Εσπερινό Γυμνάσιο με Λ.Τ. Θήβας

Σχ. Έτος 2012-2013 (Β΄ τετράμηνο)

Ασφάλεια στο διαδίκτυο

Υπεύθυνοι καθηγητές

Μπουμπούκη Μελπομένη ΠΕ10

Κανελλόπουλος Δημήτριος ΠΕ19

Θήβα, Απρίλιος 2013

Μαθητές που συμμετείχαν στην παρούσα ερευνητική εργασία ανά ομάδα

ΟΜΑΔΑ 1

«Τι είναι διαδίκτυο- Χαρακτηριστικά-Τι μας προσφέρει»

- Καραγεώργος Σωκράτης
- Πικάσης Χρήστος
- Ιφτίμιε Τσιπριάν
- Γιαούπι Ελιντόν

ΟΜΑΔΑ 2

«Θέματα ασφάλειας-1»

- Κατσέλη Σωτηρία
- Νίκας Παντελής
- Γκίκα Βασιλική

ΟΜΑΔΑ 3

«Θέματα ασφάλειας-2»

- Καραμπιτσάκου Ευαγγελία
- Τζουμανέκα Σταματία
- Κλίτσα Ουρανία

ΟΜΑΔΑ 4

«Σύνταξη και έρευνα ερωτηματολογίου-Συνεντεύξεις»

- Αγρίου Μαρία
- Ζαφάρ Αμπντουλάχ
- Λουκοπούλου Μαρία
- Νεοφώτιστος Κώστας

Ασφάλεια στο Διαδίκτυο

Περίληψη

Στα πλαίσια της μεταβαλλόμενης κοινωνίας στην οποία ζούμε, το διαδίκτυο παίζει σημαντικό ρόλο. Όμως, παρά τα αναμφισβήτητα πλεονεκτήματά του, δεν παύει να κρύβει κινδύνους που σχετίζονται με την προσωπική μας ασφάλεια. Βλαβερό λογισμικό, χάκερς και κράκερς, ασφαλείς συναλλαγές και ηλεκτρονικές απάτες, εθισμός, προσωπικά δεδομένα και κοινωνική δικτύωση. Όλα τα παραπάνω είναι θέματα ασφαλείας στα οποία βρίσκουμε λύσεις που μας προστατεύουν και μας δίνουν τη δυνατότητα να απολαύσουμε τα θετικά του ίντερνετ.

Εισαγωγή

Αντικείμενο της εργασίας αυτής αποτελεί η μελέτη θεμάτων που σχετίζονται με την ασφάλεια των χρηστών του ίντερνετ και προτείνονται τρόποι αντιμετώπισης των προβλημάτων που προκύπτουν. Η συγκεκριμένη εργασία σχετίζεται κυρίως με το μάθημα της πληροφορικής, τόσο στο περιεχόμενο όσο και στα μέσα που χρησιμοποιούνται για την υλοποίησή της. Τα κριτήρια με τα οποία επιλέξαμε το συγκεκριμένο θέμα είναι η ολοένα και συχνότερη χρήση του διαδικτύου από τους μαθητές και η ευαισθητοποίησή τους πάνω σε θέματα που αφορούν την ασφάλεια στο διαδίκτυο.

Οι μέθοδοι που χρησιμοποιήθηκαν για τη συγγραφή της εργασίας είναι:

- Βιβλιογραφική έρευνα (βιβλία, περιοδικά, εφημερίδες)
- Διαδικτυακή έρευνα
- Συνεντεύξεις
- Στατιστική έρευνα με χρήση ερωτηματολογίου

Ενότητα 1: Το Διαδίκτυο και τι μας προσφέρει

Το διαδίκτυο (Internet) είναι ένα παγκόσμιο σύστημα διασυνδεμένων δικτύων υπολογιστών και παρομοιάζεται με υπερλεωφόρο πληροφοριών. Καθημερινά διακινούνται πλήθος δεδομένων όπως κείμενα, εικόνες, ήχοι, μουσικές μέσω ψηφιακών εγγράφων τα οποία ονομάζονται ιστοσελίδες και βρίσκονται αποθηκευμένα σε διάφορους υπολογιστές ανά τον κόσμο. Όλες οι ιστοσελίδες μαζί συγκροτούν μια απ τις πιο σημαντικές υπηρεσίες διαδικτύου. Τον Παγκόσμιο Ιστό (World Wide Web).

Το πρώτο είδος διαδικτύου εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 σε πανεπιστήμιο της Καλιφόρνια με 4 υπολογιστές συνδεδεμένους μεταξύ τους. Μέχρι το 1972 οι υπολογιστές έφταναν τους 23 με ταχύτητα δικτύου 50kbps και εφαρμόζεται για πρώτη φορά το email. Το 1984 καταγράφονται 1000 υπολογιστές. Η μεγάλη άνθιση του διαδικτύου ξεκίνησε με την εφαρμογή του παγκόσμιου ιστού στο CERN το 1989 η οποία κάνει την πρόσβαση στο internet πιο εύκολη ακόμα και στην μορφή που είναι σήμερα.

Σήμερα το διαδίκτυο αγκαλιάζει κάθε γωνιά του πλανήτη. Εκατομμύρια άνθρωποι το χρησιμοποιούν καθημερινά για να επικοινωνούν και να αντλούν πληροφορίες. Η μεγάλη απήχηση οφείλεται κυρίως:

- Στις τεράστιες δυνατότητες για πληροφόρηση και επικοινωνία
- Στον εύκολο τρόπο χρήσης των υπηρεσιών
- Στο ότι οποιοσδήποτε υπολογιστής μπορεί να συνδεθεί εύκολα και γρήγορα στο διαδίκτυο με ελάχιστο επιπρόσθετο εξοπλισμό.

Το διαδίκτυο παρέχει στους χρήστες μια σειρά εργαλείων που προσφέρουν διαφορετικές δυνατότητες και τους επιτρέπει:

1) Να στείλουν ή να λάβουν μηνύματα ανά πάσα στιγμή μέσω ηλεκτρονικού ταχυδρομείου (email) σε λίγα λεπτά μέχρι την άλλη άκρη της γης με μηδενικό κόστος. Αρκεί οι υπολογιστές που ανταλλάσουν τα μηνύματα να συνδέονται στο διαδίκτυο και να γνωρίζουν την ηλεκτρονική διεύθυνση του παραλήπτη.

2) Να ανταλλάσουν μεγάλα αρχεία ηλεκτρονικής μορφής. Η διαδικασία αυτή είναι αρκετά απλή. Συνδεόμαστε μ' έναν υπολογιστή του διαδικτύου που προσφέρει διάφορα προγράμματα, επιλέγουμε αυτό που μας ενδιαφέρει και το μεταφέρουμε (download) στον υπολογιστή μας. Εκτός από χρήσιμα προγράμματα μπορούμε ακόμα

να λάβουμε ή να στείλουμε τραγούδια (σε διάφορες μορφές όπως MP3,MP4,WAV) ταινίες DVD,εικόνες, φωτογραφίες, κείμενα ή ακόμα και σύνθετα αρχεία.
3) Να συζητούν γραπτώς ταυτόχρονα με πλήθος ανθρώπων (chat-forum) φίλους ή ανθρώπους που γνωρίζουμε μέσω διαδικτύου. Ξεπερνώντας κάθε εμπόδιο απόστασης έχουμε την δυνατότητα να ανταλλάσουμε απόψεις, ιδέες με ανθρώπους με τους οποίους έχουμε κοινά ενδιαφέροντα. Αρκεί να συνδεθούμε μέσω διαδικτύου με τους υπολογιστές που μας ενδιαφέρουν και ν αρχίσουμε να πληκτρολογούμε άμεσα μηνύματα τα οποία οι άλλοι μπορούν να διαβάσουν και να απαντήσουν σε ελάχιστο χρόνο.
4) Να έχουν οπτική επαφή και ηχητική επικοινωνία με συνομιλητές αν χρησιμοποιούν την υπηρεσία τηλεδιάσκεψης, η οποία μας δίνει την δυνατότητα να έχουμε οπτικοακουστική επαφή με άλλους ανθρώπους ή μαθητές άλλων σχολείων, φίλους, συγγενείς σε οποιοδήποτε μέρος του κόσμου. Για να πραγματοποιηθεί μια τηλεδιάσκεψη απαραίτητη είναι η σύνδεση στο διαδίκτυο, μια web camera,ένα μικρόφωνο, ηχεία και το κατάλληλο λογισμικό.

Ενότητα 2: Θέματα ασφάλειας στο Διαδίκτυο

Το διαδίκτυο είναι ένας ελεγχόμενος παράδεισος. Μπορούμε να πούμε ότι μοιάζει με το μαχαίρι: μπορείς να το χρησιμοποιήσεις για να φας, μπορείς όμως να το χρησιμοποιήσεις και για να σκοτώσεις! Στο ίντερνετ μπορεί να συναντήσει κανείς όχι μόνο εκβιαστές και απατεώνες που θα σου κάνουν κακό, αλλά και επιστήμονες και ανθρώπους πρόθυμους να τον βοηθήσουν και να του λύσουν όλες του τις απορίες. Εδώ θα αναλύσουμε κάποια από τα σημαντικότερα ζητήματα που σχετίζονται με την ασφαλή χρήση του διαδικτύου.

2.1 Βλαβερό λογισμικό

Είναι το λογισμικό (προγράμματα) που προκαλούν προβλήματα στη λειτουργία του υπολογιστή. Μερικά από αυτά είναι τα εξής:

- Ιός (προκαλεί διάφορες παρενέργειες, όπως εμφάνιση διαφόρων μηνυμάτων στην οθόνη, διαγραφή ή καταστροφή αρχείων, αργή λειτουργία υπολογιστή κα).

- Σκουλήκι (Ιός που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του διαμέσου των δικτύων ηλεκτρονικών υπολογιστών).
- Δούρειος Ίππος (είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα).
- Spyware (είδος κακόβουλου λογισμικού που φορτώνεται κρυφά σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και συγκεντρώνει στοιχεία σχετικά με αυτόν, π.χ. ιστοσελίδες που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πρόσβασης πιστωτικών καρτών).

Πώς μπορούμε να προστατευτούμε;

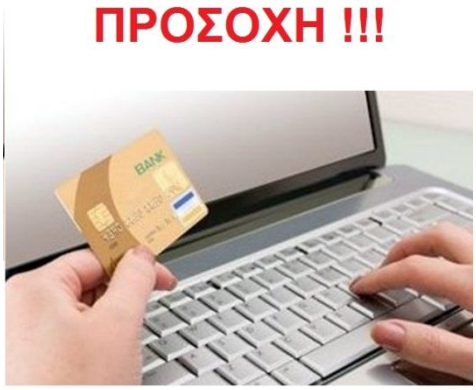
- Εγκατάσταση προγράμματος antivirus και συνεχής ενημέρωσή του, ώστε να είμαστε προστατευμένοι από το κακόβουλο λογισμικό.
- Εγκατάσταση τείχους προστασίας (firewall) ώστε να αποτρέπουμε την ανεπιθύμητη πρόσβαση στον υπολογιστή μας σε τρίτους.

2.2 Χάκερς και Κράκερς

Χάκερ (hacker) ονομάζεται κάποιος που αντλεί ευχαρίστηση από την κατανόηση της εσωτερικής λειτουργίας ενός υπολογιστικού συστήματος ή ενός δικτύου υπολογιστών, στο οποίο όμως δεν έχει δικαίωμα πρόσβασης. Ο όρος αυτός συγχέεται πολύ συχνά με τον όρο κράκερ (cracker), κάτι που αποτελεί σφάλμα. Η διαφορά τους είναι ότι ο χάκερ έχει πιο ευγενικά κίνητρα γιατί πιστεύει πως η πρόσβαση στην πληροφορία αποτελεί κοινό αγαθό, ενώ συχνά αναλαμβάνει και το ρόλο του ακτιβιστή, σε αντίθεση με τον κράκερ που θέλει να αποκτήσει πρόσβαση σε κάποιο υπολογιστικό σύστημα έχοντας ιδιοτελείς σκοπούς. Ο όρος που χρησιμοποιείται για αυτή την κατηγορία χάκερ ονομάζεται χακτιβισμός και δηλώνει τη χρήση του Διαδικτύου και των ηλεκτρονικών υπολογιστών ως μέσο διαμαρτυρίας ανθρώπων οι οποίοι υποκινούνται από πολιτικά ή ιδεολογικά κίνητρα. Οι χακτιβιστές συνήθως αλλοιώνουν την αρχική σελίδα ενός ιστότοπου ή τον θέτουν εκτός λειτουργίας. Στη δημόσια σφαίρα εξελίσσεται μια συζήτηση ανάμεσα στους υπέρμαχους και στους πολέμιους των χακτιβιστών για το αν οι δράσεις αυτών των ομάδων θα πρέπει να αντιμετωπίζονται ως πολιτικές πράξεις ή ως εγκλήματα.

2.3 Ασφαλείς συναλλαγές και ηλεκτρονικές απάτες

Μέσω του διαδικτύου έχουμε τη δυνατότητα να κάνουμε αγορές από ηλεκτρονικά καταστήματα και να έχουμε συναλλαγές με τράπεζες και δημόσιους οργανισμούς. Κατά κανόνα οι συναλλαγές αυτές είναι ασφαλείς, όμως δεν λείπουν και οι περιπτώσεις απάτης.



Πώς αναγνωρίζουμε μια αξιόπιστη ιστοσελίδα;

- Σε μια αξιόπιστη ιστοσελίδα υπάρχει ξεκάθαρος προσδιορισμός της εταιρείας με το όνομά της, τη διεύθυνση, τον αριθμό τηλεφώνου, στοιχεία επικοινωνίας κ.λπ.
- Οι όροι των συμβάσεων είναι εύκολα προσβάσιμοι και διαφανείς (συχνά θα τους βρείτε ως «όρους χρήσης»). Τα χαρακτηριστικά του προϊόντος / της υπηρεσίας και οι όροι της εγγύησης είναι σαφή και εύκολα προσβάσιμα.
- Η τιμή του προϊόντος περιλαμβάνει όλες τις τυχόν επιπλέον χρεώσεις (εκτελωνισμούς, φόρους, παράδοση στο χώρο του πελάτη, κ.λπ.).
- Ο ιστοχώρος παρέχει ασφαλή τρόπο πληρωμής (Βλ. παρακάτω).
- Οι παραγγελίες επιβεβαιώνονται με email. Οι καταναλωτές έχουν ένα σαφώς καθορισμένο δικαίωμα ανάκλησης της παραγγελίας.
- Υπάρχει Privacy policy – «Πολιτική απορρήτου» όπου διευκρινίζεται πώς θα χρησιμοποιηθούν τα προσωπικά στοιχεία που πρέπει να καταχωρίσει ο χρήστης για να πραγματοποιήσει τη συναλλαγή.

Ποιες είναι οι κυριότερες ηλεκτρονικές απάτες;

Phishing

Το phishing είναι η πρακτική της παραπλάνησης ενός χρήστη κάνοντάς τον να δώσει προσωπικές του πληροφορίες σε μια ψεύτικη φόρμα στο Διαδίκτυο. Μια τέτοιου είδους δραστηριότητα θα επιτρέψει σε έναν cracker να κλέψει ή να πλαστογραφήσει

τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς PIN, κ.λπ.

Pharming

Το pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name), που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη. Οι απατεώνες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών.

Πώς μπορούμε να προστατευτούμε;

- Θα πρέπει να είστε βέβαιοι ότι ο υπολογιστής σας δεν έχει προσβληθεί από κακόβουλο λογισμικό.
- Εγκαταστήστε φίλτρο ανεπιθύμητης αλληλογραφίας.
- Κανένας οργανισμός, και καμία αξιόπιστη εταιρία ή τράπεζα δεν θα επικοινωνούσε μαζί σας μέσω ηλεκτρονικού ταχυδρομείου για ζητήματα που αφορούν προσωπικούς κωδικούς, προσωπικά σας δεδομένα ή λογαριασμούς σας. Θυμηθείτε ότι οι συναλλαγές τέτοιου τύπου εκτελούνται αυστηρώς σε προσωπικό επίπεδο και με την προσωπική σας παρουσία. Αν λάβετε ένα τέτοιο μήνυμα, καλό είναι να απευθυνθείτε στον οργανισμό ή στην εξυπηρέτηση πελατών της εταιρίας ή της τράπεζας για να τους ενημερώσετε.
- Πριν καταχωρήσετε τα στοιχεία ενός λογαριασμού σας στο Διαδίκτυο βεβαιωθείτε πρώτα ότι βρίσκεστε στην επίσημη ιστοσελίδα της εταιρίας, ότι στο κάτω μέρος του browser υπάρχει ένα λουκετάκι και ότι η διεύθυνση αρχίζει με https://.
- Αποφύγετε να κάνετε ηλεκτρονικές συναλλαγές από υπολογιστές τρίτων ή δημόσια προσβάσιμους (π.χ. από Ίντερνετ καφέ).
- Φυλάξτε τους κωδικούς σας σε ασφαλές μέρος. Μη χρησιμοποιείτε για κωδικό ονόματα, ημερομηνίες γέννησης, επετείων κ.λπ. που εύκολα μπορεί να μαντέψει κανείς.

2.4 Εθισμός στο διαδίκτυο

Ο εθισμός στο Διαδίκτυο αναφέρεται στην «καταναγκαστική, υπερβολική χρήση του διαδικτύου και τον εκνευρισμό ή δυσθυμική συμπεριφορά που παρουσιάζεται κατά τη στέρησή της» (Mitchell, 2000). Είναι μια σχετικά νέα μορφή εξάρτησης.

Ποια είναι όμως τα αίτια του φαινομένου;

Το Ίντερνετ έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητας του χωρίς να έχει περιορισμούς.

Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει, πολλές φορές, οπτική επαφή.

Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου. Συνήθως, τα παιδιά που αντιμετωπίζουν το πρόβλημα του εθισμού στο διαδίκτυο είναι αγόρια και μεγαλώνουν σε δύσκολες καταστάσεις (δυσλειτουργικές οικογένειες).

Επίσης, ο εθισμός των εφήβων στο διαδίκτυο μπορεί, επίσης να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας, υπερκινητικότητα και κοινωνική φοβία.

Πώς μπορούμε να προστατευτούμε;

- Ενημέρωση γονέων και παιδιών και συζήτηση για θέματα που αφορούν το διαδίκτυο και τους κινδύνους που κρύβει.
- Τοποθέτηση του υπολογιστή σε κοινόχρηστο χώρο, ώστε να υπάρχει έλεγχος των παιδιών που τον χρησιμοποιούν.
- Χρήση φίλτρων για επιβλαβείς σελίδες
- Ο υπολογιστής δεν πρέπει να χρησιμοποιείται για επιβράβευση ή τιμωρία των παιδιών.

2.5 Προσωπικά δεδομένα και κοινωνική δικτύωση

Η επικοινωνία μέσω διαδικτύου είναι αρκετά συναρπαστική, αφού έχουμε τη δυνατότητα να έχουμε οπτική ή ηχητική επαφή με ανθρώπους απ' όλο τον κόσμο ή απλά να ανταλλάσσουμε μηνύματα με κάποιο πρόγραμμα chat. Τα τελευταία χρόνια κυρίαρχο ρόλο στην επικοινωνία παίζουν τα μέσα κοινωνικής δικτύωσης και ιδιαίτερα το Facebook, που είναι μια αρκετά δημοφιλής εφαρμογή στους νέους ανθρώπους (και όχι μόνο!). Όμως, υπάρχουν περιορισμοί και ποιοι κίνδυνοι κρύβονται πίσω από αυτή τη διαδικασία;

Οι ιστότοποι κοινωνικής δικτύωσης προσφέρουν στους χρήστες έναν κεντρικό χώρο στο διαδίκτυο, όπου μπορούν να δημιουργήσουν το δικό τους διαδικτυακό προφίλ που θα περιέχει προσωπικά δεδομένα, όπως το όνομά τους, την ηλεκτρονική διεύθυνσή τους, τα χόμπι τους, τι τους αρέσει και τι όχι, φωτογραφίες, βίντεο, κι όπου μπορούν επίσης να δημιουργήσουν επαφές, ή λίστες «φίλων», με τους οποίους να τα

μοιράζονται όλα αυτά. Οι χρήστες έχουν τη δυνατότητα να δημιουργούν οι ίδιοι περιεχόμενο στο Διαδίκτυο και να το μοιράζονται με άλλους χρήστες, χωρίς να έχουν εξειδικευμένες τεχνικές γνώσεις.

Θα πρέπει να αντιληφθούμε ότι μέσω των ιστοσελίδων κοινωνικής δικτύωσης εύκολα και απλά μπορούν να δημιουργηθούν τεράστιες βάσεις προσωπικών δεδομένων και προτιμήσεων από τις πληροφορίες που δημοσιεύουμε στο προφίλ μας αλλά και από τη γενικότερη δραστηριότητά μας στην ιστοσελίδα. Τα στοιχεία αυτά χρησιμοποιούνται με πολλούς τρόπους. Και εδώ πρέπει εμείς οι χρήστες να προβληματιστούμε και να ενημερωθούμε σωστά προτού αποφασίσουμε ποια στοιχεία μας θα δημοσιοποιήσουμε στις πλατφόρμες αυτές.

<u>Πώς μπορούμε να προστατευτούμε;</u>

- Πρέπει να διαβάζουμε την πολιτική απορρήτου που υπάρχει στην ιστοσελίδα της εφαρμογής για να γνωρίζουμε τον τρόπο με τον οποίο χρησιμοποιούνται τα προσωπικά μας δεδομένα.
- Δεν δημοσιεύουμε εικόνες, κείμενο ή άλλες αναρτήσεις που μπορεί αργότερα να μας φέρουν σε δύσκολη θέση.
- Από τη στιγμή που δημιουργούμε το εικονικό μας προφίλ θα πρέπει να πάμε στο μενού των ρυθμίσεων για τη διαχείριση των προσωπικών μας δεδομένων και να αλλάξουμε τις προεπιλεγμένες ρυθμίσεις.
- Να γνωρίζουμε ότι οι ιστοσελίδες κοινωνικής δικτύωσης προσφέρουν πολλές εφαρμογές (παιχνίδια, κουίζ, κ.λπ.) που παρέχονται από τρίτους, οπότε δεν υπόκεινται πάντα στην ίδια πολιτική απορρήτου που αναγράφει η ιστοσελίδα αυτή και επομένως μπορούν να διαχειριστούν τα προσωπικά μας δεδομένα με διαφορετικό τρόπο.
- Στις ιστοσελίδες κοινωνικής δικτύωσης η ανωνυμία που προσφέρεται στους χρήστες μπορεί να λειτουργήσει καμιά φορά εις βάρος των παιδιών. Συνεπώς, το «grooming» αποτελεί έναν σημαντικό κίνδυνο: Επιτήδειοι προσποιούνται ότι είναι ανήλικοι δημιουργώντας ψεύτικα προφίλ και προσπαθούν να προσεγγίσουν υποψήφια θύματα. Γι αυτό το λόγο οι γονείς πρέπει να συμβουλεύουν τα παιδιά τους να μην προσθέτουν στις λίστες φίλων τους άγνωστα άτομα.

- Καλό είναι τα παιδιά να μην ανεβάζουν στο προφίλ τους φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκονται, ειδικότερα αν πρόκειται για το σπίτι τους, το σχολείο τους ή μέρη που συχνάζουν. Έτσι μειώνονται οι πιθανότητες εντοπισμού τους στον φυσικό κόσμο.

Ενότητα 3: Ερωτηματολόγιο (Ασφάλεια στο Διαδίκτυο)

ΦΥΛΟ: _____

ΗΛΙΚΙΑ: _____

1. Έχετε πρόσβαση στο διαδίκτυο;

   Ναι ☐ Όχι ☐

2. Πόσο χρόνο περνάτε στο διαδίκτυο;

   Μέχρι 1 ώρα καθημερινά ☐ 1-2 ώρες καθημερινά ☐

   2-3 ώρες καθημερινά ☐ Περισσότερο ☐

   Λιγότερο ☐ Καθόλου ☐

3. Έχετε πέσει ποτέ θύματα απάτης στο διαδίκτυο;

   Ναι ☐ Όχι ☐

4. Πιστεύετε ότι το διαδίκτυο είναι ασφαλές για τα παιδιά;

   Ναι ☐ Όχι ☐

5. Έχετε χρησιμοποιήσει το διαδίκτυο για αγορές προϊόντων;

   Ναι ☐ Όχι ☐

6. Κατά τη γνώμη σας είναι ασφαλής η αγορά υπηρεσιών και προϊόντων μέσω διαδικτύου;

   Ναι ☐ Όχι ☐

7. Έχετε λογαριασμό στο Facebook ή σε άλλα μέσα κοινωνικής δικτύωσης;

   Ναι ☐ Όχι ☐

8. Για τα θέματα που σας αφορούν δίνετε αληθινές πληροφορίες;

   Πάντα ☐ Συνήθως ναι ☐ Μερικές φορές ☐ Ποτέ ☐

9. Έχει προσβληθεί ποτέ από ιό ο υπολογιστής σας λόγω της χρήσης του διαδικτύου;

Ναι ☐ Όχι ☐

10. Σας έχει παρενοχλήσει κάποιος μέσα από το διαδίκτυο;

Ναι ☐ Όχι ☐

11. Έχετε συναντήσει ποτέ κάποιον που γνωρίσατε μέσω διαδικτύου;

Ναι ☐ Όχι ☐

12. Έχετε κατεβάσει ποτέ παράνομα υλικό από το internet (π.χ. ταινίες, μουσική, κα);

Ναι ☐ Όχι ☐

Σας ευχαριστούμε για το χρόνο σας!!!

Αποτελέσματα της έρευνας

Ερώτηση 1

Ναι	39	Όχι	6

Ερώτηση 2

Μέχρι 1 ώρα καθημερινά	9	1-2 ώρες καθημερινά	6
2-3 ώρες καθημερινά	8	Περισσότερο	8
Λιγότερο	9	Καθόλου	5

Ερώτηση 3

Ναι	1	Όχι	44

Ερώτηση 4

Ναι	6	Όχι	39

Ερώτηση 5

Ναι	18	Όχι	27

Ερώτηση 6

Ναι	22	Όχι	23

Ερώτηση 7

Ναι	31	Όχι	14

Ερώτηση 8

Πάντα	8	Συνήθως ναι	15	Μερικές φορές	13	Ποτέ	9

Ερώτηση 9

Ναι	22	Όχι	23

Ερώτηση 10

Ναι	14	Όχι	31

Ερώτηση 11

Ναι	23	Όχι	22

Ερώτηση 12

Ναι	25	Όχι	20

Ενότητα 4: Συνεντεύξεις

Ερωτήσεις

1) Σε ποια ηλικία αρχίσατε να χρησιμοποιείτε το internet;
2) Τι κάνετε για να προστατευτείτε από τους κινδύνους που κρύβει το internet;
3) Έχετε παιδιά που χρησιμοποιούν το Facebook και τι κάνετε για να τα προστατεύσετε;
4) Μπορείτε να μας πείτε τα θετικά και τα αρνητικά του internet;
5) Έχετε πέσει θύμα στο internet; Μπορείτε να μας πείτε ένα περιστατικό που σας συνέβη;
6) Πιστεύετε ότι πρέπει να υπάρχει όριο ηλικίας των ατόμων που χρησιμοποιούν το Facebook;

1η συνέντευξη (άνδρας, 31 ετών)

1) Από 19 ετών.
2) Χρησιμοποιώ πρόγραμμα antivirus. Γενικά, όμως, δεν νιώθω να απειλούμαι.
3) Δεν έχω παιδιά, αλλά έχω τα ανίψια μου που δεν χρησιμοποιούν το Facebook.
4) Τα θετικά είναι ότι βρίσκεις οποιαδήποτε πληροφορία θες, μπορείς να βρεις τραγούδια ή βίντεο, να ενημερωθείς και να επικοινωνήσεις. Το κακό είναι ότι μπορούν να σε βρουν εύκολα και να σου κάνουν κακό κάποια άτομα και γι αυτό το λόγο χρειάζεται μεγάλη προσοχή.
5) Όχι, μέχρι τώρα δεν μου έχει τύχει τέτοιου είδους περιστατικό.

6) Το Facebook πρέπει να χρησιμοποιείται από άτομα που βρίσκονται σε ώριμη ηλικία, ώστε να γνωρίζουν τους κινδύνους που κρύβει.

2η συνέντευξη (γυναίκα, 47 ετών)

1) Από 40 ετών.
2) Δεν μπαίνω σε άγνωστες ιστοσελίδες, δεν δίνω προσωπικά δεδομένα, δεν κάνω γνωριμίες με αγνώστους και αποφεύγω τις αγορές μέσω internet.
3) Έχω κάνει συστάσεις στην κόρη μου να μην επικοινωνεί με αγνώστους μέσω internet και να μην το χρησιμοποιεί πολλή ώρα.
4) Μπορείς να βρεις ό,τι θες, να δεις άλλες χώρες, να μάθεις χρήσιμα πράγματα, να βρεις μουσική. Το αρνητικό είναι ότι κάθεσαι πολλές ώρες μπροστά στον υπολογιστή.
5) Δεν έχω πέσει ποτέ θύμα στο internet.
6) Κατά τη γνώμη μου το internet μπορούν να το χρησιμοποιούν όλοι, εκτός από τα μικρά παιδιά.

3η συνέντευξη (άνδρας, 17 ετών)

1) Από 15 ετών.
2) Δεν δίνω τα προσωπικά μου στοιχεία.
3) Έχω έναν αδερφό και του λέω απλά να προσέχει, να μη δίνει προσωπικά δεδομένα και να μη μιλά με αγνώστους.
4) Τα θετικά είναι ότι βρίσκεις ό,τι θες ανά πάσα ώρα και στιγμή. Μπορείς επίσης να βρεις διάφορες πληροφορίες και να μάθεις πολλά πράγματα που δεν γνωρίζεις. Τα αρνητικά είναι ότι μπορούν να σου κάνουν κακό εύκολα και να σε παρασύρουν.
5) Μέχρι τώρα δεν έτυχε να πέσω θύμα.
6) Πιστεύω ότι πρέπει να το χρησιμοποιούν άτομα που να γνωρίζουν τους κινδύνους που κρύβει.

Συμπεράσματα

Από τις έρευνες που κάναμε στα πλαίσια της εργασίας μας προκύπτουν αρκετά χρήσιμα συμπεράσματα. Η μεγάλη πλειοψηφία των μαθητών χρησιμοποιεί το ίντερνετ για ψυχαγωγία και ενημέρωση και είναι αρκετά ευαισθητοποιημένη και ενημερωμένη για τα προβλήματα που σχετίζονται με την ασφάλεια των χρηστών. Οι περισσότεροι διατηρούν λογαριασμό σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (κυρίως στο Facebook), αλλά προσέχουν να κάνουν σωστή χρήση και να μην δίνουν τα προσωπικά τους δεδομένα σε άτομα που δε γνωρίζουν. Πάντως, όλοι οι μαθητές, ανεξάρτητα από το επίπεδο γνώσεών τους σχετικά με την πληροφορική και το ίντερνετ, επιθυμούν να μαθαίνουν όλο και περισσότερα πράγματα σχετικά με την ασφάλεια στο διαδίκτυο.

Βιβλιογραφία-Πηγές

1) www.saferinternet.gr
2) http://www.wikipedia.org/
3) Βιβλίο Πληροφορικής Γ΄ Γυμνασίου
4) Εφημερίδα «ΤΑ ΝΕΑ», 24-1-2013