελευταίους μήνες.

Β) Μου δώσει και εκείνος το όνομα και τη διεύθυνσή του.

Γ) Έχουμε τα ίδια χόμπι, δηλ. Εάν ακούμε την ίδια μουσική και είμαστε συνομήλικοι.

Δ) Κανένα από τα παραπάνω.

Επεξήγηση: Το πραγματικό σου όνομα και η διεύθυνσή σου αποτελούν προσωπικά δεδομένα, τα οποία δεν πρέπει ποτέ να αποκαλύπτεις στο Διαδίκτυο.

3) Έχεις ένα διαδικτυακό προφίλ, σε περίπτωση που δε θέσεις περιορισμούς, οι πληροφορίες που έχεις αναρτήσει:

Α) Είναι ορατές από όλους.

Β) Μπορούν να τις βλέπουν όλοι.

Γ) Μπορούν να τις σχολιάζουν όλοι.

Δ) Όλα τα παραπάνω.

Επεξήγηση: Να θυμάσαι ότι όλες οι πληροφορίες που αναρτάς είναι ορατές και μπορούν να σχολιαστούν από όλους, εάν εσύ δε θέσεις περιορισμούς.

4) Σε περίπτωση που νιώσεις ότι «κάτι δεν πάει καλά» κατά τη διάρκεια συναλλαγής, τι πρέπει να κάνεις;

Α) Να τη διακόψεις αμέσως και να επικοινωνήσεις με την εταιρία.

Β) Να συνεχίσεις ανενόχλητος την αγορά σου. Αποκλείεται να πάει κάτι στραβά, άλλωστε έχεις κάνεις πολλές φορές διαδικτυακές συναλλαγές.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Σε περίπτωση που νιώσεις ότι «κάτι δεν πάει καλά» κατά τη διάρκεια της συναλλαγής, πρέπει να τη διακόψεις αμέσως και να επικοινωνήσεις με την εταιρία, για να εξακριβώσεις ότι δεν πρόκειται για απάτη.

5) Λαμβάνεις ένα ανεπιθύμητο email, τι πρέπει να κάνεις;

Α) Το διαγράφεις, είναι ενοχλητικό να λαμβάνεις συνεχώς τέτοια email.

Β) Το προωθείς στους φίλους σου για να το δουν και εκείνοι.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Εάν λάβεις κάποιο email που σε φοβίσει ή σε αγχώσει, το διαγράφεις, διότι είναι ενοχλητικό να λαμβάνεις συνεχώς τέτοια email. Μιλάς αμέσως στους γονείς ή τους δασκάλους σου.

6) Μπαίνεις για πρώτη φορά σε ένα chat room και σου εμφανίζεται μια ηλεκτρονική φόρμα που πρέπει να συμπληρώσεις για να εγγραφείς σε αυτό. Τι ΔΕΝ πρέπει να κάνεις;

Α) Να τη συμπληρώσεις γράφοντας όλα τα προσωπικά δεδομένα που σου ζητάει.

Β) Να συμπληρώσεις μόνο τα στοιχεία που δεν αναφέρονται στα προσωπικά δεδομένα τα δικά σου ή της οικογένειάς σου.

Γ) Να μην εγραφείς στο συγκεκριμένο chat room.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Μη δίνεις ποτέ και σε κανέναν πληροφορίες σχετικά με τα προσωπικά δεδομένα τα δικά σου ή της οικογένειάς σου και ποτέ μη συμπληρώνεις ηλεκτρονικές φόρμες προσωπικών στοιχείων.

7) Μπορείς να στείλεις σε κάποιον που μιλάς στο Διαδίκτυο τη φωτογραφία σου, μόνο όταν:

Α) Είσαι με κάποιο φίλο σου στο δωμάτιο.

Β) Εγκρίνουν οι γονείς σου και είστε μαζί στο δωμάτιο.

Γ) Είσαι με τους συμμαθητές σου στη φωτογραφία και δε φαίνεσαι καλά.

Δ) Έχεις σβήσει τα μάτια σου από τη φωτογραφία.

Επεξήγηση: Ποτέ δε δημοσιεύεις προσωπικά σου στοιχεία στο Διαδίκτυο, ακόμα και όταν πρόκειται για μια φωτογραφία. Πρέπει σε κάθε περίπτωση να ρωτάς τους γονείς σου.

8) Έχεις κανονίσει με το φίλο σου το Γιώργο να πάτε να παίξετε, αλλά εσύ έχεις κολλήσει με ένα φοβερό παιχνίδι στο Internet. Τι κάνεις;

Α) Αφήνεις τον υπολογιστή και πας να παίξεις με το φίλο σου, όπως κάνατε κάθε Σάββατο.

Β) Αφήνεις το Γιώργο να περιμένει. Δεν πειράζει, άλλωστε θα μπορείτε να παίξετε μαζί και την άλλη εβδομάδα.

Γ) Φωνάζεις το Γιώργο στο σπίτι για να σε βοηθήσει στο παιχνίδι στο Internet.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Δεν πρέπει να αφήνεις ποτέ τους φίλους σου για να ασχολείσαι με το Διαδίκτυο.

QUIZ ΓΙΑ ΤΗΝ ΥΠΟΣΕΛΙΔΑ «ΠΡΟΣΤΑΣΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

1) Ψάχνεις στο Internet για να βρεις ένα πιο ενδιαφέρον παιχνίδι και βρίσκεις ένα που αναφέρεται σε χρήστες «Άνω των 18 χρονών». Τι κάνεις σε αυτή την περίπτωση;

Α) Δεν πειράζει. Εσύ θα παίξεις γιατί σου φαίνεται φοβερό παιχνίδι.

Β) Θα ψάξεις για άλλο παιχνίδι που θα είναι για την ηλικία σου.

Γ) Θα ρωτήσεις τους γονείς σου.

Δ) Το Β και το Γ.

Επεξήγηση: Ακολουθείς πάντα τους κανόνες μιας ιστοσελίδας στο Διαδίκτυο και ρωτάς τους γονείς σου για οτιδήποτε σε προβληματίζει.

2) Λαμβάνεις ένα email το οποίο σου δείχνει ότι μπορείς να αγοράσεις το αγαπημένο σου CD σε φοβερή τιμή. Τι κάνεις;

Α) Κλικάρεις κατευθείαν το email για να λάβεις το CD σου.

Β) Δείχνεις το email στους γονείς σου για να εγκρίνουν την αξιοπιστία του.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Μην αγοράζεις ποτέ προϊόντα που διαφημίζονται σε spam e-mail και μη ακολουθείς τους συνδέσμους (links) που περιέχουν καθώς τα περισσότερα από αυτά είναι άπατες ή δημιουργούν ρήγμα ασφάλειας στον υπολογιστή σου.

3) Όταν παίζεις ένα παιχνίδι στο Διαδίκτυο, πρέπει να:

Α) Θέτεις στον εαυτό σου κανόνες.

Β) Ελέγχεις την αυθεντικότητα της διεύθυνσης στο φυλλομετρητή.

Γ) Να μπλοκάρεις κάποιον από τους συμπαίκτες σου, σε περίπτωση που σου συμπεριφέρεται άσχημα.

Δ) Όλα τα παραπάνω.

Επεξήγηση: Όταν παίζεις ένα παιχνίδι στο Διαδίκτυο, πρέπει να προσέχεις τι είδους παιχνίδια επιλέγεις να παίξεις, να θέτεις στον ευατό σου κανόνες, να ελέγχεις την αυθεντικότητα της διεύθυνσης του φυλλομετρητή, να προσέχεις ποιους εμπιστεύεσαι και να μπλοκάρεις κάποιον από τους συμπαίκτες σου, σε περίπτωση που σου συμπεριφέρεται άσχημα.

4) Κάποια άγνωστη επαφή σου στέλνει ένα μήνυμα που έχει μόνο ένα σύνδεσμο (link). Τι κάνεις;

Α) Πατάς το σύνδεσμο για να δεις περί τίνος πρόκειται.

Β) Αγνοείς το μήνυμα. Σίγουρα πρόκειται για κάποια διαφήμιση.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Μην ακολουθείς τους συνδέσμους (links) που περιέχουν τα spam e-mails καθώς τα περισσότερα από αυτά είναι απάτες ή δημιουργούν ρήγμα ασφάλειας στον υπολογιστή σου.

5) Μπαίνεις στο chat και δέχεσαι μηνύματα από κάποιον που σε κάνουν να αισθανθείς «άβολα». Τι κάνεις;

Α) Βγαίνεις αμέσως από το chat room.

Β) Αλλάζεις το αναγνωριστικό σου όνομα (nickname)

Γ) Το λες στους γονείς σου ή στους δασκάλους σου.

Δ) Όλα τα παραπάνω.

Επεξήγηση: Αν κατά τη διάρκεια της συνομιλίας σου μέσω chatroom λάβεις κάποια μηνύματα που σε κάνουν να αισθανθείς «άβολα», μην απαντήσεις. Διάκοψε αμέσως τη συνομιλία, άλλαξε το αναγνωριστικό σου όνομα και πες το στους γονείς σου ή στους δασκάλους σου.

6) Συνάντησες κάποιον σε ένα chat room και μιλάτε. Φαίνεται πολύ ευγενικός και σου ζητά να του δώσεις τον κωδικό σου. Τι πρέπει να κάνεις;

Α) Φυσικά και να τον δώσεις. Αυτό θα βοηθήσει στη διαδικτυακή φιλία σας.

Β) Όχι, δεν πρέπει να του δώσεις τον κωδικό.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Φύλαξε τους κωδικούς σου μυστικούς και άλλαξε τους τακτικά.

7) Με ποιόν τρόπο μπορείς να προστατεύσεις τον υπολογιστή σου από το κακόβουλο λογισμικό;

Α) Να κάνεις τις απαραίτητες ενημερώσεις που χρειάζεται το λειτουργικό σου σύστημα.

Β) Να χρησιμοποίησεις λογισμικό antivirus και τείχος προστασίας.

Γ) Να κάνεις αντίγραφα ασφαλείας.

Δ) Όλα τα παραπάνω.

Επεξήγηση: Οι τρόποι για να προστατευτεί ο υπολογιστής σου από το κακόβουλο λογισμικό είναι:

•Ενημέρωση του λειτουργικού συστήματος!

•Χρησιμοποίηση λογισμικού Antivirus!

•Χρησιμοποίηση λογισμικού Antisryware!

•Χρησιμοποίηση τείχους προστασίας!

•Δημιουργία αντιγραφών ασφαλείας!

8) Οι κωδικοί πρόσβασης που έχεις, πρέπει να:

Α) Είναι απλοί και να μαντεύονται εύκολα.

Β) Περιέχει το όνομα και την ημερομηνία γέννησής σου.

Γ) Περιέχει ένα συνδυασμό γραμμάτων και αριθμών που μόνο εσύ θα θυμάσαι εύκολα.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Απέφυγε τους κωδικούς πρόσβασης που είναι εύκολο να τους μαντέψει ο οποιοσδήποτε, είναι απλοί και συνδέονται με τα προσωπικά σου στοιχεία.

QUIZ ΓΙΑ ΤΗΝ ΥΠΟΣΕΛΙΔΑ «ΟΔΗΓΙΕΣ ΓΙΑ ΑΣΦΑΛΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ»

1) Μόλις γνώρισες κάποιον στο chat room και σου ζητάει να του δώσεις το νούμερο του τηλεφώνου σου. Τι πρέπει να κάνεις;

Α) Να του το δώσεις κατευθείαν.

Β) Ποτέ μη δίνεις το τηλέφωνό σου σε κάποιον στο Διαδίκτυο.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Δεν ΠΡΕΠΕΙ ποτέ να δίνεις τα προσωπικά σου στοιχεία στο Διαδίκτυο προτού ενημερώσεις τους γονείς σου.

2) Τι κάνεις όταν κάποιος που δε γνωρίζεις, επιθυμεί να τον προσθέσεις σα φίλο στο chat σου;

Α) Απορρίπτεις και μπλοκάρεις επαφές από αγνώστους.

Β) Τον προσθέτεις έτσι ώστε να έχεις περισσότερες επαφές από τους φίλους σου.

Γ) Μιλάς μαζί του για να μάθεις περισσότερα χαρακτηριστικά για εκείνον.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Στην περίπτωση που κάποιος άγνωστος επιθυμεί να τον προσθέσεις σα φίλο στο chat σου, πρέπει να τον απορρίψεις και γενικά να μπλοκάρεις τις επαφές που είναι άγνωστοι.

3) Στην περίπτωση που δημοσιεύεις μια φωτογραφία σου στο διαδίκτυο, τότε:

Α) Χάνεις τον έλεγχο για αυτήν.

Β) Μπορείς να την αποσύρεις όποτε θέλεις.

Γ) Μπορείς να μπλοκάρεις κάποιους από το να την κατεβάσουν.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Ποτέ δε δημοσιεύεις προσωπικά σου στοιχεία στο Διαδίκτυο, ακόμα και όταν πρόκειται για μια φωτογραφία.

4) Ανακάλυψες καινούργιες ιστοσελίδες στο Διαδίκτυο και καινούρια chat rooms, τα οποία οι γονείς σου δε γνωρίζουν. Τι πρέπει να κάνεις;

Α) Πρέπει να ενημερώσεις τους γονείς σου και να τα ελέγξετε μαζί.

Β) Μπορείς να περιηγηθείς μόνος σου και να γνωρίσεις καινούρια άτομα.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Ενημέρωσε τους γονείς σου έτσι ώστε να μπαίνεις μόνο σε ιστοσελίδες που επιτρέπεται για εσένα.

5) Κάποιος σου στέλνει ενοχλητικά και στενάχωρα μηνύματα. Τι πρέπει να κάνεις;

Α) Απάντησέ του με άσχημα μηνύματα.

Β) Αγνόησε τον αποστολέα, μπλόκαρέ τον, κράτησε το μήνυμα και δείξε το σε έναν ενήλικα.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Σε περίπτωση που λάβεις ενοχλητικά μηνύματα, το μόνο που πρέπει να κάνεις είναι να ενημερώσεις τους γονείς σου ή τους δασκάλους σου.

6) Είσαι στο σπίτι ενός φίλου σου. Τι κανόνες πρέπει να ακολουθήσεις από τη στιγμή που δε βρίσκεσαι στο δικό σου υπολογιστή;

Α) Ακολουθείς τους κανόνες των γονιών σου και τις οδηγίες των ιστοσελίδων που περιηγείσαι.

Β) Δε χρειάζεται να ακολουθείς τους ίδιους κανόνες στους υπολογιστές των φίλων σου, αλλά μόνο στο δικό σου.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Πάντα πρέπει να ακολουθείς τους κανόνες των γονιών σου και τις οδηγίες της κάθε ιστοσελίδας ανεξάρτητα σε ποιον ανήκει ο κάθε υπολογιστής.

7) Είσαι σε μια ιστοσελίδα όπου χρειάζεται να βάλεις το όνομα και το τηλέφωνό σου για να πάρεις μέρος σε ένα διαγωνισμό. Τι πρέπει να κάνεις;

Α) Να τα δώσεις. Εξάλλου για ένα διαγωνισμό πρόκειται μόνο, δεν μπορεί να συμβεί κάτι το ιδιαίτερο.

Β) Να μην τα δώσεις. Δεν είναι καθόλου καλή ιδέα να δώσεις σε κάποιον άγνωστο τα προσωπικά σου στοιχεία.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Πρέπει να γνωρίζεις τη διαφορά μεταξύ της διαφήμισης και της διασκέδασης. Μη δίνεις πληροφορίες σε μια εταιρία χωρίς την άδεια των γονιών σου.

8) Ο διαδικτυακός σου φίλος σου ζητά να βρεθείτε από κοντά και να μην το πεις στους γονείς σου. Τι πρέπει να κάνεις;

Α) Έχει δίκιο. Οι γονείς δε χρειάζεται να γνωρίζουν τη φιλία μας.

Β) Φυσικά και δεν πρέπει να πας. Δεν είναι καθόλου ασφαλές και πρέπει να ενημερώσεις αμέσως τους γονείς σου.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: ΠΟΤΕ δεν πρέπει να συναντηθείς με κάποιον από το Διαδίκτυο χωρίς να ενημερώσεις τους γονείς σου.

9) Ποιο από τα παρακάτω δε συμπεριλαμβάνεται στα προσωπικά στοιχεία;

Α) Να λες σε κάποιον διαδικτυακά το πραγματικό σου όνομα και τη διεύθυνση.

Β) Να λες σε κάποιον διαδικτυακά το σχολείο στο οποίο πηγαίνεις.

Γ) Να λες σε κάποιον διαδικτυακά το αγαπημένο σου χρώμα.

Δ) Να λες σε κάποιον διαδικτυακά την ημερομηνία γέννησης, αλλά όχι το όνομά σου.

Επεξήγηση: Το ονοματεπώνυμό σου, η διεύθυνση του σπιτιού σου, το τηλέφωνό σου, το σχολείο σου, η τάξη σου, οι φίλοι σου, το φύλο σου, η ηλικία σου, οι προσωπικές σου συνήθειες, τα στοιχεία των γονιών σου, τα οικονομικά στοιχεία της οικογένειάς σου και περιστατικά που έχουν να κάνουν με την υγεία σου αποτελούν ευαίσθητα προσωπικά δεδομένα σου.

10) Όταν λάβεις στα email σου, ένα email από άγνωστο αποστολέα, τι πρέπει να κάνεις;

Α) Να το ανοίξεις απευθείας.

Β) Να ενημερώσεις τους γονείς σου, γιατί μπορεί να περιέχει ιούς και να προκαλέσει σοβαρά προβλήματα στον υπολογιστή σου.

Γ) Όλα τα παραπάνω.

Δ) Τίποτα από τα παραπάνω.

Επεξήγηση: Μην ανοίγεις ποτέ e-mail και επισυναπτόμενα αρχεία από αγνώστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. Είναι πολύ πιθανό να περιέχουν ιούς και να προκαλέσουν σοβαρά προβλήματα στον υπολογιστή σου.

QUIZ ΓΙΑ ΤΗΝ ΕΝΟΤΗΤΑ «ΓΟΝΕΙΣ»

1) Γνωρίζεις τους κωδικούς που χρησιμοποιεί το παιδί σου στο Διαδίκτυο;

   Α) Ναι

   Β) Όχι

2) Γνωρίζεις πόσες ώρες την ημέρα το παιδί σου μιλάει στο chat room με άλλα άτομα;

   Α) Ναι

   Β) Όχι

3) Χρησιμοποιείς φίλτρα ασφαλείας στο Διαδίκτυο σε όλους τους υπολογιστές που έχει πρόσβαση το παιδί σου;

Α) Ναι

Β) Όχι

4) Έχεις βάλει κανόνες σχετικά με το Διαδίκτυο στο παιδί σου;

Α) Ναι

Β) Όχι

5) Ο υπολογιστής που χρησιμοποιεί το παιδί σου είναι σε κεντρική θέση στο σπίτι;

A) Ναι

B) Όχι

6) Γνωρίζει το παιδί σου όλες τις οδηγίες σχετικά με την ασφάλεια στο Διαδίκτυο, όπως περιγράφονται στη συγκεκριμένη ιστοσελίδα;

A) Ναι

B) Όχι

ΠΑΡΑΡΤΗΜΑ 2

Πίνακας 5: Σχέδιο Μαθήματος 1: Υπηρεσίες-Εφαρμογές του Διαδικτύου

ΣΧΕΔΙΟ ΜΑΘΗΜΑΤΟΣ 1: ΥΠΗΡΕΣΙΕΣ - ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ	
Περιγραφή	Αυτό το πρόγραμμα έχει σχεδιαστεί για να βοηθήσει τους μαθητές να γνωρίσουν τις υπηρεσίες και τις εφαρμογές του διαδικτύου καθώς και τους κινδύνους που εγκυμονούν.
Στόχοι	• Να είναι πιο ενήμεροι για τις υπηρεσίες και τις εφαρμογές του Διαδικτύου. • Να είναι πιο ενήμεροι για τους κινδύνους που κρύβουν οι υπηρεσίες και οι εφαρμογές. • Να βοηθήσει τους μαθητές όταν είναι συνδεδεμένοι στο διαδίκτυο να προστατευθούν από την ανάρμοστη συμπεριφορά.
Δραστηριότητες	1. Αρχικά θα χρειαστεί να γίνει μια συζήτηση γύρω από το Διαδίκτυο με σκοπό να διερευνήσουμε τις υφιστάμενες γνώσεις των παιδιών.
	2. Στη συνέχεια γίνεται προβολή της παρουσίασης Διαδίκτυο – Τι μπορεί να κάνει για σένα; Υιοθετώντας τη θέση ότι πολλοί μαθητές αυτών των ηλικιών ακόμα δε γνωρίζουν πολλά για το Διαδίκτυο, στόχος της παρουσίασης είναι να γνωρίσουν όσα παιδιά δεν ξέρουν σχετικές έννοιες και να ενημερωθούν για τη χρησιμότητα που μπορεί να έχουν για τον άνθρωπο οι διάφορες υπηρεσίες του διαδικτύου όταν

	αυτές χρησιμοποιηθούν σωστά.
	3. Ακολουθεί συζήτηση μέσα από την οποία θα αναδείξει τις απεριόριστες δυνατότητες της σωστής χρήσης του διαδικτύου. Ο εκπαιδευτικός καθοδηγεί τη συζήτηση βασιζόμενος στις πληροφορίες που προβάλλονται στην παρουσίαση, τις σχετικές διαδραστικές αφίσες και τις πιο κάτω επεξηγηματικές σημειώσεις: • Διαδίκτυο (Internet) είναι το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο (**Inter**national **Net**work). Αποτελείται από εκατομμύρια διασυνδεδεμένους υπολογιστές και εκτείνεται σχεδόν σε κάθε σημείο του πλανήτη, παρέχοντας τις υπηρεσίες του σε εκατομμύρια χρήστες Ένα "Παγκόσμιο Ηλεκτρονικό Χωριό", όπως το Διαδίκτυο, δεν μπορεί παρά να είναι πολύ καλά οργανωμένο και να παρέχει στους κατοίκους του διάφορες υπηρεσίες, για να διευκολύνει την καθημερινότητά τους, ακριβώς όπως θα συνέβαινε και σε ένα πραγματικό χωριό. Έτσι λοιπόν στο Διαδίκτυο συναντάμε κάποιες από τις βασικότερες υπηρεσίες, όπως • Ηλεκτρονικό ταχυδρομείο μέσω του οποίου οι χρήστες ανταλλάσουν γραπτά μηνύματα και αρχεία (email). • Ηλεκτρονικά καταστήματα διαφόρων ειδών από όπου οι χρήστες μπορούν να ψωνίσουν χρησιμοποιώντας την πιστωτική τους κάρτα (eshops). • Ηλεκτρονικά "δωμάτια" συνάντησης όπου οι χρήστες συναντιούνται και επικοινωνούν σε πραγματικό κυρίως χρόνο χρησιμοποιώντας είτε γραπτά μηνύματα είτε απευθείας συνομιλία (chat rooms). • Ηλεκτρονικά μουσεία τα οποία μπορούν οι χρήστες να επισκεφτούν από οποιοδήποτε μέρος του πλανήτη, να περιηγηθούν σε αυτά και να δουν τα εκθέματά τους

(emuseums).

- Ηλεκτρονικές βιβλιοθήκες όπου οι χρήστες μπορούν να αναζητήσουν και να διαβάσουν σε ηλεκτρονική μορφή (elibraries).
- Παιχνίδια με σενάριο στα οποία ο χρήστης που συνδέεται παίρνει ένα προσωπικό ρόλο και αλληλεπιδρά στο περιβάλλον του παιχνιδιού με τους υπόλοιπους απομακρυσμένους παίκτες (MUD) καθώς και Διαδικτυακά παιχνίδια που παίζονται σε πραγματικό και όχι μόνο χρόνο (egames).
- Υπηρεσία η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα και χωρίς κόστος. Οι συνομιλίες αυτές γίνονται μέσω Η/Υ συνδεδεμένου με το Διαδίκτυο ο οποίος διαθέτει μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό (voip).

Εκτός όμως από τις υπηρεσίες το Διαδίκτυο περιλαμβάνει και τις Εφαρμογές Κοινωνικής Δικτύωσης (Social Networks), οι οποίες επιτρέπουν στους χρήστες να δημιουργούν προσωπικές σελίδες μέσω εικονικών διαδικτυακών προφίλ, στοχεύοντας στη δημιουργία on-line κοινοτήτων: ανθρώπων, δηλαδή, με κοινά ενδιαφέροντα και - ή δραστηριότητες. Οι χρήστες μπορούν να δημοσιοποιούν προσωπικές πληροφορίες, φωτογραφίες, βίντεο και μηνύματα τα οποία μπορούν να δουν και να σχολιάσουν οι φίλοι τους.

Μερικές από τις πιο γνωστές Εφαρμογές Κοινωνικής Δικτύωσης είναι

- Facebook αποτελεί ένα δωρεάν Social Network στο οποίο οι χρήστες μπορούν να επικοινωνούν μέσω μηνυμάτων με τις επαφές τους και να τους ειδοποιούν όταν ανανεώνουν τις προσωπικές πληροφορίες τους. Παρέχει παιχνίδια και υπάρχει η δυνατότητα δημοσίευσης

	φωτογραφιών και βίντεο. • Twitter αποτελεί ένα δωρεάν Social Network που επιτρέπει στους χρήστες να γράφουν σύντομα μηνύματα και να διαβάζουν τα μηνύματα άλλων χρηστών της υπηρεσίας (τα γνωστά ως tweets). • Youtube αποτελεί ένα δημοφιλές Social Network το οποίο επιτρέπει αποθήκευση, αναζήτηση και αναπαραγωγή βίντεο. Τα εγγεγραμμένα μέλη αποθηκεύουν απεριόριστο αριθμό βίντεο (έως 15 λεπτά το ένα), αφήσουν σχόλια σε κάθε βίντεο, πατούν το κουμπί «Μου αρέσει» και βαθμολογούν σχόλια άλλων. Τα βίντεο μπορούν να τα δουν όλοι οι χρήστες και να πουν αν τους αρέσουν ή όχι. Για κάθε βίντεο φαίνεται ο αριθμός των μελών που το έχει δει, ώστε να φαίνονται τα πιο δημοφιλή. • MySpace αποτελεί ένα αρκετά δημοφιλές Social Network, όπου κάθε χρήστης έχει τη δυνατότητα να διαμορφώσει το προφίλ του, αλλά και να έρθει σε επικοινωνία με φίλους του και να μοιραστεί μαζί τους μηνύματα, φωτογραφίες, βίντεο κ.τ.λ. Οι χρήστες του Myspace μπορούν να ανεβάσουν μουσική και να δημιουργήσουν λίστες αναπαραγωγής.
	4. Συζητήστε με τα παιδιά εάν έχουν χρησιμοποιήσει κάποιες από τις παραπάνω υπηρεσίες ή εφαρμογές ή αν έχουν έρθει ποτέ σε επαφή μέσω του Διαδικτύου με κάποιον που δε γνωρίζουν πραγματικά.
Σενάρια για συζήτηση	1) Η Ελένη μιλάει στο διαδίκτυο εδώ και λίγες μέρες με ένα κορίτσι που ονομάζεται Κωνσταντίνα. Η Κωνσταντίνα έχει ρωτήσει τη Ελένη που μένει, πόσο χρονών είναι, σε ποιο σχολείο πηγαίνει και πώς είναι εμφανισιακά. Η Κωνσταντίνα ζήτησε από τη Ελένη να της πει που ακριβώς είναι το σχολείο που πηγαίνει. Είναι εντάξει για

	την Ελένη να της το πει; (Τι άλλο δεν θα πρέπει να πει η Ελένη στην Κωνσταντίνα;)
	2) Η Μαρία μιλάει στο διαδίκτυο εδώ και αρκετούς μήνες με την Κατερίνα. Η Κατερίνα λέει ότι είναι στην ίδια ηλικία με την Μαρία, και μένει κοντά της. Η Κατερίνα θέλει να συναντηθεί με τη Μαρία στο εμπορικό κέντρο για να πάνε για ψώνια. Πρέπει η Μαρία να πάει να τη συναντήσει; (Τι πρέπει να κάνει;)
	3) Ο Δημήτρης έλαβε ένα e-mail από κάποιον που δε γνωρίζει, με ένα επισυναπτόμενο αρχείο. Πρέπει να το ανοίξει; (Τι πρέπει να κάνει;)
	4) Η Τίνα λαμβάνει ένα μήνυμα στο διαδίκτυο από μια γυναίκα που το όνομά της είναι κα Παπαδοπούλου, και αναφέρει ότι είναι καθηγήτρια μαθηματικών. Η κα Παπαδοπούλου θέλει να μάθει σε ποιο σχολείο πηγαίνει η Τίνα και ποιο είναι το όνομα του καθηγητή της. Πρέπει η Τίνα να της δώσει αυτές τις πληροφορίες; (Τι πρέπει να κάνει;)

Πίνακας 6: Σχέδιο Μαθήματος 2: Οι Κίνδυνοι στο Διαδίκτυο

ΣΧΕΔΙΟ ΜΑΘΗΜΑΤΟΣ 2: ΟΙ ΚΙΝΔΥΝΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	
Περιγραφή	Αυτό το πρόγραμμα έχει σχεδιαστεί για να βοηθήσει τους μαθητές που χρησιμοποιούν το Διαδίκτυο για τον εντοπισμό και την αποφυγή καταστάσεων που θα μπορούσαν να απειλήσουν την ασφάλειά τους.
Στόχοι	• Να αυξηθεί η γνώση των μαθητών για την ασφάλεια στο Διαδίκτυο. • Να βοηθήσει το μαθητή για τον εντοπισμό των κινδύνων στο διαδίκτυο. • Να οικοδομήσει την κριτική σκέψη και τις δεξιότητες λήψης αποφάσεων σχετικά με τη χρήση του υπολογιστή.
Δραστηριότητες	1. Αρχικά θα χρειαστεί να παρουσιαστεί στους μαθητές το εκπαιδευτικό υλικό που υπάρχει σχετικά με την Ασφάλεια στο διαδίκτυο.
	2. Με αφορμή το εκπαιδευτικό υλικό οι μαθητές θα πρέπει να σχολιάσουν πιθανούς κινδύνους που κρύβονται στο Διαδίκτυο. Μπορούμε να επικεντρωθούμε στα εξής σημεία: • Όταν τα παιδιά χρησιμοποιούν εργαλεία επικοινωνίας στο Διαδίκτυο, διατρέχουν κίνδυνο επικοινωνίας με διαδικτυακούς διαφθορείς. • Οι διαδικτυακοί διαφθορείς κρύβονται πίσω από την ανωνυμία και προσπαθούν να δημιουργήσουν σταδιακά σχέσεις οικειότητας με άπειρα και νεαρά άτομα με στόχο την εκμετάλλευσή τους. • Τελικός στόχος τους είναι να αποσπάσουν προσωπικά στοιχεία των παιδιών (ονόματα, διευθύνσεις, τηλέφωνα) και να έρθουν σε άμεση επικοινωνία με τα παιδιά είτε τηλεφωνική ή κατά πρόσωπο.
	3. Ακολουθεί συζήτηση για τους κινδύνους που εγκυμονεί η λανθασμένη χρήση του διαδικτύου. Παράλληλα μπορεί

	να γίνεται αντιπαραβολή με τη σωστή χρήση του Διαδικτύου όπως αυτή παρουσιάστηκε στην αρχική παρουσίαση. • Αναζητώντας εικόνες ή βίντεο στον Παγκόσμιο ιστό, ιδιαίτερα αν γίνεται μη προσεκτική χρήση λέξεων-κλειδιών σε μια μηχανή αναζήτησης μπορεί να βρεθούμε μπροστά σε: ✓ Ακατάλληλο, βίαιο, ρατσιστικό ή άλλο προσβλητικό υλικό. Το διαδίκτυο περιέχει και πολλές πληροφορίες που μπορεί να μην είναι ωφέλιμες για τα παιδιά όπως πορνογραφικό υλικό, βίαια παιγνίδια, ρατσιστικά σχόλια ή άλλο ακατάλληλο υλικό. ✓ Παραπλανητικές ή λανθασμένες πληροφορίες. Το γεγονός ότι ο οποιοσδήποτε μπορεί να εκδώσει μια ιστοσελίδα χωρίς να υποστεί έλεγχο για την ορθότητα των πληροφοριών που περιλαμβάνει σε αυτή δημιουργεί τον κίνδυνο πολλές πληροφορίες στο Διαδίκτυο να είναι αναξιόπιστες, λανθασμένες ή παραπλανητικές. • Κατά την αγορά προϊόντων από μια εμπορική ιστοσελίδα μπορεί να υπάρξει ο κίνδυνος απάτης με την υποκλοπή προσωπικών στοιχείων του χρήστη και συγκεκριμένα τον αριθμό της πιστωτικής τους κάρτας. • Κατά τη χρήση του ηλεκτρονικού ταχυδρομείου μπορεί: ✓ Να μας αποσταλεί ηθελημένα ή άθελα κάποιος ιός που να προκαλέσει ζημιά στον ηλεκτρονικό μας υπολογιστή. ✓ Αν η ηλεκτρονική μας διεύθυνση πέσει σε χέρια τρίτων, να μας αποστέλλονται διαφημιστικά μηνύματα παρά τη θέλησή μας.
	4. Τέλος προκαλούμε τους μαθητές να εισηγηθούν πιθανούς τρόπους προστασίας από τους κινδύνους του Διαδικτύου. Με τη βοήθεια του εκπαιδευτικού οι μαθητές μπορούν να δημιουργήσουν ένα κώδικα σωστής χρήσης του Διαδικτύου

	συζητώντας τα παρακάτω σενάρια.
Σενάρια για συζήτηση	1) Ο Μιχάλης μιλάει στο διαδίκτυο με το φίλο του Χρήστο από το σχολείο, μελετώντας για ένα διαγώνισμα. Μελετούν μαζί για την εργασία τους. Ο Χρήστος επιμένει ότι πρέπει να βρεθούν πριν το μάθημα για να ετοιμαστούν καλύτερα για το διαγώνισμα. Είναι αυτό εντάξει; (Πρέπει να ρωτήσει και ένα γονέα για να σιγουρευτεί για αυτή τη συνάντηση;)
	2) Η Χριστίνα μιλάει στο διαδίκτυο με μία φίλη της όταν παίρνει ένα μήνυμα λέγοντας ότι υπάρχει πρόβλημα με τον υπολογιστή της και χρειάζεται να πληκτρολογήσει ξανά τον κωδικό πρόσβασης. Πρέπει να το κάνει; (Τι πρέπει να κάνει;)
	3) Ο Πέτρος μιλάει με τον Κώστα που συνάντησε στο Διαδίκτυο. Ο Κώστας προσφέρεται να τον βοηθήσει να τελειώσει την εργασία του, και ζητάει από τον Πέτρο τον αριθμό του τηλεφώνου. Είναι εντάξει για τον Πέτρο να του τον δώσει, δεδομένου ότι έχει να κάνει με την εργασία; (Τι πρέπει να κάνει;)
	4) Ο Παύλος είναι στο διαδίκτυο, όταν λαμβάνει ένα μήνυμα που λέει ότι κέρδισε ένα δωρεάν Xbox! Το μόνο που χρειάζεται είναι απλά να στείλει τη διεύθυνσή του και τον αριθμό τηλεφώνου του, ώστε να μπορεί να του αποσταλεί. Πρέπει να δώσει αυτές τις πληροφορίες; (Τι πρέπει να κάνει;)

ΠΑΡΑΡΤΗΜΑ 3

Ερωτηματολόγιο

Φόρμα αξιολόγησης BEsafe & Safesocialmedia

Στόχος της είναι η αξιολόγηση του υλικού που βρίσκεται στους δύο ιστοτόπους. Τα στοιχεία που θα συλλεχθούν είναι ανώνυμα και θα χρησιμοποιηθούν για τη βελτίωση του επιμορφωτικού υλικού που έχουμε υλοποιήσει.

1. Ο ιστότοπος BEsafe με προετοιμάζει κατάλληλα για την κατανόηση του περιεχομένου του ιστότοπου Safesocialmedia.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

2. Οι ιστότοποι με ενημερώνουν πλήρως για την ασφαλή χρήση του Διαδικτύου.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

3. Οι ιστότοποι είναι ελκυστικοί και λειτουργικοί τυπογραφικά, δηλαδή ως προς τα στοιχεία που χρησιμοποιούνται για τη διευκόλυνση της ενημέρωσης μου (υπογραμμίσεις, επισημάνσεις, χρήση κεφαλαίων, πλαγίων και έντονων γραμμάτων, χρωματικές κωδικοποιήσεις).

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

4. Μπορώ να κατανοήσω με ευκολία τα κείμενα και τις δραστηριότητες που περιγράφονται στους ιστοτόπους.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

5. Τα βίντεο συμβάλλουν στη διέγερση του ενδιαφέροντός μου.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

6. Οι διαδραστικές αφίσες είναι κατατοπιστικές για κάθε ενότητα ώστε να διευκολύνουν τη διαδικασία της ενημέρωσης - μάθησης.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

7. Οι δραστηριότητες (cmap, glogster, prezi, comicstripcreator, storybird, voki) που περιγράφηκαν στην ενότητα των εκπαιδευτικών είναι ιδιαίτερα χρήσιμες.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

8. Τα σχέδια μαθήματος βοηθούν στην καλύτερη κατανόηση του θέματος (Ασφαλή χρήση του Διαδικτύου).

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

9. Θα σύστηνα ανεπιφύλακτα τους συγκεκριμένους ιστότοπους σε συναδέλφους και γονείς σα χρήσιμους και ενδιαφέροντες.

☐ Διαφωνώ απόλυτα	☐ Διαφωνώ	☐ Ούτε Συμφωνώ/Ούτε Διαφωνώ	☐ Συμφωνώ	☐ Συμφωνώ απόλυτα

10. Παραθέστε στο διαθέσιμο χώρο οποιαδήποτε παρατήρηση ή σχόλιο που θα μπορούσε να βοηθήσει στη βελτίωση των ιστοτόπων του BEsafe και του Safesocialmedia.

ΠΑΡΑΡΤΗΜΑ 4

Πίνακας 7: Περιγραφική Ανάλυση Μεταβλητών

Statistics

		Erwthsh1	Erwthsh2	Erwthsh3	Erwthsh4	Erwthsh5	Erwthsh6	Erwthsh7	Erwthsh8	Erwthsh9
N	Valid	32	32	32	32	32	32	32	32	32
	Missing	0	0	0	0	0	0	0	0	0
Percentiles	25	4,00	4,00	4,00	4,00	4,00	4,00	4,00	4,00	4,00
	50	5,00	5,00	5,00	4,50	5,00	5,00	5,00	4,00	5,00
	75	5,00	5,00	5,00	5,00	5,00	5,00	5,00	5,00	5,00

Frequency Table
Συχνότητες Δραστηριοτήτων των Μεταβλητών

Πίνακας 8: Ερώτηση 1

Erwthsh1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Symfwnw	14	43,8	43,8	43,8
	Symfwnw apolyta	18	56,3	56,3	100,0
	Total	32	100,0	100,0	

Πίνακας 9: Ερώτηση 2

Erwthsh2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	2	6,3	6,3	6,3
	Symfwnw	10	31,3	31,3	37,5
	Symfwnw apolyta	20	62,5	62,5	100,0
	Total	32	100,0	100,0	

Πίνακας 10: Ερώτηση 3

Erwthsh3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	4	12,5	12,5	12,5
	Symfwnw	8	25,0	25,0	37,5
	Symfwnw apolyta	20	62,5	62,5	100,0
	Total	32	100,0	100,0	

Πίνακας 11: Ερώτηση 4

Erwthsh4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	1	3,1	3,1	3,1
	Symfwnw	15	46,9	46,9	50,0
	Symfwnw apolyta	16	50,0	50,0	100,0
	Total	32	100,0	100,0	

Πίνακας 12: Ερώτηση 5

Erwthsh5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	2	6,3	6,3	6,3
	Symfwnw	13	40,6	40,6	46,9
	Symfwnw apolyta	17	53,1	53,1	100,0
	Total	32	100,0	100,0	

Πίνακας 13: Ερώτηση 6

Erwthsh6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	3	9,4	9,4	9,4
	Symfwnw	7	21,9	21,9	31,3
	Symfwnw apolyta	22	68,8	68,8	100,0
	Total	32	100,0	100,0	

Πίνακας 14: Ερώτηση 7

Erwthsh7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	2	6,3	6,3	6,3
	Symfwnw	11	34,4	34,4	40,6
	Symfwnw apolyta	19	59,4	59,4	100,0
	Total	32	100,0	100,0	

Πίνακας 15: Ερώτηση 8

Erwthsh8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	2	6,3	6,3	6,3
	Symfwnw	16	50,0	50,0	56,3
	Symfwnw apolyta	14	43,8	43,8	100,0
	Total	32	100,0	100,0	

Πίνακας 16: Ερώτηση 9

Erwthsh9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oute Symfwnw/Oute Diafwnw	2	6,3	6,3	6,3
	Symfwnw	7	21,9	21,9	28,1
	Symfwnw apolyta	23	71,9	71,9	100,0
	Total	32	100,0	100,0	

Πίνακας 17: Έλεγχος Αξιοπιστίας Ερωτηματολογίου

Case Processing Summary

		N	%
Cases	Valid	32	100,0
	Excluded[a]	0	0,0
	Total	32	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,819	9

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Erwthsh1	36,16	10,459	,578	,797
Erwthsh2	36,16	9,620	,675	,782
Erwthsh3	36,22	9,467	,591	,792
Erwthsh4	36,25	10,581	,459	,808
Erwthsh5	36,25	9,677	,655	,784
Erwthsh6	36,13	9,597	,620	,788
Erwthsh7	36,19	10,738	,361	,820
Erwthsh8	36,34	10,684	,387	,816
Erwthsh9	36,06	10,770	,371	,818