ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΠΑΙΔΑΓΩΓΙΚΟ ΤΜΗΜΑ ΔΗΜΟΤΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ:

«ΠΛΗΡΟΦΟΡΙΚΗ ΣΤΗΝ ΕΚΠΑΙΔΕΥΣΗ»

Θέμα: «Ασφάλεια στο διαδίκτυο: Εκπαιδευτικοί, γονείς, παιδιά»

ΔΙΔΑΣΚΟΜΕΝΟ ΜΑΘΗΜΑ: Εκπαιδευτική αξιοποίηση του διαδικτύου

Υπεύθυνος καθηγητής: Παναγιώτης Αναστασιάδης


| | | |
|---|---|---|
| Ομάδα εκπόνησης εργασίας : | Αγγελάκη Σταματίνα | ΑΜ: 212321 |
| | Δερβίση Κατερίνα | ΑΜ: 212326 |
| | Λαθούρης Δημήτριος | ΑΜ: 212336 |
| | Παπαγεωργίου Κώστας | ΑΜ: 211340 |
| | Πορετσάνου Ιωάννα | ΑΜ: 212346 |
| | Τζιάσιου Ελένη | ΑΜ: 212349 |
| | Τσεσμελή Γεωργία | ΑΜ: 212351 |
| | Τσολακίδου Ευθυμία | ΑΜ: 212352 |
| | Χατζηγεωργίου Δέσποινα | ΑΜ: 212353 |


ΑΘΗΝΑ 2013

**Περιεχόμενα**

**Ευχαριστίες**

Με την ευκαιρία της ολοκλήρωσης της Βιβλιογραφικής μας ανασκόπησης και έρευνας, θα θέλαμε να ευχαριστήσουμε ορισμένους ανθρώπους που μας βοήθησαν στα διάφορα στάδια ανάπτυξης της εργασίας μας.

Τις θερμότερες μας ευχαριστίες θα θέλαμε να δώσουμε, στον υπεύθυνο καθηγητή του μαθήματος κύριο Παναγιώτη Αναστασιάδη, που παρά το βαρύ του πρόγραμμα, μας βοήθησε όσες φορές κι αν τον χρειαστήκαμε, μέσω των συναντήσεων μας και των εύστοχων παρατηρήσεων του, τόσο στην ανασκόπηση της βιβλιογραφίας και στον τρόπο που γίνεται αυτή όσο και στη δομή και τον έλεγχο της παρουσίασης.

Επίσης, θα θέλαμε να ευχαριστήσουμε, τους συμφοιτητές μας για τις εύστοχες παρατηρήσεις τους κατά την ώρα της παρουσίασης. Θερμές ευχαριστίες θα θέλαμε να εκφράσουμε και στους κυρίους Μαναριώτη Χρήστο (σχολικό σύμβουλο της 4ης σχολικής περιφέρειας Αχαΐας) και Κυπριανό Παντελή (αντιπρύτανη του Πανεπιστημίου Πατρών) για την παραχώρηση μέρους έρευνας τους, σχετικά με την ελληνική πραγματικότητα της ασφαλούς πλοήγησης στο διαδίκτυο. Επιθυμία μας είναι να ευχαριστήσουμε θερμά τους συναδέλφους εκπαιδευτικούς αλλά και τους μαθητές της 4ης Εκπαιδευτικής Περιφέρειας Αχαΐας που συμμετείχαν στην έρευνα. Αρκετοί συνάδελφοι εκπαιδευτικοί υλοποίησαν προγράμματα ασφαλούς πλοήγησης στο διαδίκτυο ενημερώνοντας με τον τρόπο αυτό τόσο τους μαθητές όσο και τους γονείς τους.

Τέλος, θα θέλαμε να ευχαριστήσουμε την κυρία Μαραγκοπούλου Μαρία, Ψυχοθεραπεύτρια - Οικογενειακή Θεραπεύτρια και Κοινωνική Λειτουργό, για την παραχώρηση υλικού της, μετά από σεμινάριο που παρακολούθησε όλη η ομάδα με σκοπό την πληρέστερη προσέγγιση του θέματος. Χωρίς αυτούς θα ήταν αδύνατη η διεκπεραίωση της εργασίας μας.

## 1. Αναγκαιότητα ασφαλούς χρήσης διαδικτύου

Οι νέοι χρησιμοποιούν όλο και περισσότερο το διαδίκτυο και θεωρούνται από πολλούς ερευνητές ως οι πιο συχνοί χρήστες του (Becker, 2000). Έρευνες μάλιστα υποστηρίζουν πως ιδιαίτερα οι έφηβοι το χρησιμοποιούν ακόμα συχνότερα και από τους ενήλικες (Subrahmanyam et al, 2000).

Τα παραπάνω δεδομένα μπορούν εύκολα να εξηγηθούν εφόσον το Διαδίκτυο έχει πολλές χρήσεις για τους νέους. Αξιοποιείται τόσο στο σχολείο όσο και στο σπίτι για βοήθεια στα μαθήματα, για κοινωνική δικτύωση ή ως μέσο διασκέδασης. Αναλυτικότερα, οι νέοι χρησιμοποιούν το Internet (Pastore, 2002, Rosenbaum et. al, 2000):

- για να στέλνουν e – mail και να συνομιλούν (chat)
- για να διεκπεραιώσουν σχολικές εργασίες
- για να παίξουν παιχνίδια ή να ακούσουν μουσική
- για να παρακολουθήσουν αθλήματα και να βρουν σχετικές πληροφορίες
- για ψυχαγωγία και χόμπι
- για να βρουν ιατρικές πληροφορίες
- για να πραγματοποιήσουν αγορές online

Στις Η.Π.Α. έχει διαπιστωθεί ότι περίπου 21 εκατομμύρια έφηβοι, ηλικίας 12 – 18 ετών χρησιμοποιούν το διαδίκτυο. Σε αντίστοιχη έρευνα στην Αυστραλία αναφέρεται ότι 86% των Αυστραλών νέων, ηλικίας 13 – 18 ετών, έχουν πρόσβαση στο διαδίκτυο (Flemming et al, 2006).

Ωστόσο, το Διαδίκτυο δεν απασχολεί μόνο τους εφήβους. Σε πρόσφατη έρευνα που διεξήχθη στο Βέλγιο (Valcke et al, 2007) παρατηρήθηκε ότι τα παιδιά δημοτικού σχολείου χρησιμοποιούν το Internet με μεγάλη συχνότητα. Αναλυτικότερα, σύμφωνα με την παραπάνω έρευνα, σε δείγμα 1.700 μαθητών δημοτικού από 78 σχολεία στη Φλάνδρα, διαπιστώθηκε ότι:

- 62,9% αναφέρουν ότι χρησιμοποιούν το Διαδίκτυο καθημερινά ή τρεις φορές την εβδομάδα.
- 91,2% των μαθητών δηλώνουν ότι έχουν πρόσβαση στο Διαδίκτυο από το σπίτι τους.
- σχεδόν 60% αναφέρουν ότι χρησιμοποιούν το διαδίκτυο για σχολική εργασία.

- περίπου το 50% του δείγματος δηλώνει ότι συνομιλούν στο Internet καθημερινά ή 3 φορές την εβδομάδα.

Τα δεδομένα που παρουσιάστηκαν παραπάνω και αναφέρονται στα ποσοστά χρήσης του Διαδικτύου από τα άτομα νεαρής ηλικίας (έφηβοι και παιδιά δημοτικού) δημιουργούν ανησυχία για κάποιες πτυχές της χρήσης διαδικτύου από τους νέους. Μάλιστα, αρκετοί ερευνητές έχουν εκφράσει αυτή την ανησυχία τους (Dombrowksi et al, 2004, Freeman – Longo, 2000, Greenfield, 2004, Mitchell et al, 2001) Η ανησυχία αυτή εστιάζεται στα ενδεχόμενα της παιδεραστίας καθώς και της έκθεσης σε πορνογραφικό υλικό ή σε σεξουαλική βία, τα οποία θα έχουν σοβαρές επιδράσεις στα παιδιά και τους εφήβους.

Όπως θα φανεί παρακάτω, η ανησυχία δεν είναι καθόλου αβάσιμη. Το διαδίκτυο μπορεί να έχει αρνητικό αντίκτυπο στις κοινωνικές σχέσεις γιατί σύμφωνα με έρευνες:

- 42% των παιδιών έχουν πέσει θύματα εκφοβισμού στο διαδίκτυο (cyber-bullying)
- 47% των χρηστών έχουν εκτεθεί σε προσβλητικό ή σεξουαλικό περιεχόμενο, όπως πορνογραφία, βία κ.λπ. από τα οποία μόνο το 44% το ανέφεραν στους γονείς τους (π.χ. Mitchell et al., 2003)
- Πολλά παιδιά (περίπου 16,7%) έχουν απειληθεί στο διαδίκτυο (π.χ. Valcke et al, 2007)
- Πολλά παιδιά δεν κατανοούν τους κινδύνους που έχει να δίνουν προσωπικά στοιχεία σε άγνωστους διαδικτυακούς φίλους (Livingstone, 2003, Youn, 2008). Σε έρευνα που διεξήχθη στην Αμερική (Turow & Nir, 2000) παρατηρήθηκε ότι 45% παιδιών ηλικίας 10-17 ετών ήταν διατεθειμένα να δώσουν σημαντικά προσωπικά στοιχεία σε αντάλλαγμα ενός δώρου αξίας 100$.

Σύμφωνα με ερευνητικά δεδομένα οι γονείς δεν είναι πλήρως ενήμεροι για τους κινδύνους που αντιμετωπίζουν τα παιδιά τους στο Διαδίκτυο με αποτέλεσμα μόλις 17% των γονέων να έχουν εγκαταστήσει λογισμικό «φιλτραρίσματος» (έρευνα της Australian Broadcasting Authority, 2000). Έχει, ωστόσο, παρατηρηθεί ότι τα παιδιά των οποίων οι γονείς έχουν συζητήσει σχετικά με την ασφάλεια στο Διαδίκτυο, υιοθετούν περισσότερο ασφαλείς συμπεριφορές κατά την περιήγησή τους στο Internet. (Fleming et al. 2006)

## 2. Τι σημαίνει ασφάλεια στο διαδίκτυο

Το Διαδίκτυο θεωρείται στις μέρες μας η μεγαλύτερη τεχνολογική αλλά και κοινωνικοοικονομική επανάσταση που έχει επηρεάσει σχεδόν όλες τις πτυχές της ζωής μας. Η χρήση του αυξάνεται με ραγδαίους ρυθμούς, ικανοποιώντας ποικίλες ανάγκες που αφορούν την ενημέρωση, την ψυχαγωγία, την επικοινωνία, την αναζήτηση και ανταλλαγή πληροφοριών και δεδομένων, το ηλεκτρονικό εμπόριο. (Σοφός 2009). Γνωστά είναι τα πλεονεκτήματα του διαδικτύου: το παγκόσμιο δίκτυο των δικτύων υπολογιστών, έχει ανοίξει τεράστιες δυνατότητες για την αποστολή και λήψη πληροφοριών με αποτελεσματικό τρόπο που να επιτρέπει την ταχεία αναζήτηση και ανάκτηση πληροφοριών. Το Διαδίκτυο προσφέρει στα παιδιά και τους νέους απίθανες ευκαιρίες να ανακαλύπτουν, να συνδέονται και να δημιουργούν ηλεκτρονικά. Ωστόσο, η χρήση του Διαδικτύου ενέχει και κινδύνους.

Οι δυνατότητες που προσφέρει το Διαδίκτυο είναι τεράστιες. Η αποτελεσματική αξιοποίησή του, όμως, προϋποθέτει την ορθή χρήση του. Ως εκ τούτου, σε ευρωπαϊκό επίπεδο έχουν αναπτυχθεί δράσεις και προγράμματα που στοχεύουν στη δημιουργία ασφαλέστερων συνθηκών αξιοποίησης των δυνατοτήτων του Διαδικτύου. Η άγνοια, αλλά και η έλλειψη δεξιοτήτων χρήσης των νέων τεχνολογιών είναι δυνατό σε κάποιες περιπτώσεις να οδηγήσουν σε άβολες καταστάσεις ή ακόμη και σε κάποιο κίνδυνο.

Ασφάλεια στο διαδίκτυο σημαίνει ασφαλής, ανοιχτός, προστατευμένος κυβερνοχώρος, αξιοποίηση των δυνατοτήτων του διαδικτύου για ψυχαγωγία, μάθηση και επικοινωνία.

Να πώς αντιλαμβάνονται οι μαθητές την ασφαλή χρήση του διαδικτύου και ποια δικαιώματα επιθυμούν να απολαμβάνουν, κατά την πλοήγησή τους στο διαδίκτυο, σύμφωνα με κλειστό online ερωτηματολόγιο της Δράσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου:

- Προστασία της ιδιωτικότητας
- Δικαίωμα ελέγχου στα δεδομένα που αναρτώνται
- Να μην παρενοχλούνται από επιτήδειους
- Να μπορούν να αναφέρουν εύκολα ύποπτες ή ενοχλητικές συμπεριφορές στους διαχειριστές των εκάστοτε ιστοχώρων

- Ενημέρωση για την προστασία στο διαδίκτυο
- Ανάγκη για ποιοτικό περιεχόμενο στο διαδίκτυο- Τρόποι αποφυγή επιβλαβούς ή ενοχλητικού περιεχομένου
- Παιχνίδι και συνομιλία με φίλους
- Να μπορούν να μιλάνε σε κάποιον έμπιστο για το τι τους έχει ενοχλήσει στο διαδίκτυο
- Να δημιουργούν περιεχόμενο στο διαδίκτυο

Συνοψίζοντας όλα τα παραπάνω μπορούμε να πούμε ότι η αξιοποίηση των δυνατοτήτων του διαδικτύου για ενημέρωση, ψυχαγωγία, επικοινωνία, αναζήτηση και ανταλλαγή πληροφοριών προϋποθέτει την ορθή χρήση του καθώς και τη δημιουργία ασφαλέστερων συνθηκών πλοήγησης .Επίσης θα πρέπει οι χρήστες να γνωρίζουν και να ενημερώνονται για τους κινδύνους που διατρέχουν κατά την πλοήγησή τους σε αυτό και να λαμβάνουν τα κατάλληλα μέτρα προστασίας.

## 3. Οι εμπλεκόμενοι με την ασφάλεια στο διαδίκτυο

Στις μέρες μας που στόχος σχεδόν κάθε ευρωπαϊκής χώρας είναι να προετοιμάσει τους νέους πολίτες που θα μπορούν να ανταπεξέλθουν στις απαιτήσεις της νέας εποχής του διαδικτύου ώστε από απλοί πολίτες να μετασχηματιστούν σε πολίτες των δικτύων. Στα πλαίσια της ασφάλειας στο διαδίκτυο οι κατεξοχήν εμπλεκόμενοι είναι τα παιδιά (μαθητές), οι γονείς και οι εκπαιδευτικοί. Ως εκ τούτου, έχει προκύψει η ανάγκη αποτύπωσης των εμπειριών, απόψεων ή στάσεων τους απέναντι στο διαδίκτυο και την ασφαλή χρήση του.

### 3.1 Παιδιά και ασφάλεια στο διαδίκτυο

Σχετικά με την ασφάλεια των παιδιών στο διαδίκτυο έχει πραγματοποιηθεί πληθώρα ερευνών οι οποίες εστιάζουν στις στάσεις, τα αισθήματα και τις εμπειρίες που έχουν τα παιδιά στο διαδίκτυο. Οι Stahl και Fritz (2002) μελέτησαν τη χρήση του διαδικτύου 322 μαθητών Α΄

Γυμνασίου ως Α΄ Λυκείου. Από τους συμμετέχοντες το 21% δήλωσε ότι επισκέφτηκε ιστοσελίδα με πορνογραφικό περιεχόμενο. Περίπου το 5% ανέφερε ότι πέρασε αρκετό χρονικό διάστημα σε ιστοσελίδες που σχετίζονταν με όπλα και εκρηκτικά. Οι περισσότεροι (74%) ανέφεραν ότι είχαν επικοινωνία με κάποιον άγνωστο μέσω ηλεκτρονικού ταχυδρομείου ή chat rooms. Επίσης ένα σημαντικό ποσοστό (25%) αναγνώρισε ότι έχει μοιραστεί στο διαδίκτυο προσωπικές του πληροφορίες όπως όνομα, σχολείο, διεύθυνση ή τηλεφωνικό αριθμό.

Αυτή η μελέτη υποδηλώνει μια ανάγκη για διαρκώς αυξανόμενη μαθητοκεντρική εκπαίδευση σχετικά με το μοίρασμα ταυτότητας και εργαλεία για να εμποδίζουν ανεπιθύμητες ιστοσελίδες ή προσωπικές επικοινωνίες. Η εμπλοκή των εφήβων στη χρήση διαδικτύου από ενήλικές θα πρέπει να περιλαμβάνει αυξανόμενη επίβλεψη και έρευνα για την ανίχνευση αρνητικών και θετικών συνεπειών σχετικά με την ασφάλεια.

Η έρευνα που πραγματοποιήθηκε από τους Fleming και συν. (2006) στην Αυστραλία σε μαθητές 13-16 ετών, έδειξε διαφοροποιήσεις στη στάση των μαθητών σχετικά με το αν συζητούν ζητήματα ασφάλειας με τους γονείς. Το 47% των πιο νέων μαθητών συζητά με τους γονείς, ενώ το ποσοστό πέφτει στο 39% για μεγαλύτερους μαθητές. Επίσης διαφοροποιήσεις στο συγκεκριμένο ζήτημα παρατηρούνται μεταξύ κοριτσιών που σε ποσοστό 50% μιλούν στους γονείς τους και αγοριών από τα οποία μόνο το 38% αναφέρουν ότι είχαν τέτοια συζήτηση για θέματα ασφάλειας στο διαδίκτυο με τους γονείς.

Στα πλαίσια αυτής της έρευνας γίνεται σαφές ότι οι γονείς πρέπει να συζητούν με τα παιδιά τους γιατί μόνο μέσα από την επικοινωνία γονέων-παιδιών μπορούν να αναδειχθούν ζητήματα ασφάλειας στο διαδίκτυο. Οι συζητήσεις αυτές πρέπει να επικεντρώνονται κυρίως σε τρόπους με τους οποίους τα παιδιά θα κρατιόνται μακριά από πιθανούς κινδύνους με τη χρήση αποτελεσματικότερων πρακτικών ασφάλειας στο διαδίκτυο.

Σε έρευνα που πραγματοποιήθηκε στο Βέλγιο (Valcke, et al, 2007) σε 1700 μαθητές στην περιοχή της Φλάνδρας, τα αποτελέσματα έδειξαν υψηλό επίπεδο ανασφαλούς χρήσης του διαδικτύου όπως η συζήτηση με αγνώστους (26%), η αποστολή προσωπικών πληροφοριών (13%) περιλαμβάνοντας και προσωπικές φωτογραφίες (12.7%) και η συνάντηση με αγνώστους ύστερα από ραντεβού που κανονίστηκε μέσω του διαδικτύου (7.5%). Από τους μαθητές που συνάντησαν αγνώστους ένα ποσοστό (20.9% ) πήγε μόνο του στη συνάντηση. Η έρευνα έδειξε επίσης ότι 40.7% έχει σοκαριστεί από ακατάλληλο περιεχόμενο στο διαδίκτυο (π.χ. περιεχόμενο

βίας ή σεξουαλικό). Περίπου 16.7% των μαθητών έχουν νιώσει ότι απειλούνται κατά τη διάρκεια που επικοινωνούν μέσω διαδικτύου με άτομα του αντίθετου φύλου ή με άτομα μεγαλύτερα. Τέλος μόνο το 13.7% ανέφερε ότι δεν έχει ποτέ εμπλακεί σε ανασφαλείς συμπεριφορές στο διαδίκτυο.

Θεωρώντας τα αποτελέσματα αυτής της έρευνας από την οπτική της εκπαιδευτικής πολιτικής, επισημαίνεται η αναγκαιότητα για νέες κατευθύνσεις στα σχολεία ώστε να υιοθετούν μέτρα ασφαλούς χρήσης του διαδικτύου που θα βασίζονται στην ενεργό εμπλοκή των μαθητών στα δημοτικά σχολεία. Η υπάρχουσα κατάσταση στα δημοτικά σχολεία της Φλάνδρας δείχνει ότι έχει επιτευχθεί ένα γενικό επίπεδο ενημέρωσης αλλά χρειάζονται επιπρόσθετες δράσεις που θα αναπτυχθούν και θα εφαρμοστούν σε αυτά τα σχολεία.

Στην έρευνα των Mitchell και συν. (2001), 19% των νέων υπήρξαν στόχοι ανεπιθύμητου σεξουαλικού περιεχομένου. Σε μεγαλύτερο κίνδυνο βρίσκονται κορίτσια, μεγαλύτερης ηλικίας έφηβοι, νέοι με προβλήματα, νέοι που συμμετέχουν σε συζητήσεις στο διαδίκτυο και αυτοί που επικοινωνούν με ξένους στο διαδίκτυο. Το 25% όσων ενεπλάκησαν σε τέτοιες εμπειρίες ανέφεραν υψηλά επίπεδα υπερέντασης μετά από τέτοια περιστατικά. Ο κίνδυνος υπερέντασης είναι περισσότερο κοινός ανάμεσα σε μικρότερης ηλικίας νέους, σε αυτούς που έλαβαν επιθετικής μορφής σεξουαλικό περιεχόμενο και σε αυτούς που είχαν τέτοια εμπειρία σε υπολογιστή μακριά από το σπίτι τους.

Αυτή η έρευνα παρέχει αρκετά γεγονότα που μπορούν να γίνουν αντικείμενο μελέτης για ειδικούς (π.χ. λειτουργούς δημόσιας υγείας, εκπαιδευτικούς, εργαζόμενους στον τομέα προστασίας του παιδιού) ώστε να προσθέσουν το δελεασμό στο διαδίκτυο (σε θέματα σεξουαλικού περιεχομένου) στον κατάλογο των κινδύνων που διατρέχουν τα παιδιά και για τον οποίο θα πρέπει να είναι ενήμεροι και ικανοί να παρέχουν συμβουλευτική σε οικογένειες.

Η έρευνα της Ybarra (2004) παρουσιάζει την ανασφάλεια που βιώνουν οι νέοι επικεντρώνοντας το ενδιαφέρον στη σύνδεση της διαδικτυακής παρενόχλησης με αυξανόμενη κατάθλιψη. Κάνοντας μια σύγκριση μεταξύ των δύο φύλων η έρευνα δείχνει ότι τα αγόρια επηρεάζονται πολύ περισσότερο από ότι τα κορίτσια από ανασφαλείς εμπειρίες στο διαδίκτυο. Ωστόσο αυτή η έρευνα δεν δίνει έμφαση στη συστηματική ερμηνεία αυτής της διαπίστωσης αναφέροντας ότι μάλλον είναι θέμα ψυχολογικής πρόκλησης που αφόρα τα αγόρια.

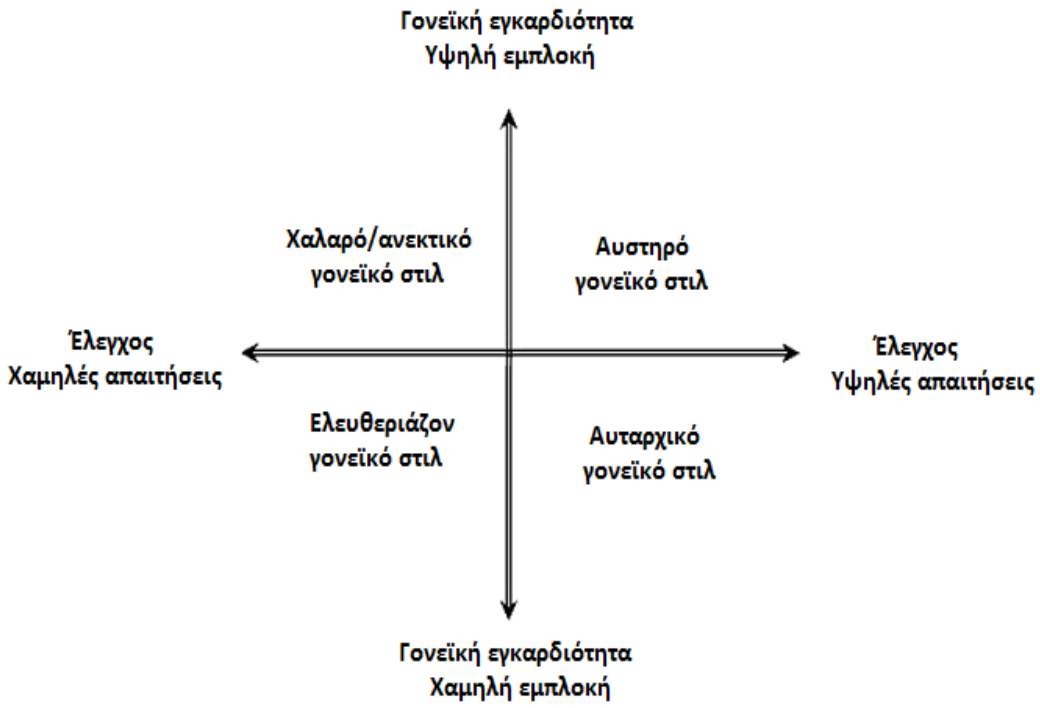
Δεδομένης και της σημαντικής νοσηρότητας που συνδέεται με την συμπτωματολογία που παρουσιάζεται στην παραπάνω έρευνα και η σύνδεσή της με παρενόχληση στο διαδίκτυο, αποκτά ιδιαίτερη αξία για μελλοντική έρευνα που θα εμπλέκει τους τομείς της δημόσιας και νοητικής υγείας.

Τέλος, σχετικά με τη διαχείριση των κινδύνων η έρευνα των Ey & Cupit (2011) έδειξε ότι περισσότερες απαντήσεις παιδιών αφορούν στρατηγικές όπως ενημέρωση ενηλίκων, κλείσιμο της ιστοσελίδα ή και του υπολογιστή και αποφυγή να ξαναμπούν στην ίδια ιστοσελίδα. Υπάρχει ένας μικρός αριθμός που αφορά ακατάλληλες συμπεριφορές ενώ λίγες απαντήσεις προσανατολίζονται προς τις στρατηγικές πρόληψης.

Μολονότι η προστασία των παιδιών στο σπίτι είναι σημαντική, η εκπαίδευση για μάθηση συμπεριφορών προστασίας στο διαδίκτυο είναι απαραίτητη για να εφαρμόζεται όχι μόνο εντός σχολικού περιβάλλοντος. Είναι αναγκαίο τα εκπαιδευτικά ιδρύματα να συνεργάζονται με τους γονείς για να διδάσκουν τα παιδιά στρατηγικές προστασίας στο διαδίκτυο.

### 3.2 Γονείς και ασφάλεια στο διαδίκτυο

Αναφορικά με το πώς αντιμετωπίζουν οι γονείς την ασφάλεια στο διαδίκτυο – σε σχέση με τα παιδιά τους, έχουν πραγματοποιηθεί ποικίλες έρευνες που θεωρούν αυτό το ζήτημα από διάφορες οπτικές. Στην έρευνα των Valcke και συν. (2010) αξιοποιείται η άποψη περί γονεϊκών στιλ για το διαδίκτυο. Η έννοια γονεϊκό στιλ χρησιμοποιείται για να συλλάβει διακυμάνσεις στις προσπάθειες των γονέων να ελέγξουν και να κοινωνικοποιήσουν τα παιδιά τους. Έτσι το γονεϊκό στιλ αναπαριστά το ποσό εμπλοκής και αυστηρότητας ενός γονέα όταν συνδιαλέγεται με το παιδί του. Από αυτές τις απόψεις προκύπτουν δύο κύριοι άξονες (όπως φαίνεται και στο παρακάτω σχήμα):




α) Ο γονεϊκός έλεγχος που αντανακλάται στο επίπεδο καθοδήγησης, παύσης συγκεκριμένων συμπεριφορών που σχετίζονται με το διαδίκτυο και την αποτύπωση κανόνων και β) η γονεϊκή εγκαρδιότητα που χαρακτηρίζεται από επένδυση στην επικοινωνία με τα παιδιά τους και με επίπεδα παρεχόμενης υποστήριξης. Στο πλαίσιο αυτών των δύο αξόνων δημιουργούνται τα ακόλουθα γονεϊκά στιλ:

- Το επιτρεπτικό στιλ αντανακλάται σε γονείς που δε θέτουν σαφή όρια. Αποφεύγουν αντιπαραθέσεις με τα παιδιά τους. Ενδίδουν σε ότι τους ζητούν τα παιδιά. Επενδύουν στη γονεϊκή εγκαρδιότητα, αλλά δύσκολα δίνουν καθοδήγηση
- Το ελευθεριάζον στιλ αντανακλάται σε γονείς με χαμηλό επίπεδο ελέγχου και χαμηλό επίπεδο εμπλοκής. Δεν παρουσιάζουν ούτε υποστηρικτική ούτε περιοριστική στάση στη χρήση του διαδικτύου από τα παιδιά τους
- Το αυστηρό στιλ αντανακλάται σε γονείς που θέτουν σαφείς κανόνες. Δεν περιορίζουν ξεκάθαρα τη συμπεριφορά αλλά περιμένουν από τα παιδιά τους να γίνουν υπεύθυνα και να λειτουργούν με έναν αυτορρυθμιστικό τρόπο. Θέτουν συνήθως πρακτικούς κανόνες π.χ. σε σχέση με το χρόνο χρήσης του διαδικτύου

- Το αυταρχικό στιλ αντανακλάται σε γονείς που ζητούν τυφλή υπακοή και τήρηση των κανόνων χωρίς εξηγήσεις.

Οι τιμές για τις μεταβλητές γονεϊκός έλεγχος και γονεϊκή εγκαρδιότητα κυμαίνονταν από το 1 ως το 5. Συνδυάζοντας και τις δύο διαστάσεις χρησιμοποιώντας την επιλογή 3 ως μέση οι γονείς κατηγοριοποιήθηκαν ανάλογα με το αντίστοιχο γονεϊκό στιλ. Τα αποτελέσματα αυτής της έρευνας δείχνουν ότι η πλειοψηφία των γονέων να τάσσεται κυρίως υπέρ του αυστηρού στιλ ακολουθεί το επιτρεπτικό, το αυταρχικό και το ελευθεριάζον. Επιπρόσθετα προσδιορίζεται και μια ακόμα κατηγορία γονέων που ακολουθούν ένα μικτό στιλ γιατί αντανακλούν επίπεδα γονεϊκής εγκαρδιότητας και ελέγχου γύρω από την τιμή.

Επιπλέον έντονες είναι οι ανησυχίες των γονέων σχετικά με τη χρήση του διαδικτύου από τα παιδιά τους. Σε έρευνα για τη γονεϊκή ενημέρωση και τον έλεγχο στους εφήβους φάνηκε ότι οι γονείς πιστεύουν ότι τα παιδιά τους επισκέπτονται ακατάλληλες ιστοσελίδες ή έχουν ριψοκίνδυνη συμπεριφορά, διαπιστώνοντας ότι οι μητέρες έχουν μεγαλύτερη ενημέρωση για την προβληματική χρήση του διαδικτύου από τα παιδιά τους (Liau et al, 2008). Αυτή η διαπίστωση, δείχνει ότι τα παιδιά είναι πιο πιθανό να αποκαλύπτουν στις μητέρες τους ότι αντιμετώπισαν ανασφαλείς-προβληματικές καταστάσεις όταν χρησιμοποιούν το διαδίκτυο, υπονοώντας ότι νιώθουν κάπως άβολα να ενημερώσουν τον πατέρα τους.

Αυτή η έρευνα έχει σημαντική συμβολή στη σύγκριση δυάδων παιδιών και των γονιών τους σχετικά με την απόκτηση καλύτερης κατανόησης του χάσματος γενεών σχετικά με το διαδίκτυο, αξιοποιώντας μια διεθνή έρευνα που πραγματοποιήθηκε σε πέντε ευρωπαϊκές χώρες. Ασφαλώς αυτή η προσπάθεια θα μπορούσε να ενισχυθεί αν υπήρχε μια ποιοτική συνιστώσα που να εξετάζει στενότερα τις αντιλήψεις των εφήβων και των γονέων για τη χρήση του διαδικτύου. Προτείνεται η μελλοντική έρευνα να περιλαμβάνει συνεντεύξεις και παρατηρήσεις για να αποσαφηνίσει την ασυμφωνία ανάμεσα στις αναφορές παιδιών και γονέων για τη χρήση του διαδικτύου στο σπίτι.

Σε έρευνα που διεξήχθη σχετικά με την επίδραση που έχει η διαμεσολάβηση των γονέων (Youn, 2008) φαίνεται ότι αναλόγως με το πλαίσιο οικογενειακής επικοινωνίας παρατηρείται επίδραση διαφορετικής μορφής ως προς τη χρήση του διαδικτύου. Σε περίπτωση που η οικογενειακή επικοινωνία περιστρέφεται γύρω από έννοιες βοηθά τους νέους να εμπλακούν σε διαμεσολάβηση μέσω συζήτησης που επηρεάζει όσα αφορούν την ιδιωτική ζωή. Από την άλλη

σε περίπτωση που οικογενειακή επικοινωνία αφορά κοινωνικές δεξιότητες/συμπεριφορές αυτό έχει ως αποτέλεσμα τη διαμόρφωση κανόνων και την πλοήγηση στο διαδίκτυο με τους γονείς.

Το γεγονός ότι η έρευνα στους νέους και σε ζητήματα προστασίας προσωπικών δεδομένων πρόσφατα άρχισε να αναδεικνύεται έχει ως αποτέλεσμα να μην έχει δημιουργηθεί μια τυπική κλίμακα σχετικά και με τη διαμεσολάβηση των γονιών σε τέτοια θέματα. Προκύπτει συνεπώς η ανάγκη για μελλοντική έρευνα που να επικεντρώνεται στη δημιουργία μιας κλίμακας που να μετρά κάτι τέτοιο.

### 3.3 Εκπαιδευτικοί και ασφάλεια στο διαδίκτυο

Οι εκπαιδευτικοί έχουν αποτελέσει αντικείμενο μελέτης σχετικά με τις απόψεις, στάσεις, αντιλήψεις τους για την ασφάλεια στο διαδίκτυο. Η έρευνα των Anastasiades & Vitalaki (2011) έδειξε ότι οι εκπαιδευτικοί δεν έχουν τις κατάλληλες δεξιότητες για να προωθήσουν την ενημέρωση για την ασφάλεια στο διαδίκτυο, αφού η πλειοψηφία τους δεν έχει αναπτύξει τις αντίστοιχες δεξιότητες για τη χρήση του διαδικτύου. Συγκεκριμένα, το 54% δήλωσε ότι έχει λίγες κατάλληλες δεξιότητες, ενώ το 23% απάντησε εντελώς αρνητικά. Το 17% δήλωσε ότι έχουν κάποιες δεξιότητες ενώ απόλυτα θετικά απάντησε μόλις το 6%. Από την άλλη, εκείνοι που τείνουν να ενσωματώνουν νέες τεχνολογίες στη διδασκαλία τους είναι πιο αποτελεσματικοί στην προώθηση του ζητήματος της ασφάλειας του διαδικτύου. Οι εκπαιδευτικοί πρωτοβάθμιας εκπαίδευσης που εκτιμούν τις εφαρμογές του διαδικτύου φαίνονται πιο ικανοί να ενσωματώσουν ζητήματα ασφάλειας διαδικτύου στην παιδαγωγική που εφαρμόζουν στη σχολική τάξη.

Ενδιαφέρον εύρημα αυτής της έρευνας που ίσως εξηγεί και κάποια από τα παραπάνω ευρήματα είναι ότι το 39,1% των εκπαιδευτικών δικαιολογεί το γεγονός ότι αποφεύγει να προάγει θέματα ασφάλεια διαδικτύου με τους μαθητές εξαιτίας του φτωχού τεχνολογικού εξοπλισμού των σχολείων, ενώ το 58,7% παραδέχτηκε ότι δε βρίσκει κανένα ενδιαφέρον στο να εντάξει τέτοιου είδους ζητήματα στην ευρύτερη παιδαγωγική που εφαρμόζουν στη σχολική τάξη. Παράλληλα, η συντριπτική πλειοψηφία των εκπαιδευτικών (86%) υποστήριξε ότι είναι ευθύνη του κράτους να δώσει τις κατάλληλες οδηγίες και ενθάρρυνση στους εκπαιδευτικούς για να ενσωματώσουν θέματα ασφάλειας στο διαδίκτυο στην παιδαγωγική τους.

Μια σφαιρική θεώρηση αυτής της έρευνας δείχνει ότι οι εκπαιδευτικοί ενώ αναγνωρίζουν τις δυνατότητες απελευθέρωσης και ενίσχυσης που έχει το διαδίκτυο φαίνονται να αγωνιούν σχετικά με το πώς να διαχειριστούν το δίκτυο και να ελέγξουν την ασφαλή του χρήση από μαθητές δημοτικού.

Στην έρευνα των Δημητρακάκη και συν. (2011), τα αποτελέσματα δείχνουν ότι οι εκπαιδευτικοί έχουν καλή γνώση του Διαδικτύου και των κινδύνων στους οποίους εκτίθενται σι μαθητές κατά την πρόσβασή τους στο Διαδίκτυο, λόγω του ακατάλληλου ή παράνομου περιεχομένου του. Εντούτοις, πρόβλημα εντοπίζεται στο ζήτημα της ανάληψης δράσης των εκπαιδευτικών, σε περίπτωση εντοπισμού παράνομου ή ακατάλληλου περιεχομένου για νέους στο Διαδίκτυο από το 50% του δείγματος, και αυτό αποδίδεται πιθανόν στην έλλειψη μιντιακού γραμματισμού ή και στην απουσία ενημέρωσής τους σε θέματα προστασίας των μαθητών από την «έκθεσή» τους στο Διαδίκτυο.

Αναφορικά με τη λήψη μέτρων και παρεμβάσεων για την προστασία των παιδιών κατά τη χρήση του Διαδικτύου, αν και η πλειονότητα των εκπαιδευτικών, κρίνει το Διαδίκτυο ως επισφαλές και επικίνδυνο, δηλώνουν ότι καταβάλλονται κάποιες ενέργειες προστασίας των μαθητών, οι οποίες δεν επαρκούν. Η έκθεση των παιδιών σε διαδικτυακούς κινδύνους, αποτελεί επιχείρημα, για περιορισμένη και ελεγχόμενη πρόσβαση τους στο Διαδίκτυο.

Στο θέμα της ενημέρωσης από τους εκπαιδευτικούς για την ασφάλεια στο διαδίκτυο στη σχολική τάξη έχει βρεθεί ότι αυτή συνήθως πραγματοποιείται στα πλαίσια του αντικειμένου των Νέων Τεχνολογιών μέσω προγραμμάτων που αξιοποιούν το διαδίκτυο προάγοντας την ασφαλή χρήση του (Wishart, 2004). Ωστόσο, αναδεικνύεται η ανάγκη για πραγματοποίηση παρεμβάσεων για την ασφάλεια στο διαδίκτυο και αξιολόγηση των μαθησιακών αποτελεσμάτων στους μαθητές από τέτοιες παρεμβάσεις ως αντικείμενο μελέτης και έρευνας.

Η έρευνα αυτή συνιστά σε φορείς που ασχολούνται με την ασφάλεια στο διαδίκτυο είτε πρόκειται για κρατικούς οργανισμούς είτε πρόκειται για οργανισμούς που ασχολούνται με τα παιδιά παρέχουν α) συμβουλές που να συμβάλουν στη στήριξη των σχολείων ώστε να βοηθήσουν τα παιδιά μέσα από τη διδακτική διαδικασία να χρησιμοποιούν το διαδίκτυο (π.χ. chat rooms) με ασφάλεια, β) ενημερωμένες υπηρεσίες που θα προειδοποιούν τα σχολεία σχετικά με τις νέες τεχνολογίες και θα δίνουν καθοδήγηση για τη χρήση τους στο σχολείο, γ) διδακτικό

υλικό που μπορεί να χρησιμοποιείται στα σχολεία ώστε οι μαθητές να μπορούν να πλοηγούνται με ασφάλεια στο διαδίκτυο τόσο εντός όσο και εκτός σχολικού περιβάλλοντος.

Η έρευνα των Chou και Peng (2011) έδειξε ότι παρόλο που πολλοί εκπαιδευτικοί στην Ταϊβάν δεν είναι εξοικειωμένοι με το διαδίκτυο και στερούνται του νεανικού ενθουσιασμού για το διαδίκτυο, είναι ενημερωμένοι όχι μόνο για το πόσο δημοφιλές είναι το διαδίκτυο στους μαθητές αλλά και τις μεγάλες επιπτώσεις του στην κοινωνική και ψυχολογική τους ανάπτυξη.

Από το πρόγραμμα που πραγματοποιήθηκε προέκυψε η ανάγκη για προγράμματα επιμόρφωσης των εκπαιδευτικών που μπορεί να αφορά online επιμόρφωση με ενσωμάτωση της διαδικτυακής ασφάλειας στα διάφορα γνωστικά αντικείμενα. Προτείνεται δε ο συνεχής εκσυγχρονισμός της υπάρχουσας γνώσης σχετικά με την ασφάλεια στο διαδίκτυο, ώστε έννοιες όπως ασφάλεια διαδικτύου ("Internet safety") και ηλεκτρονική ασφάλεια ("e-safety") να εξελίσσονται κατά τρόπο ώστε να ταξινομούν εκ νέου και να εισάγουν σχετικές έννοιες.

### 3.4 Αποτίμηση ερευνών

Αποτιμώντας τις έρευνες σχετικά με τις στάσεις, αντιλήψεις, απόψεις, εμπειρίες των εμπλεκομένων σχετικά με την ασφάλεια στο διαδίκτυο, διαπιστώνονται κάποιες κοινές επισημάνσεις (π.χ. το γεγονός ότι τα παιδιά συχνά έχουν ανασφαλείς εμπειρίες στο διαδίκτυο) παρότι οι προσεγγίσεις αλλά και το επίκεντρο ενδιαφέροντος τους μπορεί να ποικίλουν. Επίσης διατυπώνονται προτάσεις που ως επί το πλείστον επισημαίνουν την ανάγκη επικοινωνίας μεταξύ γονέων και παιδιών αλλά και του μετασχηματισμού του σχολείου σε τόπο μάθησης ασφαλούς χρήσης του διαδικτύου. Τέλος το γεγονός ότι το θέμα «ασφάλεια στο διαδίκτυο» είναι ιδιαίτερα επίκαιρο παρουσιάζονται προτάσεις και για μελλοντική έρευνα στο συγκεκριμένο θέμα.

## 4. Κίνδυνοι στο διαδίκτυο

### 4.1 Κίνδυνοι κατά την ηλεκτρονική αλληλογραφία

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες - εγκληματίες.

#### 4.1.1 Κίνδυνοι από κακόβουλα λογισμικά: «malware»

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε λογισμικά που εγκαθίστανται στον υπολογιστή και εκτελούν ανεπιθύμητες εργασίες, συχνά προς όφελος κάποιου τρίτου (ist.mit.edu). Άρα πρόκειται για προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) καθώς και οι δούρειοι ίπποι (Trojan horses).

**α) Ιοί (Viruses)**

Ο συνηθέστερος τρόπος μετάδοσης των ιών πραγματοποιείται μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Ο ιός (Λάζος, 2001) είναι ένα πρόγραμμα Η/Υ που έχει σχεδιαστεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δε έχει την δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από ένα σύστημα σε άλλο , με σκοπό να εκτελέσει την αποστολή του η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων , την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων. Ουσιαστικά είναι ένας βλαβερός εκτελέσιμος κώδικας, ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Έχουν παρασιτική συμπεριφορά, καθώς επιζούν με το να «μολύνουν» άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη συμπεριφορά (ο τρόπος που ζουν και πολλαπλασιάζονται) των οργανικών ιών.

Με πιο απλά λόγια ο ιός επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου.

Ξεκίνησαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. ή εταιριών προϊόντων υψηλής τεχνολογίας όπως XEROX, BELL κλπ.

Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλον τον κόσμο. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό. Σε περίπτωση που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταρρέουν αρχεία εταιρειών, πανεπιστημίων, υπουργείων, ακόμα και κυβερνήσεων.

Σύμφωνα με τον Kyas (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό (Τσουραμάνης, 2005):

**1**. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).

**2**. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).

**3**. Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).

**4**. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων Anti-Virus (Polymorphous Viruses).

**5**. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).

**6**. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).

**7**. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

**β) Δούρειοι ίπποι (Trojan Horses)**

Πρόκειται για ένα είδος προγράμματος, το οποίο δεν αναπαράγεται και δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του. Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σαν να ήταν το αυθεντικό. Όταν ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα χρησιμοποιεί την έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά.

Πιο συγκεκριμένα, ένας δούρειος ίππος αποτελείται από δύο (2) μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον 30 υπολογιστή του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω

των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall) (Λάζος, 2001).

Είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. Έτσι, ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού , αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου.

Στις περισσότερες των περιπτώσεων, ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης (http://www.securitymanager.gr).

**γ) Σκουλήκια (worms)**

Τα σκουλήκια είναι και αυτά προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για τον λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλαδή έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους από τους ιούς αναφέρεται ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους (Λάζος, 2001). Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα των λειτουργικών προγραμμάτων των υπολογιστών. Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.

### 4.1.2 Ανεπιθύμητη αλληλογραφία (spamming- spam mail)

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του

διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα.

Η ιστορία της λέξης «spam» ξεκινά το 1937 όταν ένα καινούριο είδος κρέατος παρουσιάστηκε στην αγορά. Ήταν ένα καινοτομικό προϊόν καθώς προσέφερε «φρέσκο» κρέας χωρίς ανάγκη κατάψυξης σε μια εποχή που το φρέσκο κρέας ήταν δυσεύρετο. Μετά τη λήξη του πολέμου όμως και το πέρασμα των χρόνων με τη βελτίωση του βιοτικού επιπέδου, το SPAM κατέληξε να είναι ένα «αζήτητο» προϊόν (http://www.noc.ntua.gr), όπως και τα μηνύματα ηλεκτρονικού ταχυδρομίου που συχνά λαμβάνουν οι χρήστες.

Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει, αφού είναι «αζήτητο». Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη» καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας (Λάζος, 2001). Έτσι αποτελεί μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming :

- **Απρόκλητο**: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.

- **Εμπορικό:** Το spamming αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.

- **Μαζικό**: Το spamming συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

Για να προστατευτεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το

διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, και αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Κρίνεται σκόπιμο κάθε χρήστης να εγκαταστήσει στον Η/Υ ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων όπως επίσης να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει.

Παρόλο που το spamming ξεκίνησε ως κάτι άκακο και διασκεδαστικό και η ανάγνωση τέτοιων μηνυμάτων μπορούσε να θεωρηθεί ως ευχάριστο διάλειμμα από τη δουλειά, τελικά κατέληξε να είναι μαζί με τους ιούς (worms & viruses) ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Η αυξανόμενη ποσότητα spam έχει όλο και μεγαλύτερο αντίκτυπο σε χρόνο και χρήμα του τελικού χρήστη καθώς αυτός λαμβάνει περισσότερο όγκο δεδομένων από ότι χρειάζεται και θέλει. Παράλληλα αυξάνει την χρησιμοποίηση δικτυακών πόρων για τη διακίνηση ανάμεσα στους παρόχους Internet και επιβαρύνει τη διαχείρισή των ηλεκτρονικών μηνυμάτων στους κεντρικούς εξυπηρετητές καταναλώνοντας υπολογιστικούς και αποθηκευτικούς πόρους. Η ποσότητα των μηνυμάτων spam που λαμβάνει ο μέσος χρήστης αυξάνεται με όλο και μεγαλύτερο ρυθμό τα τελευταία χρόνια.

### 4.1.3 Ηλεκτρονικές απάτες και προσωπικά δεδομένα

**α) Μηνύματα απατηλού περιεχομένου (hoaxes)**

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου και χωρίζονται στις εξής κατηγορίες: (www2.e-yliko.gr)

- **Προειδοποιητικά**: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα.
- **Συμπαράστασης**: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.

- **Εκφοβισμού**: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» («send this to everyone you know»). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.

Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

**β) Ηλεκτρονικό ψάρεμα (phishing)**

Το phishing (αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών από απατεώνες που προσπαθούν να αποσπάσουν προσωπικά-οικονομικά στοιχεία από τα θύματά τους, όπως τα στοιχεία της πιστωτικής κάρτας τους ή του τραπεζικού τους λογαριασμού. Τα υποψήφια θύματα λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν να επιβεβαιώσουν τα προσωπικά τους στοιχεία (π.χ. όνομα χρήστη, αριθμοί καρτών και λογαριασμών, κωδικοί πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν μία συναλλαγή.

Η πλειοψηφία των phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα όπως: τεχνικά προβλήματα σε υπολογιστές της τράπεζας, σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί ή κάποια «μοναδική ευκαιρία».

Έτσι, ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου είτε χρησιμοποιούνται εντολές javascript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο. Αυτό έχει ως αποτέλεσμα το θύμα να αποστέλλει τα προσωπικά στοιχεία που έχουν ζητηθεί κατευθείαν στους απατεώνες, οι οποίοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών-θυμάτων τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

Παρόλο που οι περισσότεροι browsers έχουν ήδη αναπτύξει τεχνολογία anti-phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία ή την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα. Γενικότερα, θα πρέπει να γνωρίζουμε ότι οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους.

**γ) Απάτη με τη Νιγηριανή Επιστολή**

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη (Τσουραμάνης Χρ., 2005). Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο

του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας, διαθέτοντας το λογαριασμό τραπέζης του. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό.

Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής.

Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

**δ) Ισπανικό Λόττο**

«Ισπανικό Λόττο» ονομάζεται η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου (www.astynomia.gr).

Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση. Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

### 4.2 Ασφάλεια κατά την άμεση συνομιλία (chat rooms)

Εκατομμύρια άνθρωποι χρησιμοποιούν καθημερινά το Διαδίκτυο για να δημιουργήσουν και να διατηρήσουν διαπροσωπικές σχέσεις, χρησιμοποιώντας τα δωμάτια συνομιλίας (chat rooms). Τα chat rooms είναι από τα πιο γρήγορα αναπτυσσόμενα «κομμάτια» του internet, ως αυτόνομες υπηρεσίες ή συνδεδεμένα με κάποιο website γνωριμιών. Πρόκειται για ένα χώρο που επιτρέπει στους χρήστες του internet να συνομιλούν μεταξύ τους είτε με γραπτό κείμενο σε πραγματικό χρόνο είτε με video και ήχο, αν διαθέτουν τον κατάλληλο εξοπλισμό (κάμερα και μικρόφωνο).

Οι συνομιλίες μπορούν να είναι είτε δημόσιες είτε ιδιωτικές. Σε κάθε περίπτωση τα chat rooms είναι ιδιαίτερα δημοφιλή και αυτή η δημοτικότητα τους όλο και αυξάνει καθώς η ανάγκη για επικοινωνία κάνει τους χρήστες του διαδικτύου να τα θεωρούν ένα πολύ χρήσιμο εργαλείο.

Σύμφωνα με έρευνα της M.E.Y (μονάδα εφηβικής υγείας) το 2007,σε δείγμα 897 παιδιών(430 αγόρια, 467 κορίτσια) στην Ελλάδα ,το 26% ανέφεραν καθημερινή χρήση του διαδικτύου και το 8% χρήση >20 ώρες εβδομαδιαίως. Ως δεύτερος πιο συχνός λόγος χρήσης του διαδικτύου- μετά τα ψηφιακά παιχνίδια- εμφανίζονταν η χρήση chat.

Σε αντίστοιχη έρευνα του JAMA (Journal of the American Medical Association) το 2008 μέσω τηλεφωνικών συνεντεύξεων σε 1501 νέους φαίνεται ξεκάθαρα πως ένα μεγάλο ποσοστό του δείγματος (838 παιδιά) επισκέπτεται τα Chat rooms και συνομιλεί με αγνώστους.

Οι συνομιλίες αυτές ενέχουν κυρίως 2 κατηγορίες κινδύνου :

- Την αποπλάνηση ανηλίκου (grooming)

- Την ηλεκτρονική παρενόχληση - εκφοβισμό (Cyberbulling)

### 4.2.1 Αποπλάνηση ανηλίκου (grooming)

Η ευρεία χρήση του Διαδικτύου στην εκπαιδευτική και κοινωνική ζωή των νέων ανθρώπων είναι μια σχετικά νέα εκπαιδευτική τάση. Κατά συνέπεια, μόνο την τελευταία δεκαετία η επιστημονική κοινότητα προσπάθησε να κατανοήσει και να αντιμετωπίσει την αποπλάνηση ανήλικων μέσα από το διαδίκτυο (grooming). Ωστόσο, είναι δύσκολο να αναπτύξει μια ισχυρή βάση των στοιχείων της, σε αυτά τα λίγα χρόνια, και αυτό εξηγείται λόγω της έλλειψης βιβλιογραφίας σχετικά με τα κίνητρα, τις στάσεις, τις συμπεριφορές και τις εμπειρίες των online groomers. (European Online Grooming Project et al., 2012)

***Παράγοντες που συντελούν στην εύκολη αποπλάνηση***

***Α)ΣΤΟ ΙΔΙΟ ΤΟ ΠΑΙΔΙ***

***Το φύλο του παιδιού***

Όσον αφορά τη σεξουαλική κακοποίηση των παιδιών offline, η έρευνα δείχνει ότι τα κορίτσια είναι πιο πιθανά θύματα από ό, τι τα αγόρια (Finkelhor, Ormrod, Turner, & Hamby, 2005; Finkelhor, Turner, Ormrod, & Hamby, 2009).Σε μελέτες έχει επίσης διαπιστωθεί πως τα κορίτσια διατρέχουν μεγαλύτερο κίνδυνο στοχοποίησης από τα αγόρια. (Baumgartner, Valkenburg, & Peter, 2010; Brå, 2007; Helweg-Larsen,Schütt, & Larsen, 2011;). Ομοίως, οι Finkelhor, Mitchell, και Wolak (2000) διαπίστωσαν ότι τα κορίτσια ήταν σε μεγαλύτερο ποσοστό στόχος για online σεξουαλική παρενόχληση από τα αγόρια ( σχεδόν διπλάσιο ποσοστό:66% γυναίκες και 34% άνδρες). Έρευνα των ίδιων συγγραφέων έδειξε επίσης ότι τα κορίτσια λάμβαναν περισσότερα αιτήματα για σεξουαλικές φωτογραφίες .Ωστόσο, δεν πρέπει να θεωρηθεί πως και τα αγόρια δε διατρέχουν κίνδυνο σεξουαλικής κακοποίησης. Επιπλέον, είναι πιθανό ότι η σεξουαλική κακοποίηση των αγοριών online συχνά δεν καταγγέλλεται λόγω του αρνητικού στίγματος μιας τέτοιας αναφοράς (O'Leary & Barber, 2008).

***Η ηλικία του παιδιού***

Δεν έχει καθοριστεί επακριβώς από έρευνες ποιες ηλικιακές ομάδες πλήττονται περισσότερο από το την αποπλάνηση μέσω διαδικτύου. Κάποιες μελέτες δείχνουν πως το μεγαλύτερο ποσοστό εμφανίζεται στην προ-εφηβεία ενώ άλλες υποστηρίζουν πως το σημείο αιχμής είναι στην εφηβεία. (Children's Bureau and Department of Health and Human Services, 2010; Murthi & Espelage, 2005).Σε κάθε περίπτωση πάντως οι έρευνες συγκλίνουν στο γεγονός ότι τα παιδιά κοντά στην εφηβεία, έχουν περισσότερες πιθανότητες να πέσουν θύματα αποπλάνησης από τα παιδιά παιδικής ηλικίας. (Baumgartner et al., 2010; Child Exploitation and Online Protection Centre, 2008) Οι πιθανότεροι λόγοι είναι αφενός το γεγονός ότι η χρήση chat γίνεται κυρίως από παιδιά μεγαλύτερης ηλικίας και αφετέρου η έμφυτη τάση των εφήβων να ανακαλύψουν την σεξουαλική τους ταυτότητα( πειραματισμός περιέργεια αποδοχή κτλ) (Dombrowski et al, 2004).

Συμπερασματικά, οι έφηβοι λόγω της απειρίας, της παρορμητικότητας και της επικινδυνότητας σε συνδυασμό με το διαδικτυακό περιβάλλον, και την τάση τους να εξερευνήσουν την σεξουαλική τους ταυτότητα είναι πιθανό να είναι ιδιαίτερα ευάλωτη ομάδα στην αποπλάνηση μέσω διαδικτύου (Wolak et al., 2008).

***Χαρακτηριστικά προσωπικότητας χρήστη διαδικτύου***

Η χαμηλή αυτοεκτίμηση, η ευαισθησία στην πειθώ και η ανωριμότητα είναι όλα τα χαρακτηριστικά που σχετίζονται με τα θύματα σεξουαλικής κακοποίησης .

Παρόμοιες ευπάθειες έχουν βρεθεί σε έρευνα σχετικά με το grooming .Οι νέοι που διατρέχουν μεγαλύτερο κίνδυνο είναι άτομα με χαμηλή αυτοεκτίμηση, συναισθηματικές και ψυχολογικές διαταραχές (European Online Grooming Project et al., 2012, Soo & Bodanovskaya, 2012) Τα προβλήματα ψυχικής υγείας (όπως η κατάθλιψη) και η παραβατική συμπεριφορά μπορεί να κάνει ένα νεαρό άτομο πιο ευάλωτο σε αποπλάνηση.

Επιπλέον από έρευνες που έχουν γίνει σε ενήλικες που είχαν υποστεί κάποιο είδος κακοποίησης ως παιδιά, διαπιστώθηκε πως υπάρχει μια σύνδεση μεταξύ του τραύματος στην παιδική ηλικία και τα χαρακτηριστικά της προσωπικότητας. (Allen & Lauterbach, 2007, Bradley et al., 2005 ).

Άλλες έρευνες φανερώνουν ότι οι δράστες συχνά αξιολογούν τα θύματα τους με βάση τα χαρακτηριστικά εκείνα της προσωπικότητάς τους, που τα κάνουν ευάλωτα στην αποπλάνηση.

Ειδικότερα, τα χαρακτηριστικά της προσωπικότητας όπως χαμηλή αυτοπεποίθηση και αυτοεκτίμηση αφήνουν τους νέους εκτεθειμένους στους θύτες (Olson et al., 2007).

Ωστόσο, οι περισσότερες έρευνες στηρίζονται κυρίως σε χαρακτηριστικά κακοποίησης και αποπλάνησης εκτός διαδικτύου, καθώς η έρευνα στην online αποπλάνηση και κακοποίηση βρίσκεται ακόμα σε πρώιμο στάδιο.

***Παιδιά με ειδικές ανάγκες /Αναπηρία/μαθησιακές δυσκολίες***

Υποστηρίζεται γενικά από έρευνες ότι υπάρχει άμεση συσχέτιση μεταξύ αναπηρίας και ευπάθειας στην παιδική σεξουαλική κακοποίηση εκτός διαδικτύου (Yancey & Hansen, 2010). Τα παιδιά με αναπηρία χρησιμοποιούν λιγότερο το Διαδίκτυο συγκριτικά με τους συνομηλίκους τους χωρίς αναπηρία (Livingstone & Bober, 2005), καθώς το Διαδίκτυο μπορεί να τους προσφέρει την παρηγοριά και την υποστήριξη που τους λείπει από την καθημερινή τους ζωή. Ωστόσο, δεν είναι λίγες οι φορές που στα δωμάτια επικοινωνίας (chat rooms) άτομα με αναπηρία βιώνουν περαιτέρω περιθωριοποίηση (Söderström, 2009). Όπως και τα υπόλοιπα παιδιά, είναι εκτεθειμένα στον κίνδυνο αλλά είναι λιγότερο σε θέση να τον αναγνωρίσουν ή να τον αντιμετωπίσουν.

Σε μια πανευρωπαϊκή μελέτη στην οποία συμμετείχαν 25 χώρες (ανάμεσα τους και η Ελλάδα) με 25.142 παιδιά 11-16 ετών, Livingstone et al. (2011) διαπιστώθηκε πως οι νέοι με ειδικές ανάγκες βρίσκονται σε υψηλότερο ποσοστό διαδικτυακού κινδύνου για grooming, κυρίως μέσω των επαφών τους στα Chat rooms από ότι στον πραγματικό κόσμο .

Τα παιδιά με μαθησιακές δυσκολίες μπορεί να γίνουν επίσης ευκολότερη λεία για online groomers και αυτό γιατί έχουν την τάση να εμπιστεύονται ενήλικες περισσότερο (Sorenson & Bodanovskaya, 2012)

***Β)ΣΤΗΝ ΟΙΚΟΓΕΝΕΙΑ***

***Οικογενειακό περιβάλλον***

Έρευνες έδειξαν διάφορους παράγοντες εντός της οικογένειας που αυξάνουν σημαντικά τους κινδύνους για αποπλάνηση και παρενόχληση των παιδιών εκτός διαζυγίου. Μονογονεϊκές οικογένειες κακή σχέση μεταξύ των μελών της οικογένειας και έλλειψη συνοχής κ.α .

Οι δράστες από ολόκληρη την Ευρώπη εντοπίζουν λογαριασμούς υποψήφιων θυμάτων με οικογενειακά προβλήματα. Αναγνωρίζουν ότι το νεαρό άτομο μπορεί να ζητήσει την προσοχή από έναν ενήλικα και το εκμεταλλεύονται. (European Online Grooming Project etal., 2012)

Η γονική κατάχρηση ουσιών ,η παραβατική συμπεριφορά τους και ο αλκοολισμός, έχει βρεθεί επίσης να είναι παράγοντες που αυξάνουν σημαντικά τον κινδύνο για την αποπλάνηση των παιδιών μέσα στο διαδίκτυο (Berger, Slack, Waldfogel, & Bruch, 2010 , Suseg et al., 2008 ). Μια πιθανή εξήγηση που δίνουν οι ερευνητές είναι ότι στις παραπάνω υποθέσεις η έκταση του ελέγχου του γονέα μπορεί που μπορεί να ασκήσει πάνω στο παιδί του, σχετικά με τη χρήση του διαδικτύου είναι αρκετά μειωμένη. (Livingstone et al., 2005).

***Κοινωνικοοικονομική κατάσταση***

Ενώ η φτώχεια δεν οδηγεί αναπόφευκτα σε κακομεταχείριση, είναι γενικά αποδεκτό ότι παιδιά από τις χαμηλές κοινωνικοοικονομικές ομάδες είναι πιο επιρρεπείς σε κοινωνικά προβλήματα όλων των ειδών, συμπεριλαμβανομένης και της σεξουαλικής κακοποίησης (Bagley & Mallick, 2000).

Ωστόσο, από έρευνες φαίνεται να υπάρχει ελάχιστη σχέση μεταξύ της σεξουαλικής κακοποίησης των παιδιών και της κοινωνικοοικονομικής τους κατάστασης. Σε ό,τι αφορά την αποπλάνηση μέσω διαδικτύου φαίνεται πως το ποσοστό αυτό είναι ακόμα μικρότερο καθώς τα οικονομικά προβλήματα δυσχεραίνουν την εύκολη πρόσβαση στο διαδίκτυο. Έτσι παιδιά με υψηλό κοινωνικοοικονομικό υπόβαθρο και υψηλό εισόδημα είναι πιο πιθανά «θύματα» του grooming καθώς έχουν ευκολότερη πρόσβαση στο διαδίκτυο (από υπολογιστή, φορητές συσκευές, κτλ) (Livingstone, Bober, & Helsper,2005, Soo & Bodanovskaya, 2012, Spielhofer, 2010).

Μελέτη, σε όλη την Ευρώπη, (Livingstone et al. 2011a, 2011b)ανέφερε ότι οι νέοι της υψηλότερης κοινωνικοοικονομικής κατάστασης έχουν πιο ευρύ φάσμα επαφών στις διαδικτυακές τους συνομιλίες, συμπεριλαμβανομένων άγνωστων ατόμων που πολλές φορές αποδείχθηκαν παιδεραστές .

Εντούτοις στα αποτελέσματα συνεκτιμήθηκε το μορφωτικό επίπεδο των γονιών που αποτέλεσε σημαντικό ανασταλτικό παράγοντα στα παιδιά- υποψήφια θύματα ανεξαρτήτως οικονομικής κατάστασης.

Έτσι στις μέχρι τώρα έρευνες δεν έχει αποδειχθεί αν τα στερημένα από οικονομικής άποψης παιδιά είναι πιο ευάλωτα ως θύματα του grooming.

### *Γ) ΣΤΟ ΚΟΙΝΩΝΙΚΟ ΠΕΡΙΒΑΛΛΟΝ*

#### *Φίλοι*

Τα παιδιά με λίγους ή καθόλου φίλους, αισθάνονται αποξενωμένα και είναι πιο πιθανό να είναι ευάλωτα στην αποπλάνηση μέσω διαδικτύου σε απευθείας συνομιλίες (Stanley, 2001). Η συναισθηματική μοναξιά, είναι επίσης ένα βασικός κίνδυνος αποπλάνησης (European Online Grooming Project et al.,2010). Τα μοναχικά και ντροπαλά παιδιά μπορεί να χρησιμοποιήσουν τα δωμάτια συνομιλίας για να επικοινωνούν με τους άλλους αντισταθμίζοντας τις κοινωνικές δυσκολίες της ζωής τους εκτός διαδικτύου. (Peter, Valkenburg, & Schouten, 2005). Αξιοσημείωτο, σημείο ερευνών επίσης δείχνει ότι η χρήση κυρίως των δωματίων συνομιλίας (περισσότερο από ό, τι άλλες ηλεκτρονικές επικοινωνίες), θέτει παιδιά και εφήβους σε κίνδυνο σεξουαλικής προσέγγισης (Wolak et al., 2008).

Από την άλλη πλευρά ,η έρευνα έδειξε ότι παιδιά με υψηλή ικανοποίηση από την κοινωνική τους ζωή και τη σχέση τους με τους φίλους τους αλλά και των δασκάλων τους (Elmore & Huebner,2010, Suldo & Huebner, 2006)είχαν όχι μόνο μικρότερο ποσοστό θυματοποίησης αλλά προέβλεψαν πολλές φορές τον κίνδυνο.

#### *Σχολείο*

Το σχολείο είναι συνήθως το πρώτο σημαντικό περιβάλλον στο οποίο εκτίθενται τα παιδιά και περιβάλλονται από άγνωστούς συνομηλίκους και ενήλικες (Cicchetti & Toth, 2005). Αρκετές μελέτες έχουν τεκμηριώσει πως η εκτός διαδικτύου αποπλάνησης παιδιού συνδέεται με την ακαδημαϊκή επίδοση (Boden et al, 2007, Daignault & Hébert, 2009, Veltman & Browne, 2001). Ωστόσο, οι επιπτώσεις της αποπλάνησης και κακοποίησης των παιδιών με κακή ακαδημαϊκή επίδοση θα πρέπει να εξεταστούν, λαμβάνοντας υπόψη παράγοντες όπως το ευρύτερο ψυχοκοινωνικό πλαίσιο του παιδιού, την κατάχρηση διαδικτύου, κοινωνικοοικονομικούς παράγοντες κτλ.

Σε έρευνα του 2005 φάνηκε πως παιδιά που είχαν κακοποιηθεί σεξουαλικά ήταν εξίσου πιθανό να πετύχουν ακαδημαϊκά, όπως εκείνοι οι οποίοι δεν είχαν κακοποιηθεί (Πόρπη, Lancaster,

Powell, & Higgins, 2005). Διαπιστώθηκε βέβαια πως η ευφυΐα να είναι ένας προστατευτικός παράγοντας για σεξουαλικά κακοποιημένους νέους (Πόρπη et al., 2005).

Ο Brå (2007) ανέφερε ότι οι νέοι οι οποίοι ήταν δυσαρεστημένοι με το σχολείο (συμπεριλαμβανομένων των εμπειριών του εκφοβισμού) είχαν περισσότερες πιθανότητες να προσεγγιστούν σεξουαλικά από έναν ενήλικο, τόσο online όσο και offline. Επιπλέον, υπάρχουν αποδείξεις ότι παιδιά και έφηβοι με χαμηλό επίπεδο εκπαίδευσης διατρέχουν μεγαλύτερο κίνδυνο σεξουαλικής παρενόχλησης από ό, τι αυτοί με ανώτερη εκπαίδευση (De Graaf & Vanwesenbeeck, 2006).

Ωστόσο, δεν κατέστη δυνατό να διαπιστωθεί κατά πόσο βιώνουν την κακοποίηση λόγω κακής σχολικής επίδοσης ή έχουν κακή σχολική επίδοση λόγω της κακοποίησης και αυτό γιατί πολλοί άλλοι παράγοντες μπορεί συμβάλλουν στην σχέση μεταξύ των δύο.

Τελευταίες υπάρχουσες έρευνες δείχνουν ότι η δυσαρέσκεια και οι δυσκολίες στο σχολείο μπορεί να είναι συμβάλλουν και να αυξήσουν το ποσοστό κινδύνου σεξουαλική προσέγγισης , τόσο εκτός διαδικτύου όσο και μέσα στο διαδίκτυο στα δωμάτια συνομιλίας.

***Γεωγραφικό περιβάλλον***

Σε μια ανασκόπηση 25 μελετών όπου εξετάστηκαν τα offline κρούσματα παιδικής κακοποίησης, οι ερευνητές ( Coulton, Crampton, Irwin, Spilsbury και Korbin 2009) βρήκαν ότι υπάρχει ισχυρή ένδειξη σχέσης μεταξύ του περιβάλλοντος μέσα στο οποίο ζει το παιδί( αστικό, ημιαστικό, αγροτικό) και της κακοποίησης. Τα παιδιά που ζουν σε περιβάλλοντα που χαρακτηρίζονται από τη φτώχεια, διατρέχουν υψηλότερο κίνδυνο offline κακοποίησης (Coulton, Korbin, & Su,1999). Έρευνες όμως εξετάζουν και τα πιθανά τρωτά σημεία του περιβάλλοντος διαβίωσης σε σχέση την online αποπλάνηση. Ο Ofcom (2008) ανέφερε ότι η πρόσβαση στο διαδίκτυο είναι υψηλότερη στα παιδιά αστικών περιοχών σε σχέση με αυτή των παιδιών από αγροτικές περιοχές. Ωστόσο, άλλες μελέτες δεν βρήκαν στοιχεία για τη διαφορά χρήσης στο διαδίκτυο με βάση τη γεωγραφική θέση (Spielhofer, 2010).

Αξίζει επίσης να σημειωθεί πως προβλήματα δικτύου κάλυψης σε κινητά τηλέφωνα σύμφωνα με τους Peter, Valkenburg, και Schouten (2006) αποτέλεσαν έναν από τους λόγους που οι νέοι επέλεξαν να μιλούν με αγνώστους στο Διαδίκτυο, ως αποτέλεσμα πλήξης. Ως εκ τούτου, από πολλές έρευνες έχει προκύψει ως συμπέρασμα πως λόγω του γεωγραφικού αποκλεισμού είναι

πιο πιθανό τα παιδιά ημιαστικών και αγροτικών περιοχών να ανταποκριθούν σε groomers στα chat rooms .

***Εθνικότητα***

Η σεξουαλική κακοποίηση παιδιών είναι ένα παγκόσμιο πρόβλημα (Bourke & Hernandez, 2009). Οι έρευνες που προσεγγίζουν τη σχέση ανάμεσα στη σεξουαλική κακοποίηση και την εθνικότητα είναι ελάχιστες και αφορούν κυρίως την εκτός διαδικτύου κακοποίηση (McCloskey & Bailey, 2000). Οι Pereda κ.α. (2009) διαπίστωσαν πως ενώ η σεξουαλική κακοποίηση παιδιών ήταν πολύ υψηλή στη Νότια Αφρική, αυτό μπορεί να μην είναι αντιπροσωπευτικό. Η διαφορετική κουλτούρα, οι επιπτώσεις που θα μπορούσε να έχει μια καταγγελία και πολλοί άλλοι παράγοντες συμβάλουν στη μεταβολή και αναγνώριση του τι θεωρείται αποπλάνηση. Λαμβάνοντας υπόψη την πιθανή προκατάληψη μεταξύ των χωρών, είναι δύσκολο να εξαχθούν συμπεράσματα σχετικά με την σεξουαλικής κακοποίησης παιδιών (είτε online είτε offline) μεταξύ διαφορετικών εθνικοτήτων.

Η έρευνα γύρω από την εθνικότητα των θυμάτων τόσο σε offline σεξουαλική κακοποίηση παιδιών όσο και online σπανίζει.

### 4.2.2 Cyber bulling- Εκφοβισμός στον κυβερνοχώρο

Είναι γεγονός πως η σχολική βία υπήρχε πάντα στο σχολείο. Τον 21ο όμως αιώνα, η σχολική βία αποκτά μια νέα μορφή. Οι νέες τεχνολογίες έχουν καταστήσει ευκολότερη την απόκτηση πρόσβασης των θυτών στα θύματά τους. Αυτή η μορφή του εκφοβισμού στον κυβερνοχώρο έχει γίνει γνωστή ως cyber-bullying.( Susan Keith & Michelle E. Martin,2005)

Ο εκφοβισμός στον κυβερνοχώρο περιλαμβάνει τη χρήση των πληροφοριών και τις τεχνολογίες επικοινωνίας. Η εσκεμμένη, επαναλαμβανόμενη, εχθρική συμπεριφορά από ένα άτομο ή ομάδα ατόμων, που προορίζεται να προκαλέσει εκφοβισμό ή και να βλάψει άλλους μέσα στο διαδίκτυο ονομάζεται cyberbulling (Belsey, 2004).

Τα παιδιά χρησιμοποιούν το διαδίκτυο καθημερινά και επικοινωνούν με τρόπους συχνά άγνωστους στους ενήλικες και χωρίς εποπτεία. Σε έρευνα του National i-Safe Survey στις ΗΠΑ, το 2004 διαπιστώθηκε πως:

• 57% των μαθητών δήλωσε ότι είχε πει προσβλητικά πράγματα για συμμαθητές του, όντας σε κατάσταση θυμού στο διαδίκτυο (με το 13% να λέει αυτό συμβαίνει «αρκετά συχνά»)

• 53% των μαθητών παραδέχτηκε συνειδητά και χωρίς να βρίσκεται εν βρασμό ψυχής, λέει είναι επιζήμια πράγματα και 7% παραδέχτηκε ότι το κάνει «αρκετά συχνά»

• 35% των μαθητών έχουν απειληθεί σε απευθείας σύνδεση με ένα 5% να αναφέρει ότι αυτό συμβαίνει «αρκετά συχνά».

**1. Προφίλ θυμάτων- θυτών**

Η χαμηλή αυτοεκτίμηση, η ευαισθησία, η ανωριμότητα, η έλλειψη φίλων είναι μερικά από τα χαρακτηριστικά που σχετίζονται με το προφίλ των θυμάτων/θυτών βίας στο διαδίκτυο. Σε έρευνα των Soo & Bodanovskaya, το 2012 βρέθηκε πως τα παιδιά που διατρέχουν μεγαλύτερο κίνδυνο να γίνουν θύματα είναι άτομα με χαμηλή αυτοεκτίμηση, συναισθηματικές και ψυχολογικές διαταραχές. Επιπλέον από άλλες έρευνες φαίνεται πως στην κατηγορία των θυμάτων ανήκουν τα «κλειστά» παιδιά που δεν μοιράζονται εύκολα τα προβλήματα τους με κάποιον ενήλικα. Αυτά κυρίως γίνονται στόχος μετά από αναζήτηση του προφίλ τους από τους δράστες στο διαδίκτυο. Όπως προαναφέρθηκε, οι δράστες συχνά αξιολογούν τα θύματα τους με βάση τα χαρακτηριστικά εκείνα της προσωπικότητας τους, που το κάνουν ευάλωτο όπως χαμηλή αυτοπεποίθηση και αυτοεκτίμηση αφήνουν τους νέους εκτεθειμένους στους θύτες (Olson et al., 2007).

Στο σημείο αυτό θα πρέπει να τονιστεί πως μέσα από την ανασκόπηση της βιβλιογραφίας γίνεται φανερή η αντίθεση της βίας στον κυβερνοχώρο με την παραδοσιακή βία σε ό,τι αφορά το προφίλ του θύτη/ θύματος. Στον κυβερνοχώρο είναι όλοι εν δυνάμει θύτες και θύματα καθώς πίσω από την ανωνυμία που προσφέρει το διαδίκτυο ξεδιπλώνονται πτυχές του εαυτού μας που στην πραγματική ζωή δεν γίνονται φανερές. Έτσι συναντούμε συχνά θύτες αδύναμα παιδιά που μέσα από την ανωνυμία του διαδικτύου ενεργούν όπως δεν μπορούν να ενεργήσουν στην κανονική ζωή. Θύματα επίσης μπορεί να είναι παιδιά με ισχυρή προσωπικότητα που είναι ακάλυπτα σε παρόμοιους κινδύνους και δεν γνωρίζουν πώς να το χειριστούν.

## 2. Φύλο και παρενόχληση στον κυβερνοχώρο

Σε έρευνες που έχουν γίνει τα τελευταία χρόνια, δεν φαίνεται να υπάρχουν σημαντικές διαφορές μεταξύ αγοριών και κοριτσιών που έπεσαν θύματα cyber bulling. Εντούτοις, ελαφρύ προβάδισμα φαίνεται να έχουν τα αγόρια, τουλάχιστον προεφηβική ηλικία (Hinduja & Patchin, 2010).Οι έρευνες όμως φαίνεται να αντιστρέφονται στην εφηβική ηλικία. Στην παρενόχληση στον κυβερνοχώρο, οι έφηβες φαίνεται πως είχαν περισσότερες πιθανότητες από τους άνδρες εφήβους να πέσουν θύματα παρενόχλήσης. Ενδιαφέρον εντούτοις αποτελεί το γεγονός ότι οι γυναίκες πολλές φορές στην εφηβική ηλικία «αναλαμβάνουν» το ρόλο του θύτη. Αυτό το εύρημα είναι ενδιαφέρον συγκριτικά με το γεγονός ότι στον παραδοσιακό εκφοβισμό, το ρόλο του θύτη αναλαμβάνουν κυρίως οι άντρες .Τα αγόρια συνήθως εμπλέκονται στον παραδοσιακό εκφοβισμό ως πιο δυναμικά (Schwartz, 2000, Solberg et al., 2007).Στον εκφοβισμό όμως του κυβερνοχώρου ,πίσω από την κάλυψη του υπολογιστή τα πράγματα γίνονται πιο εύκολα και τόσο για τους μη «νταήδες» εφήβους όσο και για τις γυναίκες. Μία εξήγηση για τη διαπίστωση αυτή είναι ότι οι γυναίκες τείνουν να χρησιμοποιούν την παρενόχληση στον κυβερνοχώρο, πιο συχνά από τους άνδρες. Η παρενόχληση αυτή θεωρείται έμμεση καθώς μπορεί να προσφέρει μια ευκαιρία στις γυναίκες να συμμετάσχουν σε πιο επιθετικές συμπεριφορές δίνοντας τους επιπλέον τρόπους για να είναι επιθετικές, χωρίς να καταφεύγουν σε σωματική βία (Wolak et al., 2007).

## 3. Η ηλικία και ο εκφοβισμός

Μαθητές στα δημοτικά σχολεία είναι σύμφωνα με έρευνες ,τα περισσότερα θύμτα εκφοβισμού από ότι μαθητές στα σχολεία δευτεροβάθμιας εκπαίδευσης (Telljohann, 2003). Φαίνεται πως οι μεγαλύτεροι μαθητές είναι πιο πιθανό να εκφοβίσουν τους μικρότερους. Στο διαδίκτυο αυτό το ποσοστό μεγαλώνει καθώς μεγαλύτεροι μαθητές που στην πραγματική ζωή τους δεν είναι βίαιοι, μέσω της ανωνυμότητας βγάζουν ένα πιο σκληρό εαυτό. Ομοίως, οι Ybarra και Mitchell (2004b) διαπίστωσαν ότι όσο μεγαλύτερο είναι το παιδί τόσο πιο πιθανό είναι να εμπλέκεται σε online βία ως δράστης. Ισχυρίστηκαν ότι αυτές οι διαφορές μεταξύ παραδοσιακής και απευθείας σύνδεση επιθετικότητας μπορεί να οφείλεται σε ορισμένες πτυχές της ηλεκτρονικής παρενόχλησης όπως η δυναμική ενέργεια που μπορεί να διαφέρει στον παραδοσιακό εκφοβισμό. Ενδιαφέρον τέλος. αποτελεί η διαπίστωση των Khoury-Kassabri (2009) πως ενώ ορισμένες

μορφές επιθετικής συμπεριφοράς μειώνονται με την ηλικία (π.χ., σχολικός εκφοβισμός) άλλες μορφές που μπορεί να συμβαίνουν έξω από το σχολείο (π.χ., η παρενόχληση στον κυβερνοχώρο), είναι πιο διαδεδομένες μεταξύ των μεγαλύτερων μαθητών.

**4. Οικογένεια –κοινωνία**

Όπως προαναφέρθηκε στους παράγοντες που ενισχύουν το grooming, η οικογένεια και η κοινωνία παίζουν πολύ σημαντικό ρόλο και στον κίνδυνο του cyber bulling. Η γονική κατάχρηση ουσιών ,η παραβατική συμπεριφορά τους και ο αλκοολισμός, έχουν βρεθεί ως οικογενειακό υπόβαθρο σε παιδιά θύτες (Berger, et al, 2010 , Suseg et al., 2008 ).Η ίδια έρευνα έδειξε πως από οικογένειες με παρόμοια προβλήματα προέρχονται και θύματα. Συνυπολογίζουμε βέβαια πως σε αυτό συμβάλει και η χαμηλή αυτοπεποίθηση που έχουν συνήθως τα παιδιά αυτών των οικογενειών.

Ελάχιστη σχέση φαίνεται να υπάρχει μεταξύ της βίας στο διαδίκτυο και της κοινωνικοοικονομικής κατάστασης των παιδιών (θυτών και θυμάτων). Σε ότι αφορά τους θύτες φαίνεται πως το ποσοστό αυτό είναι ακόμα μικρότερο καθώς τα οικονομικά προβλήματα δυσχεράνουν την εύκολη πρόσβαση στο διαδίκτυο, όπως προαναφέρθηκε. Στα παιδιά θύματα δεν έχουμε κάποια έρευνα που να υποδεικνύει ως υπαίτια την οικογένεια ή το κοινωνικό περιβάλλον.

### 4.3 Ασφάλεια κατά την περιήγηση σε δικτυακούς τόπους

#### 4.3.1 Βίαια παιχνίδια στο διαδίκτυο

Σύμφωνα με έρευνες που έχουν γίνει εκατομμύρια άτομα αφιερώνουν χρόνο, σε καθημερινή βάση σε βίαια ηλεκτρονικά παιχνίδια στο διαδίκτυο. Οι ερευνητές έχουν μελετήσει τις αρνητικές συνέπειες που έχουν αυτά τα παιχνίδια στα άτομα (http://www.appdata.com).

Τα αποτελέσματα αυτών των ερευνών δείχνουν ότι η βία στα ηλεκτρονικά παιχνίδια μπορεί να προκαλέσει αντικοινωνική και πολεμοχαρή συμπεριφορά στην καθημερινότητα των παιδιών. Ακόμη ο εθισμός στα διαδικτυακά παιχνίδια συνοδεύεται, συνήθως, με ακραίες συμπεριφορές,

συναισθήματα ευφορίας, συμπτώματα στέρησης, υποτροπής, επαναφοράς και σύγκρουσης (Charlton & Danforth, 2007). Πρέπει να αναφερθεί πως υψηλά επίπεδα έκθεσης σε βίαια ηλεκτρονικά παιχνίδια μπορεί σχετίζονται έντονα, με αυξανόμενη επιθετική συμπεριφορά στο σχολείο και στον ελεύθερο χρόνο ακόμα και στο παιχνίδι και είναι πιθανό να οδηγήσουν τα άτομα στην εγκληματικότητα. Επιπλέον, μπορούμε να πούμε πως οι παίκτες που παίζουν περισσότερο από 41 ώρες την εβδομάδα, θεωρούνται εθισμένοι και η πολύωρη διαδικτυακή ενασχόληση είναι ιδιαίτερα πιθανό να έχει αρνητική επίδραση πάνω σε πτυχές της ζωής και της προσωπικότητας τους.

### 4.3.2 Ηλεκτρονικός τζόγος

Με τον όρο Ηλεκτρονικός Τζόγος εννοούμε τη δραστηριότητα κατά την οποία δύο ή περισσότερα άτομα συναντώνται διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων.

Υπάρχουν πολλοί λόγοι για τους οποίους οι άνθρωποι παίζουν τυχερά παιχνίδια. Μερικοί από αυτούς είναι πιθανότατα η απόπειρα να ρυθμίσουν τη διάθεσή τους, να ξεφύγουν προφανώς από άλλα προβλήματα. Ακόμη σε πολλές περιπτώσεις η ενασχόληση των ατόμων με τον ηλεκτρονικό τζόγο μπορεί να σχετίζεται και με το οικονομικό κέρδος. Τέλος τα άτομα, κυρίως νεαρής ηλικίας επιθυμούν να αντλήσουν κάποιου είδους ευχαρίστησης από τον τζόγο καθώς πολλές φορές αντιμετωπίζεται σαν ένα είδος διασκέδασης. (Lloyd et al, 2010).

Δυστυχώς οι συνέπειες από μια τέτοια ενασχόληση είναι επικίνδυνες. Καταρχήν μια τέτοια δραστηριότητα περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας. Ακόμη ο ηλεκτρονικός τζόγος μπορεί να οδηγήσει τα άτομα σε εξάρτηση. Από έρευνες που έχουν γίνει σχετικά με αυτό το θέμα έχει βρεθεί ότι η πολύωρη ενασχόληση με τον ηλεκτρονικό τζόγο επηρεάζει σε μεγάλο βαθμό την διάθεση, προκαλεί ψυχολογικές μεταπτώσεις και υπάρχει ο κίνδυνος να οδηγήσει ακόμα και στην κατάθλιψη, πολλές φορές συνδέεται με την κατανάλωση αλκοόλ και ουσιών. Τέλος η εξάρτηση από τον ηλεκτρονικό τζόγο και η πιθανή οικονομική απώλεια μπορεί να οδηγήσει τα άτομα ακόμα και στην πιθανότητα να βλάψουν τον εαυτό τους (Lloyd et al, 2010).

### 4.3.3 Παραπληροφόρηση στο Διαδίκτυο

Η ποσότητα των πληροφοριών που διατίθενται μέσω του Διαδικτύου ολοένα και αυξάνεται. Η παραπληροφόρηση στο Διαδίκτυο είναι δυνατό να συμβεί με την παρουσίαση διάφορων ψευδών ή αναληθών ή τροποποιημένων πληροφοριών σε ιστοσελίδες, με πιθανό σκοπό την παραπλάνησή μας. Παραπληροφόρηση συμβαίνει και όταν οι πληροφορίες είναι ελλιπείς με αποτέλεσμα να οδηγήσουν σε λανθασμένα συμπεράσματα. Ο κίνδυνος είναι σοβαρός ιδιαίτερα για τους μαθητές οι οποίοι αναζητούν πληροφορίες στο διαδίκτυο και είναι δυνατόν να βρούνε πληροφορίες με σοβαρά λάθη, οι οποίες να σχετίζονται ακόμα και με θέματα υγείας.

Δυστυχώς το Διαδίκτυο, σε πολλές περιπτώσεις, δεν διαθέτει ασφαλιστικές δικλίδες για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται, με αποτέλεσμα ο καθένας να μπορεί να δημοσιεύει σχόλια και πληροφορίες. (http://www.pi.ac.cy/InternetSafety)

### 4.3.4 Διαμοιρασμός αρχείων

Η ψηφιοποίηση των πληροφοριών, με τη δικτύωση στο διαδίκτυο, αλλάζει ριζικά το περιβάλλον της παραβίασης πνευματικών δικαιωμάτων. Ένα τέτοιο παράδειγμα είναι ο διαμοιρασμός αρχείων. Διαμοιρασμός αρχείων είναι η δυνατότητα, που προσφέρει το Διαδίκτυο στους χρήστες του, να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται μέσω διαφόρων προγραμμάτων (που διατίθενται στο διαδίκτυο ελεύθερα ή με πληρωμή). (Domona et al, 2004)

Η χρήση των προγραμμάτων διαμοιρασμού αρχείων παραβιάζει τους κανόνες «υγιεινής» του υπολογιστή μας. Αυτό σημαίνει πως μοιραζόμαστε «αρχεία» με χρήστες που δεν τους γνωρίζουμε και επομένως δεν μπορούμε να τους εμπιστευτούμε. Ο κίνδυνος είναι μεγαλύτερος για τους μαθητές επειδή τα περισσότερα από τα προγράμματα διαμοιρασμού αρχείων στο Διαδίκτυο επιτρέπουν την πρόσβαση ανήλικων σε ακατάλληλα βίντεο ή εικόνες.

Τέλος αν, από λάθος στις ρυθμίσεις του προγράμματος διαμοιρασμού αρχείων, γίνει κοινόχρηστος ολόκληρος ο σκληρός δίσκος του τοπικού υπολογιστή, τότε προσωπικά δεδομένα, που πιθανόν έχετε στον υπολογιστή σας όπως αριθμοί πιστωτικών καρτών ή φορολογικά δεδομένα, θα εκτεθούν σε όλους τους χρήστες που χρησιμοποιούν το πρόγραμμα αυτό (http://www2.e-yliko.gr/htmls/safety/sfshare.aspx).

## 5. Πώς μπορώ να αντιμετωπίσω τους κινδύνους στο διαδίκτυο; - Τρόποι παρέμβασης

http://www.madseadog.comillustrationDon%20Quixote%20w-%20Wind%20Mills.jpg

Ύστερα από την παραδοχή όλων αυτών των κινδύνων που διατρέχει κάποιο παιδί ή ένας έφηβος χρησιμοποιώντας το Διαδίκτυο θα πρέπει να εξετάσουμε όλους εκείνους τους τρόπους με τους οποίους θα μπορούσαμε να ελαχιστοποιήσουμε ή να εξαλείψουμε αυτούς τους κινδύνους. Οι τρόποι παρέμβασης κατηγοριοποιούνται ως εξής:

### 5.1 Τεχνικοί τρόποι παρέμβασης

Η πρώτη μεγάλη κατηγορία τρόπων αντιμετώπισης των κινδύνων του Διαδικτύου περιλαμβάνει όλα εκείνα τα τεχνικά μέσα (κυρίως λογισμικά) που υπάρχουν προκείμενου να ελέγχεται, να καταγράφεται και να προλαμβάνεται η χρήση επιβλαβούς υλικού από κάποιον ανήλικο στο Διαδικτύου, η προστασία των προσωπικών δεδομένων του αλλά και η ασφάλεια του υπολογιστή του. Παρακάτω αναφέρονται πιο αναλυτικά διάφορες κατηγορίες λογισμικών αλλά και τεχνικών μέσων γενικότερα όπως επίσης και κάποια παραδείγματα αυτών.

Τα **συστήματα φιλτραρίσματος και γονικού ελέγχου** μπορούν να εγκατασταθούν είτε σε προσωπικό υπολογιστή είτε σε κάποιο κεντρικό υπολογιστή, όπως είναι ο web server του σχολείου. Στις λειτουργίες τους περιλαμβάνεται η καταγραφή των ιστοσελίδων που επισκέπτεται κάποιος, οι κινήσεις που κάνει όταν περιηγείται στο Διαδίκτυο, προειδοποιήσεις για ακατάλληλο περιεχόμενο ή και η διακοπή της σύνδεσης σε τέτοιου είδους ιστοσελίδες ή ακόμη και πλήρης διακοπή της λειτουργίας του υπολογιστή. Επίσης με τα φίλτρα ελέγχεται και το περιεχόμενο που εξέρχεται από τον υπολογιστή όπως προσωπικά δεδομένα.

Το *Windows Family Safety* που ανήκει στα λογισμικά αυτά, δίνει τη δυνατότητα να οριστούν ιστοσελίδες που επιτρέπεται να επισκέπτεται ο ανήλικος (ασφαλείς ιστοσελίδες) και καταγράφει τις κινήσεις του στο Διαδίκτυο.

Το *ParetoLogic PGsurfer* είναι δωρεάν πρόγραμμα το οποίο φιλτράρει το περιεχόμενο των ιστοσελίδων, τα chat rooms, τα μηνύματα άμεσης συνομιλίας, τα μηνύματα ηλεκτρονικού ταχυδρομείου, τις p2p εφαρμογές και διάφορες άλλες.

Οι **μηχανές αναζήτησης για παιδιά** αλλά και οι **φυλλομετρητές για παιδιά** επιτρέπουν το άνοιγμα μόνο εγκεκριμένων ιστοσελίδων και είναι μια καλή λύση για άτομα μικρής ηλικίας όσον αφορά στην ασφαλή περιήγησή τους στο Διαδίκτυο.

Ο φυλλομετρητής *KidRocket* είναι ένας αρκετά ασφαλής, δωρεάν φυλλομετρητής για παιδιά, καθώς κόβει από μόνος του όλες τις επικίνδυνες ιστοσελίδες του Διαδικτύου και δεν μπορεί κάποιος να τις επισκεφθεί.

Ο φυλλομετρητής *KidZui* σχεδιάστηκε για εύκολη και ασφαλή περιήγηση των παιδιών στο Διαδίκτυο. Δεν επιτρέπει την πρόσβαση παντού παρά μόνο σε ιστοσελίδες που έχουν εγκριθεί από εκπαιδευτικούς και γονείς. Η λίστα αυτών των ιστοσελίδων περιέχει εκατομμύρια κόμβους και μεγαλώνει συνεχώς.

Προγράμματα **προστασίας από υιούς (antivirus)** και **προγράμματα τείχους προστασίας (firewall)** είναι απαραίτητα σε κάθε υπολογιστή με σύνδεση στο Διαδίκτυο. Τα πρώτα προστατεύουν τον υπολογιστή από κάποιον ενδεχόμενο υιό. Τα δεύτερα αποτρέπουν την απομακρυσμένη πρόσβαση τρίτων στον προσωπικό μας υπολογιστή μέσω του Διαδικτύου.

Το *Avast* και το *AVG* είναι αντιϊικά προγράμματα που προστατεύουν τον υπολογιστή μας από διάφορων ειδών κακόβουλα λογισμικά που μπορεί να εγκατασταθούν σε αυτόν χωρίς την άδειά μας. Διατίθενται και δωρεάν για χρήση σε προσωπικό υπολογιστή.

Το *Online Armor Free* είναι ένα από τα καλύτερα και πιο ισχυρά firewalls που είναι δωρεάν και συμβάλλει στην προστασία του υπολογιστή μας από απειλές του Διαδικτύου.

**Λογισμικά αντικατασκοπείας, ηλεκτρονικού ψαρέματος, φίλτρα για spam και διαφόρων άλλων τύπων** διατίθενται (πολλά από αυτά και δωρεάν) για την αντιμετώπιση διαφόρων κινδύνων του Διαδικτύου όπως υποκλοπή πολύτιμων ή προσωπικών στοιχείων από τον υπολογιστή μέσω δικτύων. Πιο συγκεκριμένα, φίλτρα για spam (ανεπιθύμητης αλληλογραφίας)

συνήθως παρέχονται από τον ίδιο τον πάροχο της ηλεκτρονικής αλληλογραφίας και αποκλείουν μηνύματα τέτοιου είδους (μηνύματα που έχουν πολύ μεγάλο αριθμό παραληπτών και είναι συνήθως διαφημιστικά ή με κακόβουλο περιεχόμενο).

Το *Spyware Terminator* εξασφαλίζει τον εντοπισμό και την εξάλειψη κάθε προγράμματος που βάζει σε κίνδυνο τον υπολογιστή ή προσπαθεί να συλλέξει διάφορα προσωπικά δεδομένα από αυτόν.

Το *Windows Defender* προστατεύει τον υπολογιστή σε πραγματικό χρόνο από αναδυόμενα παράθυρα, χαμηλή απόδοση αλλά και διάφορες άλλες απειλές που προκαλούνται από λογισμικά υποκλοπής και κακόβουλα λογισμικά.

Κλείνοντας την κατηγορία των τεχνικών μέσων με τα οποία μπορούμε να ελαχιστοποιήσουμε τους κινδύνους που διατρέχει κάποιος ανήλικος χρησιμοποιώντας το Διαδίκτυο, καλό θα ήταν να κάνουμε μια αναφορά και στις δυνατότητες, μέσω της τεχνολογίας, που έχουν τα κοινωνικά δίκτυα για να αυξήσουν την ασφάλειά τους ως προς την υποκλοπή προσωπικών δεδομένων όπως φωτογραφιών. Παιδιά μικρής ηλικίας ξεκινούν και δημιουργούν λογαριασμούς σε διάφορους ιστότοπους κοινωνικής δικτύωσης (facebook, twitter, hi5, youtube) χρησιμοποιώντας μάλιστα πολλές φορές ψεύτικα στοιχεία μιας και στο facebook για παράδειγμα επιτρέπεται άνω των 13 ετών να δημιουργήσει κάποιος λογαριασμό. Επιπλέον πολλά από αυτά ανεβάζουν στους λογαριασμούς αυτούς προσωπικές φωτογραφίες αγνοώντας τον κίνδυνο που διατρέχουν για παράνομη αντιγραφή και χρήση αυτών από αγνώστους. Τα κοινωνικά δίκτυα λοιπόν, χρησιμοποιώντας κάποιο υδατογράφημα στα προσωπικά δεδομένα των χρηστών τους καθιστούν πολύ πιο δύσκολη την παράνομη αντιγραφή και χρήση αυτών χωρίς την άδεια τους. Μέχρι στιγμής σύμφωνα με τους (Zigomitros et al) σε πείραμα που έγινε σε δυο από τα μεγαλύτερα κοινωνικά δίκτυα δεν χρησιμοποιείται κάποιος μηχανισμός δημιουργίας υδατογραφήματος στα προσωπικά δεδομένα.

www.123rf.com

## 5.2 Παιδαγωγικοί τρόποι παρέμβασης

### 5.2.1 Διαρκής ενημέρωση γονέων, εκπαιδευτικών και μαθητών πάνω σε θέματα κινδύνων και ασφάλειας διαδικτύου

Σε παγκόσμια κλίμακα, τα κράτη αναπτύσσουν διάφορες δράσεις για την προστασία των πολιτών τους. Μια από τις κύριες δραστηριότητες είναι η ενημέρωση των πολιτών, τόσο των ίδιων των νέων όσο και των γονέων, για τις συνέπειες (θετικές / κινδύνους) της χρήσης του Διαδικτύου. Μια ομάδα πολιτών στην οποία θα πρέπει να δοθεί ιδιαίτερο βάρος, όσον αφορά την ενημέρωση και τη συνειδητοποίηση της οντότητας του Διαδικτύου είναι οι γονείς. Οι γονείς που έχουν την κύρια ευθύνη της ασφάλειας των παιδιών στο διαδίκτυο, ασκούν συχνά μειωμένη εποπτεία στη διαχείριση της διαδικτυακής συμπεριφοράς των παιδιών, λόγω της έλλειψης μιντιακού γραμματισμού και διαθέσιμου χρόνου (Ελληνικό Κέντρο Ασφαλούς διαδικτύου 2007). Υπάρχει ένα ψηφιακό χάσμα μεταξύ του γονιού και του παιδιού όσον αφορά τη χρήση και αξιοποίηση του διαδικτύου. Ο κύριος λόγος βασίζεται στο γεγονός ότι τα παιδιά έχουν γεννηθεί μετά την εξάπλωση του διαδικτύου θεωρώντας τη χρήση του ηλεκτρονικού υπολογιστή και του διαδικτύου δεδομένη (Οδηγός ασφαλούς χρήσης διαδικτύου Microsoft).

Κάποιοι γονείς μπορεί να αγνοούν πλήρως τους κινδύνους από τη χρήση του Διαδικτύου, κάποιοι άλλοι να πιστεύουν ότι τους γνωρίζουν όλους, ενώ άλλοι υποτιμούν τον κίνδυνο εμπλοκής του παιδιού τους σε επικίνδυνες συμπεριφορές στο διαδίκτυο.

Από την άλλη, οι εκπαιδευτικοί παρουσιάζονται να διαθέτουν σε μεγαλύτερο βαθμό από τους γονείς ψηφιακό και μιντιακό γραμματισμό, με μόνο το 41% να δηλώνει ανεπάρκεια στην καθοδήγηση στη χρήση του διαδικτύου. Στο ίδιο συμπέρασμα καταλήγει και άλλη έρευνα, όπου διαπιστώνεται μια αντίφαση από τους εκπαιδευτικούς: αν και το 57% των εκπαιδευτικών προτρέπει τους μαθητές να χρησιμοποιούν το διαδίκτυο, ταυτόχρονα δηλώνει αδυναμία να το ελέγξει σοβαρά. Οι εκπαιδευτικοί προσδίδουν στο σχολείο ως θεσμό περισσότερο αυξημένο ρόλο για την εκπαίδευση των μαθητών στη σωστή χρήση του Διαδικτύου από ότι έχουν οι ίδιοι. (Κατερέλος 2009).

Γονείς και εκπαιδευτικοί υποεκτιμούν τον θεμελιώδη ρόλο τους στο μιντιακό γραμματισμό των μαθητών. Αυτό μπορεί να οφείλεται στην υποτίμηση του θέματος αλλά και στο φοβικό σύνδρομο για την τεχνολογία από το οποίοι φαίνεται ότι διακατέχονται οι ψηφιακά αναλφάβητοι γονείς και εκπαιδευτικοί. (Ελληνικό Κέντρο ασφαλούς διαδικτύου 2010).

Από τα παραπάνω προκύπτει πως γονείς και εκπαιδευτικοί χρειάζεται να ενημερωθούν σε θέματα χρήσης και ασφάλειας διαδικτύου, ώστε, χωρίς φόβους και προκαταλήψεις, να μπορούν να καθοδηγήσουν και να βοηθήσουν ουσιαστικά τους μαθητές στην ασφαλή πλοήγησή τους το διαδίκτυο (Δημητρακάκης και συν., 2011). Εκστρατείες ευαισθητοποίησης γονέων, εκπαιδευτικών και μαθητών, οργανωμένες από το κράτος και αρμόδιους φορείς, σε διεθνές και εθνικό επίπεδο, σχολές γονέων, προγράμματα, δράσεις και ημερίδες μπορούν να λειτουργήσουν προς αυτή την κατεύθυνση, επικεντρωμένες στους κινδύνους που έχουν προαναφερθεί και σε οδηγίες για την αντιμετώπισή τους (Valcke και συν., 2011)

### 5.2.2 Επαγρύπνηση των γονέων και ουσιαστική επικοινωνία με τα παιδιά τους

Όπως συμβαίνει για κάθε ενασχόληση των παιδιών, είναι σημαντικό να γνωρίζουν οι γονείς με τι ασχολούνται τα παιδιά τους στο διαδίκτυο και να τα υποστηρίζουν σε αυτές τους τις δραστηριότητες. Τα παιδιά ίσως θέλουν να κρατήσουν την ενασχόλησή τους με το Διαδίκτυο μυστική, ιδιαίτερα εάν πιστεύουν ότι οι γονείς τους θα τα περιορίσουν αναφορικά με τη χρήση του Διαδικτύου. Το Διαδίκτυο είναι μια καταπληκτική πηγή, που περιέχει τεράστιους όγκους συναρπαστικών και εκπαιδευτικών πληροφοριών. Είναι σημαντικό οι γονείς να μην

υπερβάλουν, ούτε να θέτουν υπερβολικούς περιορισμούς στη χρήση του Διαδικτύου από τα παιδιά τους. Οι κίνδυνοι πρέπει να γίνονται κατανοητοί, έτσι ώστε τα παιδιά να προστατεύονται και να εκμεταλλεύονται απόλυτα αυτό το καταπληκτικό εργαλείο. Τα παιδιά μαθαίνουν με τον πειραματισμό, δοκιμάζοντας και σφάλλοντας.

Οι γονείς χρειάζεται να δείξουν στα παιδιά τους ότι είναι κοντά τους, έτοιμοι να συζητήσουν εποικοδομητικά μαζί τους και να βοηθήσουν. Όσο περισσότερα γνωρίζουν για τον τρόπο με τον οποίον χρησιμοποιεί το παιδί τους το Διαδίκτυο, τόσο ευκολότερο θα είναι να τους εξηγούν τι είναι αποδεκτό και τι είναι ασφαλές. Η πείρα που έχει ένας ενήλικος από τη ζωή μπορεί βοηθήσει τα παιδιά να κατανοήσουν πώς πρέπει να συμπεριφέρονται στον εικονικό κόσμο. Η επίβλεψη των γονέων, υπαγορεύει όρια και κανόνες στη χρήση του διαδικτύου, στην πρόσβαση σε εφαρμογές, ή διαμεσολαβεί ενεργητικά, όταν οι γονείς μαζί με το παιδί τους χρησιμοποιούν ή συζητούν για το διαδίκτυο (Valcke και συν. 2011). Οι δραστηριότητες που πραγματοποιούνται στον υπολογιστή, τα μέσα πρόσβασης και ο χρόνος που δαπανάται χρειάζεται να επιβλέπονται από τους γονείς (Verheecke 2008).

Χρειάζεται βέβαια να υπάρχει συνεργασία ανάμεσα στην οικογένεια και το σχολείο, ώστε και οι δύο πλευρές συμβουλών να δίνουν στα παιδιά τα ίδια μηνύματα ( Wishart 2004).

Πρακτικές συμβουλές για τους γονείς θα μπορούσαν να είναι οι ακόλουθες:

- Τοποθετήστε τον υπολογιστή σε ένα δωμάτιο που χρησιμοποιείται από όλη την οικογένεια. Έτσι, το να συζητάτε για το Διαδίκτυο και να ρίχνετε μια ματιά πώς χρησιμοποιείται γίνεται μέρος της καθημερινής σας ζωής. Είναι ευκολότερο να συζητάτε τα προβλήματα όταν ο υπολογιστής βρίσκεται σε κοινό δωμάτιο. Μπορείτε ακόμα να χρησιμοποιείτε το Διαδίκτυο από κοινού.

- Συζητήστε για το Διαδίκτυο. Εκδηλώστε ενδιαφέρον για όσα κάνει το παιδί σας και οι φίλοι του, τόσο στο Διαδίκτυο όσο και εκτός. Συζητήστε μαζί του για τα υπέροχα και συναρπαστικά πράγματα για τα οποία μπορείτε να χρησιμοποιήσετε το Διαδίκτυο, καθώς και για τα προβλήματα που μπορεί να συναντήσετε. Συζητήστε με το παιδί σας τι θα πρέπει να κάνει αν αισθανθεί άσχημα σε κάποια κατάσταση στο Διαδίκτυο.

- Χρησιμοποιήστε το Διαδίκτυο μαζί: Βρείτε τοποθεσίες κατάλληλες για παιδιά ή μάθετε πώς μπορείτε να εντοπίζετε χρήσιμες πληροφορίες: προγραμματίστε μαζί ένα ταξίδι για διακοπές,

δείτε μαζί εκπαιδευτικές τοποθεσίες για να υποστηρίξετε τις σχολικές τους εργασίες ή βρείτε πληροφορίες για τα χόμπι και τα ενδιαφέροντα των παιδιών σας. «Σερφάροντας» μαζί στο Διαδίκτυο μπορείτε επίσης να βοηθήστε τα παιδιά σας να εκτιμήσουν την αξία των πληροφοριών που θα βρείτε. Μπορείτε να τοποθετήσετε σελιδοδείκτες στις αγαπημένες σας διαδικτυακές τοποθεσίες, έτσι ώστε να μπορείτε να ανατρέξετε εύκολα στις τοποθεσίες που μπήκατε μαζί.

- Κάντε μια συμφωνία με τα παιδιά σας, για το πώς και το πότε θα χρησιμοποιούν το Διαδίκτυο. Μπορεί να είναι χρήσιμο να συμφωνήσετε σε συγκεκριμένες ώρες και συγκεκριμένες διαδικτυακές τοποθεσίες που μπορούν τα παιδιά να χρησιμοποιούν στο Διαδίκτυο. Θα χρειαστεί να συζητήσετε μαζί τους αυτό το θέμα και να συμφωνήσετε από κοινού.

- Υποστηρίξτε το παιδί σας αν συναντήσει δυσάρεστο ή ανάρμοστο υλικό στο διαδίκτυο. Αποφύγετε τις υπερβολικές αντιδράσεις, έτσι ώστε το παιδί σας να αισθάνεται άνετα και να εξακολουθήσει σας μιλά για τέτοιου είδους περιστατικά και στο μέλλον. Επισημάνετε στο παιδί σαφώς ότι δεν πρόκειται για δικό του λάθος.

Μιλήστε στο παιδί σας για τους τρόπους με τους οποίους μπορεί να αποφεύγει τέτοιου είδους καταστάσεις στο μέλλον μεταξύ των οποίων και η χρήση μηχανών αναζήτησης φιλικών προς τα παιδιά και η διαγραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου από πρόσωπα που δεν γνωρίζουν.

### 5.2.3 Ο ρόλος του εκπαιδευτικού

Η σύγχρονη έρευνα έχει δείξει ότι οι γονείς αλλά και η κοινωνία θεωρούν ότι το σχολείο πρέπει να παίξει κεντρικό ρόλο στην ανάπτυξη στάσεων και συμπεριφορών ασφαλούς χρήσης του διαδικτύου. Οφείλει το σχολείο να προσφέρει σαφέστερη καθοδήγηση σχετικά με την ασφαλή χρήση του διαδικτύου και των δυνατοτήτων του (chat, email, ιστοσελίδες, φίλτρα, λογισμικό αποκλεισμού κ.α) (Children's Charities' Coalition for Internet Safety, 2001, Wishart 2004).

Ο εκπαιδευτικός μπορεί να κάνει γνωστούς τους κινδύνους στους μαθητές και να τους εφοδιάσει με δεξιότητες και εργαλεία ασφαλούς χρήσης. Χρειάζεται βέβαια πρώτα ο εκπαιδευτικός να είναι ενημερωμένος για τους κινδύνους και τις στρατηγικές αντιμετώπισης και στη συνέχεια με

αληθινό ενδιαφέρον να σταθεί δίπλα στο μαθητή, ενθαρρύνοντάς τον να μοιραστεί τις επιθυμίες, τους φόβους αλλά και τις εμπειρίες του μέσα από τη χρήση του διαδικτύου και των χώρων κοινωνικής δικτύωσης. (εκπαιδευτικός σύμβουλος και συνοδοιπόρος) (Παπαλεωνίδας και συν. 2011).

Είναι ανάγκη λοιπόν οι εκπαιδευτικοί να επιδιώξουν την ανάπτυξη συγκεκριμένων δεξιοτήτων και στρατηγικών με βάση τις εμπειρίες αλλά και τις ανάγκες των μαθητών, που αφορούν στη χρήση του Διαδικτύου (Action Innocence, 2009). Η ενημέρωση, η γνώση και οι δεξιότητες που επιτρέπουν στα παιδιά να αντιμετωπίσουν τους πιθανούς κινδύνους στο διαδίκτυο κρίνονται προτιμότεροι από την απαγόρευση στην πρόσβασή του (Wishart 2004).

Πιο πρακτικά, οι εκπαιδευτικοί μπορούν:

- Να κάνουν συζήτηση με τους μαθητές, στο επίπεδο της τάξης, για τη χρήση του Internet.
- Να δημιουργήσουν τη δική τους λίστα με προτεινόμενες σελίδες, με κατάλληλο περιεχόμενο που θα αναδεικνύει τις ανθρωπιστικές αξίες και θα προάγει το γνωστικό και πνευματικό επίπεδο των μαθητών.
- Να διδάσκουν τους μαθητές να μη δίνουν ποτέ προσωπικά στοιχεία και πληροφορίες.
- Να ελέγχουν τα Αγαπημένα (Bookmarks) και το Ιστορικό (History) του προγράμματος φυλλομετρητή (browser), για να δουν ποιες σελίδες επισκέπτονται οι μαθητές.
- Να επιβλέπουν τους μαθητές κατά τη χρήση του διαδικτύου στο σχολικό εργαστήριο ή στη σχολική τάξη.
- Με τις ενέργειες και το παράδειγμά τους μπορούν να προωθήσουν στην πράξη τις πρακτικές καλής χρήσης του Internet και των διαδικτυακών υπηρεσιών (Ηλιάδη).

Επίσης, η επένδυση σε σχολικά εργαστήρια όπου θα υπάρχει οργανωμένη και ασφαλής χρήση θα αποτελέσει το καλύτερο παράδειγμα για τους μαθητές για το μέλλον.

### 5.2.4 Μάθημα ασφάλειας διαδικτύου στα σχολεία ανεξάρτητα ή μη από το μάθημα της Πληροφορικής

Καθώς ο ρόλος του σχολείου φαίνεται θεμελιώδης, γεννιέται το ερώτημα αν η ευαισθητοποίηση και η ενημέρωση των μαθητών για το πώς να χρησιμοποιούν το διαδίκτυο με ασφάλεια διδασκαλία της ασφάλειας στο διαδίκτυο θα αποτελέσει αυτόνομο διδακτικό αντικείμενο στα πλαίσια του αναλυτικού προγράμματος ή όχι, σε ποιες τάξεις θα απευθύνεται και με ποιο περιεχόμενο (Wishart 2004). Απαιτείται κατάλληλο διδακτικό υλικό και εκπαιδευτικά προγράμματα για να χρησιμοποιηθούν μέσα στην τάξη από τους μαθητές με στόχο την ανάπτυξη γνώσεων και δεξιοτήτων ασφαλούς πλοήγησης εντός και εκτός σχολείου (Valcke και συν. 2007).

Στην Ελλάδα, ο διδακτικός στόχος της ασφαλούς χρήσης του διαδικτύου προβλέπεται στο ΔΕΠΠΣ Πληροφορικής τόσο για το Δημοτικό όσο και για το Γυμνάσιο. Συγχρόνως όμως, είναι δυνατόν να αναπτυχθούν σχετικές δραστηριότητες στα Πλαίσια σχολικών δραστηριοτήτων Αγωγης Υγείας ή και Πολιτιστικών αλλά και διαθεματικές δραστηριότητες.

Ο εκπαιδευτικός μπορεί να διαγνώσει τις ανάγκες των μαθητών που αφορούν τη χρήση του διαδικτυου: με τη χρήση μικρών ομάδων εργασίας ή και ατομικά οι μαθητές απαντούν σε ερωτήσεις για τη δική τους χρήση του διαδικτύου αλλά και για το τι θα ήθελαν να μάθουν περισσότερο. Με βάση τις απαντήσεις τους, ο εκπαιδευτικός οργανώνει συμμετοχικές ή άλλες δραστηριότητες.

### 5.2.5 Διδακτικά σενάρια- Βιωματική / συμμετοχική εκπαίδευση

**Παρακολούθηση βίντεο με στόχο την αλλαγή στάσεων**

Η ασφαλής χρήση του διαδικτύου πέρα από γνώση είναι και στάση και συμπεριφορά, η αλλαγή της οποίας αποτελεί δύσκολο εγχείρημα και συμβαίνει εκπαιδευτικά μόνο με βιωματικό τρόπο. Για παράδειγμα, με την ανάπτυξη της ενσυναίσθησης και την εκπαιδευτική μέθοδο της προσομοίωσης με αφορμή την παρακολούθηση ενός βίντεο σχετικά με την παρενόχληση ενός 12χρονου μέσω διαδικτύου, οι μαθητές κατανοούν τον κίνδυνο, αναρωτιούνται για το τι θα

έπρεπε να προσέξει το «θύμα», τι πληροφορίες δεν πρέπει να δίνουμε, πώς πρέπει να αντιδράσει κανείς, τι πρέπει να κάνει ο καθένας ως μαθητής, εκπαιδευτικός, σύλλογος διδασκόντων και Διευθυντής, προκειμένου να προλάβουν αλλά και να αντιμετωπίσουν ένα τέτοιο περιστατικό (Πανσεληνάς 2010). Οι μαθητές κατανοούν τι αποτελεί παρενόχληση μέσω των ΤΠΕ, αναγνωρίζουν την επίδραση που μπορεί να έχουν φαινόμενα παρενόχλησης στους ανθρώπους, στοχάζονται σχετικά με τη δική τους συμπεριφορά στο διαδίκτυο, έτσι ώστε να βοηθούν τον εαυτό τους και τους άλλους, μαθαίνουν στρατηγικές ώστε να αποφεύγουν την εμπλοκή τους ως θύματα, θύτες αλλά και ως συνεισφέροντες σε αρνητικές καταστάσεις στο χώρο του διαδικτύου.

**Παιχνίδι ρόλων Net-Detectives**

Όσον αφορά στο ρόλο του σχολείου, συχνά γίνεται αναφορά σε τρόπους παρέμβασης όπως κανόνες, έλεγχος, παρακολούθηση, αλλά δεν περιλαμβάνονται διδακτικές στρατηγικές που εξασφαλίζουν την ενεργό συμμετοχή των μαθητών με αποτέλεσμα την απόκτηση γνώσεων και δεξιοτήτων. Μια τέτοια διδακτική στρατηγική είναι το παιχνίδι ρόλων, το οποίο, σύμφωνα με τους Wishart, Oades και Morris (2006) έχει θετική επίδραση στους μαθητές. Στο παιχνίδι ρόλων που εφάρμοσαν, στηριγμένο στους υπολογιστές, με το όνομα Net-Detectives, οι μαθητές γίνονται ντετέκτιβ για να ερευνήσουν την κακή χρήση των υπολογιστών του σχολείου.

Τα παιδιά, χωρισμένα σε ομάδες, με την επίβλεψη των δασκάλων τους, γίνονται ντετέκτιβ του διαδικτύου, ρωτούν μέσω ίντερνετ ειδικούς, και βοηθούν στη λύση προβληματικών σεναρίων της πραγματικής ζωής. Για παράδειγμα, το σενάριο «Μπορείς να βοηθήσεις ένα φίλο;» βασίζεται σε θέματα ασφάλειας διαδικτύου που προκύπτουν, όταν ένα 13χρονο κορίτσι εκφράζει ανησυχία για τη συμπεριφορά διαδικτυακού φίλου με τον οποίο συνομιλούσε στο chat (εξαπάτηση).

Έτσι, μέσα από το παιχνίδι ρόλων οι μαθητές συμπάσχουν με τους άλλους, συνειδητοποιούν τα κίνητρά τους και ασκούν στην πράξη όσα διδάσκονται για την ασφάλεια του διαδικτύου. Τα αποτελέσματα έδειξαν αλλαγές στις στάσεις και στη συμπεριφορά των μαθητών. Επιπλέον, τα παιδιά συζήτησαν τα κίνητρά τους και ασκήθηκαν σε δεξιότητες στις ΤΠΕ, σε συνεργασία με άλλους μαθητές. Οι μαθητές έμαθαν για την ασφάλεια στο διαδίκτυο μέσα από ένα συναρπαστικό και γεμάτο προκλήσεις περιβάλλον (Wishart 2007).

Φαίνεται πως τα παιχνίδια ρόλων αλλά και κάθε είδους δραστηριότητες που μπορεί να επινοήσει ο δάσκαλος, οι οποίες κινητοποιούν τους μαθητές και τους ενθαρρύνουν να συμμετέχουν για την αντιμετώπιση προβληματικών καταστάσεων της καθημερινής ζωής, σχετικές πάντα με την ασφάλεια στο διαδίκτυο, είναι τα πιο ελπιδοφόρα και αποτελεσματικά μέσα για την αλλαγή στάσεων και υιοθέτηση κανόνων κατά την πλοήγηση στο διαδίκτυο (Valcke 2007).

**Μαθαίνοντας την Ασφάλεια του Διαδικτύου με χρήση του SimSafety**

Το έργο «SimSafety: Flight Simulator for Internet Safety» (http://www.simsafety.eu) με συγχρηματοδότηση από την Ευρωπαϊκή Ένωση, απευθύνεται σε γονείς, μαθητές κι εκπαιδευτικούς και προσεγγίζει ζητήματα ασφαλούς χρήσης του διαδικτύου υπό το πρίσμα της συνεργασίας και της αλληλεγγύης μεταξύ των νεωτέρων και των μεγαλυτέρων με στόχο τη δημιουργία μιας κοινής αντίληψης ως προς την κατανόηση των κινδύνων που επιφυλάσσει η χρήση του διαδικτύου αλλά και του τρόπου αντιμετώπισής τους. Πρόκειται για παιχνίδι ρόλων, όπου κάθε παίχτης παραλαμβάνει μια ταυτότητα / κρυφό ρόλο τον οποίο πρέπει να παίξει όσο καλύτερα μπορεί, προσπαθώντας ταυτόχρονα να καταλάβει το ρόλο των άλλων. Ενθαρρύνει τη συζήτηση μέσα στην τάξη για τους κανόνες συμπεριφοράς και καλής χρήσης στο διαδίκτυο. Οι ενότητες του παιχνιδιού αφορούν στη δημοσίευση προσωπικών στοιχείων, στην ευαισθητοποίηση σε συμπεριφορές που μπορεί να πληγώνουν διαδικτυακούς φίλους και στο πώς χειριζόμαστε την πρόσβαση σε δεδομένα ή αντικείμενα άλλου http://www.pi.ac.cy/InternetSafety/drastiriotites_simsafety.html.

### 5.2.6 Κανόνες ασφαλούς χρήσης διαδικτύου

- Συζητώ με τους γονείς μου για να μάθω τους κανόνες χρήσης του Διαδικτύου.
- Δεν αποκαλύπτω προσωπικά δεδομένα, όπως διεύθυνση του σπιτιού, αριθμός τηλεφώνου, αριθμούς πιστωτικών καρτών ή το όνομα του σχολείου μου, χωρίς την άδεια των γονέων μου.
- Ενημερώνω τους γονείς μου, εάν δω ή λάβω κάτι από το Διαδίκτυο που με ενοχλεί ή νιώθω ότι με απειλεί.

- Δε συμφωνώ να συναντήσω κάποιον που γνώρισα στο Διαδίκτυο, χωρίς την άδεια των γονέων μου.
- Δε στέλνω φωτογραφίες δικές μου ή μελών της οικογένειάς μου σε άλλους, μέσω του Διαδικτύου ή με την τακτική αλληλογραφία, χωρίς την άδεια των γονέων μου.
- Δεν αποκαλύπτω τους κωδικούς πρόσβασης στο Διαδίκτυο σε κανέναν (ούτε και στους καλύτερούς μου φίλους), παρά μόνο στους γονείς μου.
- Φέρομαι σωστά όταν βρίσκομαι στο Διαδίκτυο και δεν κάνω τίποτα που μπορεί να προσβάλει ή να εξοργίσει άλλους ή είναι παράνομο.
- Δεν κάνω κάτι που κοστίζει χρήματα, χωρίς την άδεια των γονέων μου.

### 5.3 Άλλοι (εξειδικευμένοι) τρόποι

Όλοι οι παραπάνω τρόποι που αναφέρθηκαν (τεχνικοί και παιδαγωγικοί) λειτουργούν προληπτικά. Υπάρχουν όμως και περιπτώσεις που χρειάζεται η παρέμβαση κάποιας δημόσιας αρχής προκειμένου να λυθεί κάποιος κίνδυνος ή κάποια απειλή που συμβαίνει μέσω του Διαδικτύου. Αυτή η αρχή ονομάζεται **Δίωξη Ηλεκτρονικού Εγκλήματος** και ασχολείται με όλες τις εγκληματικές ενέργειες που διαπράττονται μέσω δικτύων.

Επιπρόσθετα, μέσω διάφορων κοινωνικών φορέων και δράσεων μπορεί κάποιος να αναφέρει σε κάποιον αρμόδιο την ύπαρξη ιστοσελίδας παράνομου περιεχομένου ή κάποιας απειλής στο Διαδίκτυο. Η **Ελληνική Ανοιχτή Γραμμή SafeLine** δέχεται καταγγελίες για ιστοσελίδες και υπηρεσίες νέων όπου υπάρχει ρατσιστικό, παράνομο, ξενοφοβικό περιεχόμενο ή εικόνες κακομεταχείρισης παιδιών. Επίσης το δίκτυο **INHOPE** επικεντρώνεται στον εντοπισμό παράνομου περιεχομένου στο Διαδίκτυο.

Στην ιστοσελίδα **www.saferinternet.gr** υπάρχουν πολλές ενημερωτικές πληροφορίες για εκπαιδευτικούς, γονείς αλλά και μαθητές για τους κινδύνους που διατρέχουμε στο Διαδίκτυο, πώς μπορούμε να τους εξαλείψουμε αλλά και σε ποιους αρμόδιους φορείς θα πρέπει να απευθυνθούμε αν έρθουμε αντιμέτωποι με κάποιον από αυτούς.

Το *Cyberkids* είναι μία πρωτοβουλία του Υπουργείου Προστασίας του Πολίτη και του Αρχηγείου της Ελληνικής Αστυνομίας, που υλοποιείται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, με τη χορηγία γνωστής εταιρείας παροχής υπηρεσιών κινητής, σταθερής τηλεφωνίας και internet στο πλαίσιο ενημέρωσης και ευαισθητοποίησης παιδιών ηλικίας μέχρι 12 ετών, καθώς και των γονέων τους σχετικά με την ασφάλεια στο Διαδίκτυο. Αποσκοπεί στην ασφαλή εξοικείωση αυτών με τις νέες τεχνολογίες και κυρίως με το Διαδίκτυο. Στόχος του είναι η προβολή των θετικών πλευρών του Διαδικτύου, όπως είναι η αναζήτηση χρήσιμων πληροφοριών και η ψυχαγωγία. Παράλληλος στόχος είναι η ενημέρωση για τους πιθανούς κινδύνους που κρύβονται. Οι γονείς μπορούν να το επισκεφτούν μαζί με τα παιδιά τους, να διασκεδάσουν και να ενημερωθούν για το πώς μπορούν να πλοηγηθούν με ασφάλεια.

## 6. Ασφάλεια στο διαδίκτυο: Η ελληνική πραγματικότητα.

### Έρευνα στην 4η Περιφέρεια Αχαΐας

### ΓΕΝΙΚΑ

Το Διαδίκτυο είναι σήμερα καθημερινό εργαλείο στη ζωή μας: για την αναζήτηση πληροφοριών, για επικοινωνία, για αγορές, για ψυχαγωγία. Από μικρή ηλικία τα παιδιά έχουν πρόσβαση στο Διαδίκτυο και το θεωρούν ως μια αγαπημένη απασχόλησή τους. Η έρευνα δείχνει ότι τα παιδιά στην πλειοψηφία τους χρησιμοποιούν το Διαδίκτυο πολλές φορές την ημέρα, ενώ η χρήση του Διαδικτύου και των κινητών τηλεφώνων είναι σχεδόν αυτονόητη για την ευρωπαϊκή νεολαία. Σε γενικές γραμμές, οι νέοι γνωρίζουν τις προκλήσεις όταν χρησιμοποιούν το Διαδίκτυο, ωστόσο, όταν αντιμετωπίσουν πρόβλημα, οι ανήλικοι απευθύνονται στους μεγαλύτερους μόνο ως τελευταία λύση (Ευρωβαρόμετρο, 2007).

Οι δυνατότητες που προσφέρει το Διαδίκτυο είναι τεράστιες. Η αποτελεσματική αξιοποίησή του, όμως, προϋποθέτει την ορθή χρήση του. Ως εκ τούτου, σε ευρωπαϊκό επίπεδο έχουν αναπτυχθεί δράσεις και προγράμματα που στοχεύουν στη δημιουργία ασφαλέστερων συνθηκών αξιοποίησης των δυνατοτήτων του Διαδικτύου.

Το θέμα της ασφαλούς χρήσης του Διαδικτύου απασχολεί εδώ και αρκετά χρόνια τον εκπαιδευτικό κόσμο και εμείς οι δάσκαλοι, καλούμαστε από τη μια να προσφέρουμε τη

δυνατότητα πρόσβασης όλων των παιδιών στις νέες τεχνολογίες και στο Διαδίκτυο και από την άλλη τη διαπαιδαγώγηση ορθής αξιοποίησής τους. Η ασφάλεια των παιδιών και η εκπαίδευσή τους στη διαχείριση των κινδύνων που αντιμετωπίζουν, είτε αυτοί οι κίνδυνοι αφορούν στην καθημερινή φυσική τους ζωή είτε στη χρήση του Διαδικτύου προς αναζήτηση πληροφοριών, κοινωνικής δραστηριότητας ή απλώς ανταλλαγής υλικού, είναι μια από τις προτεραιότητες τόσο τις δικές μας όσο και της Ευρωπαϊκής Ένωσης.

**ΕΙΣΑΓΩΓΗ**

Αντικείμενο της παρούσας εμπειρικής έρευνας, είναι η αποτύπωση και διερεύνηση των ιδεών των μαθητών της Στ΄ τάξης των Δημοτικών σχολείων της 4ης Εκπαιδευτικής Περιφέρειας Πρωτοβάθμιας Εκπαίδευσης της Περιφερειακής ενότητας Αχαΐας.

Πρόκειται για δώδεκα (12) σχολεία της πόλης των Πατρών που βρίσκονται στις περιοχές της Άνω Πόλης, των Ζαρουχλέικων και στο νοτιοανατολικό τομέα της πόλης. Η οργανικότητα ποικίλει: εφτά (7) δωδεκαθέσια, δύο (2) δεκαθέσια, ένα (1) οχταθέσιο και δύο (2) εξαθέσια.

Η έρευνα διεξήχθη από τον Νοέμβριο του 2012 ως τον Ιανουάριο του 2013 και τα δεδομένα της αναλύθηκαν με το στατιστικό πακέτο SPSS (Maykut & Morehouse, 1994).

Για τους σκοπούς της έρευνας φτιάχτηκε ένα ερωτηματολόγιο και διανεμήθηκε στους μαθητές που φοιτούν στα Δημοτικά σχολεία της παραπάνω περιφέρειας.

Βασικά ερωτήματα ήταν:

- Πόσο συχνά χρησιμοποιούν οι μαθητές το διαδίκτυο, τις Ιστοσελίδες κοινωνικής δικτύωσης (Facebook, Hi5, My space..), τα Chat Rooms (MSN, Yahoo) και πόσο συχνά παίζουν διαδικτυακά παιχνίδια, ανταλλάσσουν αρχεία ή ακούνε μουσική και παρακολουθούν ειδήσεις.
- Με ποιο τρόπο (σταθερό τηλέφωνο, κινητό ή υπολογιστή) επικοινωνούν με τους φίλους τους.
- Αν έχουν δεχτεί κάποιου είδους παρενόχληση κατά τη χρήση του διαδικτύου και αν γνωρίζουν για την ασφάλεια και τους κινδύνους που κρύβει η χρήση του.

Ως αντικειμενικό πληθυσμό, ορίσαμε τους μαθητές στους οποίους δόθηκαν τα ερωτηματολόγια (Παρασκευόπουλος, 1993).

## ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η χρήση του Διαδικτύου στις μέρες μας έχει ξεπεράσει κάθε προσδοκία – λίγοι γνωρίζουν ότι το σύστημα αυτό στήθηκε για πρώτη φορά στα τέλη της δεκαετίας του 1960 (τότε που περπάτησε ο πρώτος άνθρωπος στο φεγγάρι!). Στην αρχική του μορφή, πέτυχε, για πρώτη φορά, τη σύνδεση δικτυακών υποδομών πανεπιστημίων και κυβερνητικών υπηρεσιών στις ΗΠΑ, για ανταλλαγή ηλεκτρονικών πληροφοριών και αρχείων. Η χρήση του Διαδικτύου διευρύνθηκε τη δεκαετία του 1990, με την εισαγωγή του World Wide Web από τον Tim Berners-Lee, θέτοντας τη βάση για τα σημερινά «κλικ» που με τόση ευκολία μεταφέρουν τον χρήστη από τη μια ιστοσελίδα στην άλλη. Σήμερα το Διαδίκτυο έχει διεισδύσει σε όλους σχεδόν τους τομείς της ζωής των πολιτών – καλύπτοντας, μεταξύ άλλων, τομείς όπως της ενημέρωσης, επικοινωνίας, εκπαίδευσης, ψυχαγωγίας, κρατικών υπηρεσιών και επιχειρήσεων (http://www.saferinternet.org).

Η ευρεία χρήση των υπηρεσιών κοινωνικής δικτύωσης από ένα πολύ μεγάλο αριθμό πολιτών σε παγκόσμιο επίπεδο, σε συνδυασμό με την ευρεία χρήση των «έξυπνων κινητών» τα τελευταία χρόνια, έχει συμβάλει σε μεγάλο βαθμό στο φαινόμενο της συνεχής παρουσίας και επικοινωνίας των χρηστών μέσω του Διαδικτύου. Οι χρήστες καθίστανται, κατά τη διάρκεια της ημέρας, περισσότερο 'ενωμένοι'. Την ίδια στιγμή, με τη χρήση των υπηρεσιών κοινωνικής δικτύωσης, οι πολίτες διευκολύνονται στην έκφραση και διάδοση ιδεών και σκέψεων, καθώς και στην ανταλλαγή πληροφοριών όπως φωτογραφίες και βίντεο, ανά το παγκόσμιο – και μάλιστα, σε χρόνο λίγων δευτερολέπτων. Ταυτόχρονα, ο κάθε χρήστης είναι σε θέση να λαμβάνει μεγάλο αριθμό μηνυμάτων και πληροφοριών μέσω του Διαδικτύου.

Οι πραγματικότητες του σημερινού Διαδικτύου απαιτούν πλέον τη χρήση αυτού του εξαιρετικά χρήσιμου εργαλείου με αυξημένη αίσθηση ευθύνης και σεβασμού προς την κοινωνία και τους άλλους χρήστες. Πέρα από τα θέματα ηθικής και σωστής συμπεριφοράς στο Διαδίκτυο καθώς και της καλλιέργειας αλληλοσεβασμού σε όλες τις ηλεκτρονικές δραστηριότητες του κάθε χρήστη, υπάρχει και η άλλη όψη του νομίσματος – αυτή της προστασίας των πολιτών από τα (πολλά πλέον) κακόβουλα στοιχεία που κυκλοφορούν στο Διαδίκτυο. Είναι γνωστές οι πολλές ιστορίες περί παρενόχλησης (σεξουαλικής και μη), εκμετάλλευσης, υποκλοπής δεδομένων, πρόκλησης κακόβουλων ζημιών, κλοπής, απάτης, παρακολούθησης κ.λπ. που έχουν

παρατηρηθεί τα τελευταία χρόνια στον ηλεκτρονικό κόσμο. Δυστυχώς είναι πολλοί αυτοί που δεν έχουν αίσθηση της ευθύνης και του σεβασμού στη χρήση του Διαδικτύου και για τον λόγο αυτό ο κάθε χρήστης ενώ πρέπει να γνωρίζει πώς να συμπεριφέρεται σωστά για να μην δημιουργεί προβλήματα σε άλλους, ταυτόχρονα πρέπει να ενημερώνεται και να προφυλάσσεται από τους κινδύνους που ελλοχεύουν (http://ec.europa.eu/information_society/activities/sip/index_en.htm).

**Ασφάλεια και παιδί στο διαδίκτυο**

Στη σημερινή εποχή, τα παιδιά αρχίζουν να χρησιμοποιούν το διαδίκτυο μέσω υπολογιστών και κινητών σε όλο και μικρότερες ηλικίες. Στην Ελλάδα αυτό γίνεται κατά μέσο όρο στην ηλικία των 11 χρόνων. Η χρήση του διαδικτύου είναι ήδη απόλυτα ενσωματωμένη στην καθημερινότητα.

Κάθε γονιός χρειάζεται να κατέχει σχετική παιδεία και ο ίδιος, για να είναι σε θέση να την μεταφέρει στο παιδί του, πριν το αφήσει ελεύθερο στον «αυτοκινητόδρομο του διαδικτύου» και στην «κοινωνία της πληροφορίας» (Safeline, www.safeline.gr).

Οι πληροφορίες παρέχονται πια όλο και περισσότερο σε ψηφιακή μορφή. Έτσι αποθηκεύονται, μεταδίδονται και διαδίδονται ευκολότερα και οικονομικότερα ακόμη και στις πιο απομακρυσμένες περιοχές της χώρας. Η επικοινωνία με άτομα εντός και εκτός χώρας με φίλους, γνωστούς αλλά και με αγνώστους έχει γίνει πιο εύκολη και απλή.

Ο καθένας μας μπορεί να καταλάβει πια, πως αν δεν προστατέψουμε τις πληροφορίες που «επικοινωνούμε» μέσω διαδικτύου, αυτές θα είναι διαθέσιμες όχι μόνο σε φίλους και γνωστούς αλλά και σε κάθε άτομο που έχει πρόσβαση στο διαδίκτυο.

Επίσης είναι αυτονόητο ότι πρέπει να μάθουμε να φιλτράρουμε τις πληροφορίες αυτές, αφού η ίδια η έννοια της πληροφορίας έχει αλλάξει. Η λέξη πληροφορία αντιπροσωπεύει πλέον όλα τα δεδομένα που υπάρχουν στο διαδίκτυο, άσχετα αν μας αφορούν άμεσα, έμμεσα ή καθόλου. Αρκετές πληροφορίες όπως π.χ. διαφημιστικά μηνύματα μας παρουσιάζονται πια χωρίς να έχουμε επιλέξει εμείς να τις δούμε (http://www.paidorama.com).

Στα πλαίσια της ενημέρωσης των μαθητών των Δημοτικών σχολειών της 4ης Περιφέρειας, αποφασίσαμε μια σειρά δράσεις οι οποίες υλοποιήθηκαν από την αρχή της σχολικής χρονιάς

2012-13 και συνεχίζουν να υλοποιούνται. Οι δράσεις, σε συνεργασία με τους Διευθυντές των σχολικών μονάδων, περιλάμβαναν σειρά ενημερωτικών συναντήσεων με εκπαιδευτικούς κυρίως των Στ΄ τάξεων, τους μαθητές αλλά και τους γονείς τους (Κέκκερης, Γ.& Δέλλας, Σ., (2003).

Οι δράσεις που αφορούσαν και συνεχίζονται για τους μαθητές περιείχαν το στοιχείο της ενημέρωσης με διαφάνειες προβολή βίντεο με μικρές ιστορίες για τους κινδύνους του διαδικτύου, και δρώμενα από τα παιδιά που παρουσίασαν είτε στους συμμαθητές τους είτε σε κοινές εκδηλώσεις με τους γονείς τους. το Νοέμβριο του 2012, όταν κρίθηκε ότι οι μαθητές είχαν ενημερωθεί επαρκώς, τους δόθηκε το ερωτηματολόγιο που τα στοιχεία του θα παρουσιάσουμε παρακάτω.

**Δράσεις που υλοποιήθηκαν στα σχολεία**

Αναζητήθηκαν στο διαδίκτυο και συγκεκριμένα στην ιστοσελίδα του Πανελληνίου Σχολικού δικτύου καθώς και στη σελίδα του Κυπριακού Υπουργείου Παιδείας οδηγίες και συμβουλές τόσο για μαθητές όσο και για τους γονείς τους. Παραθέτουμε ένα μέρος του υλικού που δόθηκε:

**«ΓΙΑ ΠΑΙΔΙΑ ΑΠΟ 5 ΜΕΧΡΙ 12 ΕΤΩΝ»**

1) ***Δυνατότητες Διαδικτύου***

**Ανταλλαγή Αρχείων/Διαμοιρασμός**

Αυτή μπορεί να γίνει με διάφορους τρόπους:

Μέσω του ηλεκτρονικού ταχυδρομείου, όπου τα αρχεία φτάνουν ως συνημμένα

με τη μεταφορά αρχείων (ftp - file transfer protocol) με τη χρήση προγραμμάτων «peer to peer», όπου η επικοινωνία και η ανταλλαγή γίνεται μεταξύ δύο υπολογιστών καθώς πλοηγούμαστε στο Διαδίκτυο μπορούμε να κατεβάσουμε αρχεία στον υπολογιστή μας.

Εξ αποστάσεως μάθηση (distance learning) είναι η εκπαιδευτική διαδικασία κατά την οποία ο εκπαιδευόμενος και ο εκπαιδευτής βρίσκονται σε φυσική απόσταση και η διδασκαλία επιτυγχάνεται με διάφορα μέσα επικοινωνίας με μικρή ή καθόλου φυσική επαφή.

**Επικοινωνία (Σύγχρονη/Ασύγχρονη)**

Η γνωστότερη μορφή επικοινωνίας στο Διαδίκτυο είναι το ηλεκτρονικό ταχυδρομείο (email). Ένα άλλο είδος ασύγχρονης επικοινωνίας είναι οι ομάδες συζητήσεων (forum). Εκτός από την επικοινωνία μέσω e-mail υπάρχουν κι άλλοι τρόποι επικοινωνίας, όπως η συνομιλία (chat), σε «πραγματικό χρόνο». Ένα τέτοιο είδος επικοινωνίας το ονομάζουμε σύγχρονη επικοινωνία.

**Ηλεκτρονικές Υπηρεσίες**

Μέσω του Διαδικτύου, μπορούμε να κάνουμε τραπεζικές συναλλαγές οποιαδήποτε ώρα της ημέρας, να πληροφορηθούμε για τα υπόλοιπα των τραπεζικών λογαριασμών μας, να πληρώσουμε τους λογαριασμούς ηλεκτρικού ρεύματος, τηλεφώνου κ.ά., να ανανεώσουμε άδειες, να κάνουμε κρατήσεις σε ξενοδοχεία της χώρας μας ή του εξωτερικού, να πάρουμε αεροπορικά εισιτήρια, να ενοικιάσουμε αυτοκίνητα, να ψάξουμε και να βρούμε εργασία, να συμπληρώσουμε και να υποβάλουμε ηλεκτρονικά κάποιες αιτήσεις.

**Ηλεκτρονικό Εμπόριο**

Με το ηλεκτρονικό εμπόριο έχουμε τη δυνατότητα να πραγματοποιούμε αγορές προϊόντων από όλο τον κόσμο μπαίνοντας στα ηλεκτρονικά καταστήματα, που έχουν δημιουργηθεί για αυτό το σκοπό ή συμμετέχοντας σε ιστοσελίδες δημοπρασιών. Επίσης, μπορούμε να διαφημίσουμε και να πουλήσουμε τα προϊόντα μας.

**Κινητό Τηλέφωνο**

Πέρα από τις γνωστές υπηρεσίες αποστολής απλών μηνυμάτων (SMS), ανταλλαγής φωτογραφιών και αποστολής μηνυμάτων πολυμέσων (MMS), μπορούμε τώρα μέσω του κινητού μας τηλεφώνου να έχουμε πρόσβαση στο Διαδίκτυο, να λαμβάνουμε email, να «κατεβάζουμε» φωτογραφίες, βίντεο, μουσική, να δημοσιεύουμε το περιεχόμενο που παράγουμε με το κινητό μας όπως φωτογραφίες ή βίντεο στο Διαδίκτυο (Moblog) ή ακόμη να στέλλουμε από το Διαδίκτυο μαζικά SMS και MMS σε κινητά (Bulk SMS).

**Κοινωνικά Δίκτυα**

Με τον όρο ιστοσελίδα Κοινωνικού Δικτύου εννοούμε τις ιστοσελίδες εκείνες, στις οποίες μπορούμε να αναρτήσουμε στοιχεία, που θα αποτελέσουν το διαδικτυακό μας προφίλ, να

έρθουμε σε επικοινωνία με φίλους ή να κάνουμε νέες φιλίες και επαγγελματικές επαφές, να ανταλλάξουμε γνώση, να ζητήσουμε άμεση υποστήριξη ή ακόμα απλά να ψυχαγωγηθούμε. Οι ιστοσελίδες κοινωνικής δικτύωσης τύπου Facebook, Hi5 και MySpace είναι οι πιο διαδεδομένες.

**Πληροφόρηση**

Χρησιμοποιώντας ένα φυλλομετρητή (browser), μπορούμε να περιηγηθούμε στις πολλές ιστοσελίδες που υπάρχουν και να πληροφορηθούμε για οτιδήποτε μας ενδιαφέρει. Αυτή η πληροφόρηση είναι άμεση και επίκαιρη.

**Ψυχαγωγία**

Μέσω του Διαδικτύου μπορούμε να ακούσουμε τον αγαπημένο μας ραδιοφωνικό σταθμό ή να παρακολουθήσουμε τηλεοπτικές εκπομπές. Μπορούμε, επίσης, να ακούσουμε μουσική και να παρακολουθήσουμε σύντομα φιλμάκια ή ολόκληρες ταινίες, να διαβάσουμε περιοδικά, την εφημερίδα της ημέρας ή ακόμα και προηγούμενων ημερών, από οποιοδήποτε μέρος του πλανήτη. Ένα μεγάλο μέρος του χρόνου αναλώνεται στα ηλεκτρονικά παιχνίδια. Έχει σχεδιαστεί ένα σύστημα από τον πανευρωπαϊκό οργανισμό PEGI για να βοηθήσει στην επιλογή των κατάλληλων παιχνιδιών. Το σύστημα PEGI αναφέρει την κατάταξη του παιχνιδιού σε ηλικιακές ομάδες και το χαρακτηρισμό του περιεχόμενου.

### *2) Κίνδυνοι Διαδικτύου*

**Ακατάλληλο Περιεχόμενο**

Ο όρος ακατάλληλο περιεχόμενο είναι υποκειμενικός σε σχέση με την ηλικία ή και την ψυχική κατάσταση του κάθε ατόμου. Συνήθως με τον όρο ακατάλληλο περιεχόμενο, αναφερόμαστε σε περιεχόμενο το οποίο μπορεί να περιλαμβάνει ρατσιστικό ή ξενοφοβικό περιεχόμενο, προώθηση επιβλαβών συμπεριφορών, προώθηση τυχερών παιχνιδιών, παρουσίαση πορνογραφικού υλικού, προώθηση βίας κ.τ.λ.

**Ανεπιθύμητα Μηνύματα (Spam)**

Ανεπιθύμητα Μηνύματα θεωρούνται τα μηνύματα εκείνα που υπό κανονικές συνθήκες οι χρήστες δεν θα επέλεγαν να δουν και τα οποία διανέμονται σε μεγάλο αριθμό παραληπτών.

**Αποξένωση**

Η αλόγιστη και πολύωρη χρήση του Διαδικτύου, δημιουργεί συναισθηματική απόσταση και αλλοιώνει την ποιότητα επικοινωνίας ανάμεσα στους ανθρώπους, κάτι το οποίο πολλές φορές οδηγεί στην Αποξένωσή τους από τον Πραγματικό Κόσμο.

**Αποπλάνηση (Grooming)**

Αποπλάνηση συμβαίνει όταν άγνωστοι κακόβουλα εκμεταλλεύονται το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικα παιδιά με στόχο τη σεξουαλική παρενόχληση.

**Βίαια Παιχνίδια**

Σύμφωνα με έρευνες, εκατομμύρια άτομα αφιερώνουν χρόνο σε καθημερινή βάση σε ηλεκτρονικά παιχνίδια. Η κατηγορία βολών θεωρείται η πλέον βίαια κατηγορία παιχνιδιών και έχει κατακριθεί ιδιαίτερα για τα κακά πρότυπα και τις αρνητικές επιδράσεις που πιθανότατα να έχει, ειδικά σε νεαρά άτομα. Βία όμως που εκφράζουμε στα παιχνίδια μπορεί να την εμφανίσουμε και στην κανονική μας ζωή. Για το λόγο αυτό, συμβουλευόμαστε πάντα τη σήμανση του Πανευρωπαϊκού Συστήματος Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (Pan European Game Information - PEGI).

**Εθισμός (Internet Addiction)**

Εθισμός στο Διαδίκτυο μπορεί να προκύψει με την πολύωρη ενασχόληση ατόμων σε διαδικτυακές δραστηριότητες όπως είναι τα παιχνίδια, δωμάτια συζητήσεων, ηλεκτρονικός τζόγος και άλλα.

**Εκφοβισμός (Cyberbullying)**

Εκφοβισμός είναι δυνατό να συμβεί μέσω του Διαδικτύου, κυρίως μέσω του ηλεκτρονικού ταχυδρομείου (email), των ιστολογίων (blogs) και δωματίων συναντήσεων (chat rooms), και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης.

**Επιβλαβείς Συμπεριφορές**

Το γεγονός ότι το Διαδίκτυο δεν είναι υπό τη δικαιοδοσία οποιουδήποτε καθιστά αδύνατο τον έλεγχο του περιεχομένου του. Ιστοσελίδες για βουλιμία, ανορεξία, αυτοκτονία, σατανισμό και τυχερά παιχνίδια υπάρχουν πολλές και παρακινούν σε επιβλαβείς συμπεριφορές.

**Ηλεκτρονικός Τζόγος**

Με τον όρο Ηλεκτρονικός Τζόγος εννοούμε τη δραστηριότητα κατά την οποία δύο ή περισσότερα άτομα συναντιόνται διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων. Μια τέτοια δραστηριότητα περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους.

**Ιοί (Virus)**

Ιός είναι κακόβουλο πρόγραμμα το οποίο εγκαθίσταται στον υπολογιστή συνήθως εν αγνοία του χρήστη και ενεργοποιείται είτε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια.

**Παιδική Πορνογραφία**

Παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η παιδική πορνογραφία θεωρείται έγκλημα και υπόκειται σε ποινικές κυρώσεις.

**Παραβίαση Ιδιωτικότητας**

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο "προσφέρουμε" προσωπικές πληροφορίες. Η περιήγηση μας στο Διαδίκτυο έχει πολλά κοινά με τη ζωή μας στο φυσικό κόσμο. Έτσι τίθενται κάποια πολύ σοβαρά ζητήματα: της προστασίας των προσωπικών μας δεδομένων, της ορθής και ηθικής επικοινωνίας με την βοήθεια της τεχνολογίας και το γεγονός πως ότι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη.

**Παραπληροφόρηση (Misinformation)**

Παραπληροφόρηση στο Διαδίκτυο είναι δυνατό να συμβεί με την παρουσίαση διαφόρων ψευδών ή αναληθών ή τροποποιημένων πληροφοριών σε ιστοσελίδες, με πιθανό σκοπό την παραπλάνηση μας. Παραπληροφόρηση συμβαίνει και όταν οι πληροφορίες είναι ελλιπείς με αποτέλεσμα να οδηγήσουν σε λανθασμένα συμπεράσματα.

**Παραποίηση Γλώσσας**

Η ανάγκη για γρήγορη και εύκολη επικοινωνία, μια συνήθεια που την αποκτήσαμε με την είσοδο της κινητής τηλεφωνίας και του Διαδικτύου στη ζωή μας, άρχισε να οδηγεί στην Παραποίηση της Γλώσσας μας. Αντί ελληνικά δηλαδή χρησιμοποιούνται τα greeklish, ελληνικά γραμμένα με λατινικούς χαρακτήρες, στα οποία ο τονισμός και η ορθογραφία δεν είναι σημαντικά. Για παράδειγμα η φράση «θα σε δω σε λίγο» θα γραφόταν «tha se do se ligo».

**Υποκλοπή Προσωπικών στοιχείων (Phishing)**

Είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών, κωδικούς πρόσβασης κ.λπ). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα (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, κωδικούς TAN, κ.λπ.

**Φυσικές Παθήσεις**

Η πολύωρη χρήση του Διαδικτύου, εγκυμονεί κινδύνους για την υγεία μας. Πέρα από τις διαταραχές στην όραση και τις υποψίες για ενδεχόμενα προβλήματα εξαιτίας της έκθεσης σε ακτινοβολία, κυρίως από τις οθόνες, εκείνοι που ασχολούνται για ώρες μπροστά στον υπολογιστή χωρίς διάλειμμα ή εναλλαγή δραστηριοτήτων κάνοντας μεγάλο αριθμό επαναλαμβανόμενων κινήσεων μπορεί να προσβληθούν από διάφορες μυοσκελετικές παθήσεις. Κακώσεις όπως ο ευθειασμός του αυχένα, ο πόνος του αγκώνα (tennis elbow), τενοντίτιδα, πηχαιοκαρπική άρθρωση και άλλες παθήσεις έχουν συνδέσει το όνομα τους με την υπερβολική χρήση του υπολογιστή.

**Χρήσιμες Συμβουλές**

Πριν χρησιμοποιήσουμε το Internet ζητούμε άδεια από κάποιον ενήλικα

Εάν κάποιες σελίδες μας κάνουν να νιώθουμε άβολα, τις κλείνουμε αμέσως και το αναφέρουμε σε κάποιον ενήλικα.

Σταματούμε αμέσως συνομιλίες που μας κάνουν να νιώθουμε άβολα και το αναφέρουμε σε κάποιον ενήλικα.

Δεν δίνουμε σε κανένα τα προσωπικά μας στοιχεία.

Δεν συναντάμε άτομα τα οποία γνωρίσαμε στο Διαδίκτυο.

Είμαστε πάντα ευγενικοί και φιλικοί με τα άτομα τα οποία γνωρίζουμε στο Διαδίκτυο.

### *3) Γονείς και Εκπαιδευτικοί*

**Δυνατότητες**

Το Διαδίκτυο έχει πολλές δυνατότητες τις οποίες μπορούμε να ανακαλύψουμε και να αξιοποιήσουμε. Είτε χρησιμοποιούμε το Διαδίκτυο για ψυχαγωγία, είτε για μάθηση, είτε για επικοινωνία, έχουμε στα χέρια μας εργαλεία και πηγές που μπορούν να μας προσφέρουν δυνατότητες που να ενισχύουν τη ζωή μας στην κοινωνία του 21ου αιώνα.

Η αξιοποίηση του Διαδικτύου και των δυνατοτήτων του έχει ως προϋπόθεση την ορθή χρήση του. Η άγνοια, αλλά και η έλλειψη δεξιοτήτων χρήσης των νέων τεχνολογιών είναι δυνατό σε κάποιες περιπτώσεις να οδηγήσουν σε άβολες καταστάσεις ή ακόμη και σε κάποιο κίνδυνο. Για αυτό και στην ιστοσελίδα αυτή, μετά την ενημέρωση για την κάθε μία από τις σημαντικότερες δυνατότητες του Διαδικτύου ακολουθεί σύντομη αναφορά για πιθανούς κινδύνους από τη χρήση του Διαδικτύου και βασικές εισηγήσεις σε καλές πρακτικές της χρήσης του.

Σκοπός της ενότητας είναι να δώσει ενδεικτικά σημαντικές δυνατότητες του Διαδικτύου, τις προκλήσεις ή/και κινδύνους που μπορεί να προκύψουν από τις δυνατότητες αυτές και βασικές εισηγήσεις αντιμετώπισής τους. Οι αναφορές αυτές έχουν προκύψει από ανασκόπηση της σχετικής βιβλιογραφίας, από τα αποτελέσματα ομαδικών συζητήσεων και μέσα από διαδικασίες, όπως αυτή του δομημένου διαλόγου, στις οποίες συμμετείχαν εκπρόσωποι εμπλεκόμενων φορέων, εκπαιδευτικοί και ψυχολόγοι.

**Κίνδυνοι**

Το Διαδίκτυο είναι ένα δυνατό εργαλείο στα χέρια μας, που όμως αν δεν το χρησιμοποιούμε σωστά μπορεί να εμπερικλείει κινδύνους. Η πρόκληση στο Διαδίκτυο είναι να μπορούμε να αναγνωρίζουμε πιθανούς κινδύνους, να γνωρίζουμε τρόπους πρόληψης και αντιμετώπισης των κινδύνων και να έχουμε επιλογές για αποφυγή τους και τερματισμό τους.

Οι κυριότεροι κίνδυνοι που συνεπάγονται από τη χρήση του Διαδικτύου είναι:

- Ακατάλληλο Περιεχόμενο
- Ανεπιθύμητα Μηνύματα (Spam)
- Αποξένωση
- Αποπλάνηση (Grooming)

- Βίαια Παιχνίδια
- Εθισμός (InternetAddiction)
- Εκφοβισμός (Cyberbullying)
- Επιβλαβείς Συμπεριφορές
- Ηλεκτρονικός Τζόγος
- Ιοί (Virus)
- Παιδική Πορνογραφία
- Παραβίαση Ιδιωτικότητας
- Παραπληροφόρηση (Misinformation)
- Παραποίηση Γλώσσας
- Υποκλοπή Προσωπικών στοιχείων (Phishing)
- Φυσικές Παθήσεις

### *4) Ασφάλεια*

**Προτάσεις αντιμετώπισης των κινδύνων**

Η διάδοση της χρήσης του Διαδικτύου η οποία εξαπλώθηκε, πολύ λογικά, και στο χώρο των εφήβων καθώς και σε πολύ μικρότερες ηλικίες, έφερε μαζί και αρκετούς κινδύνους που σχετίζονται με τη χρήση του. Η μη συνειδητοποιημένη χρήση του Διαδικτύου μπορεί να έχει δυσμενείς επιπτώσεις, όπως: βλάβες στον ηλεκτρονικό υπολογιστή, υποκλοπή προσωπικών πληροφοριών, διαδικτυακό εκφοβισμό (cyberbulling) και εκμετάλλευση από αγνώστους, ανεπιθύμητη αλληλογραφία (spam), εθισμό, αντικοινωνική συμπεριφορά, φυσικές παθήσεις.

Σε παγκόσμια κλίμακα, τα κράτη αναπτύσσουν διάφορες δράσεις για την προστασία των πολιτών τους. Μια από τις κύριες δραστηριότητες είναι η ενημέρωση των πολιτών, τόσο των ίδιων των νέων όσο και των γονέων, για τις συνέπειες (θετικές / κινδύνους) της χρήσης του Διαδικτύου. Μια ομάδα πολιτών στην οποία θα πρέπει να δοθεί ιδιαίτερο βάρος, όσον αφορά την ενημέρωση και τη συνειδητοποίηση της οντότητας του Διαδικτύου είναι οι γονείς. Κάποιοι γονείς μπορεί να αγνοούν πλήρως τους κινδύνους από τη χρήση του Διαδικτύου, ενώ κάποιοι άλλοι να πιστεύουν ότι τους γνωρίζουν όλους.

Στους γονείς θα πρέπει να δοθούν χρήσιμες συμβουλές κατά τη χρήση του Διαδικτύου ως προς:

- την αναζήτηση πληροφοριών,
- τη χρήση των κοινωνικών δικτύων,
- την προστασία του ηλεκτρονικού υπολογιστή,
- την προστασία προσωπικών μας δεδομένων,
- το ηλεκτρονικό εμπόριο,
- τη χρήση του ηλεκτρονικού ταχυδρομείου,
- τη χρήση Webcams,
- την υγιή απασχόληση των παιδιών στο Διαδίκτυο.»

## ΣΧΗΜΑΤΑ ΚΑΙ ΠΙΝΑΚΕΣ

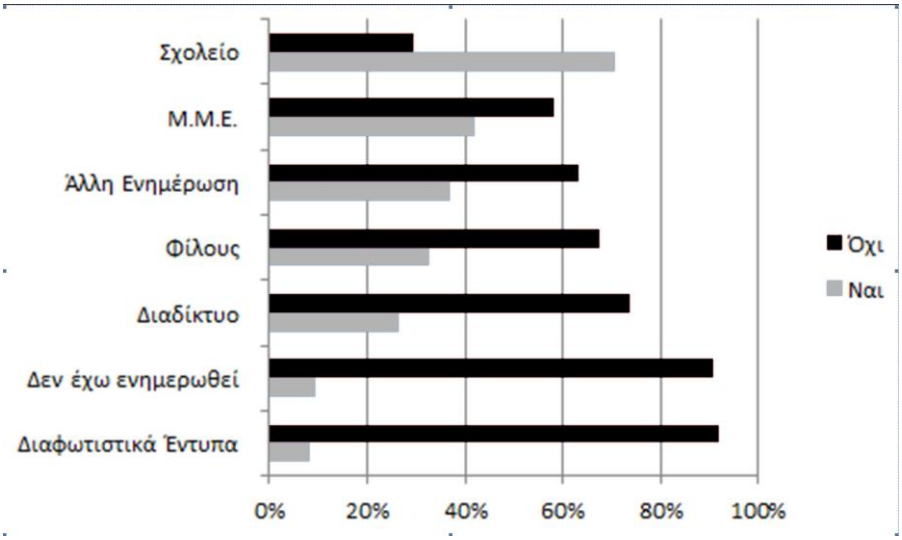
Στους μαθητές δόθηκαν εκατόν είκοσι ένα (121) ερωτηματολόγια μέσω των δασκάλων τους. Δόθηκαν οδηγίες για την συμπλήρωσή τους, τονίστηκε η ανωνυμία και η μη υποχρεωτική συμπλήρωσή τους. Από αυτά επεστράφησαν τα εκατόν δύο (102), ποσοστό συμμετοχής 84%, και αναλύθηκαν τα ενενήντα εννιά (99) επειδή υπήρχαν τρία (3) ερωτηματολόγια κενά. Από τους 99 μαθητές οι 55 ήταν αγόρια (55,6%) και τα υπόλοιπα κορίτσια.

Η έρευνα στην παρούσα στιγμή δεν είναι διερευνητική αλλά περιγραφική και αποτυπώνει τις θέσεις των μαθητών όπως καταγράφηκαν μετά τις δράσεις που αναφέρθηκαν παραπάνω. Στη συνέχεια παρουσιάζονται ορισμένα ποσοτικά ευρήματα με σχήματα και πίνακες, που απαντούν στους στόχους της έρευνας, όπως αυτοί αναφέρονται παραπάνω. Τα ποιοτικά στοιχεία της έρευνας είναι ενθαρρυντικά για το ρόλο που μπορεί να παίξει η σωστή ενημέρωση τόσο από το σχολείο όσο και η οικογένεια. Διαπιστώνεται ότι η πλειοψηφία των μαθητών δεν έχει δεχτεί κανενός είδους παρενόχληση, ούτε έχουν συναντηθεί με κάποιον που γνώρισαν μέσω διαδικτύου. Οι ελάχιστοι μαθητές που συναντήθηκαν με κάποιο άτομο, πήραν μαζί τους ένα φιλικό πρόσωπο είτε έναν φίλο τους είτε μεγαλύτερο αδελφό τους. Τα άτομα που συνάντησαν ήταν είτε μαθητές άλλων σχολείων είτε φίλοι μικρών συγγενών τους. Επίσης, οι ελάχιστοι μαθητές που έδωσαν τα στοιχεία τους μέσω διαδικτύου το έκαναν σε ήδη γνωστά τους άτομα.

**Σχήματα**

Ο ρόλος του σχολείου στη διαμόρφωση στάσεων και αξιών είναι καθοριστικός για τους μαθητές. Κατέχει τον κυρίαρχο ρόλο στην ενημέρωσή τους για τους κινδύνους του διαδικτύου, όπως φαίνεται στο παρακάτω σχήμα. Σε ποσοστό 70,4% οι μαθητές ενημερώθηκαν από το σχολείο είτε από τον δάσκαλό τους είτε από τον δάσκαλο που διδάσκει το μάθημα της Πληροφορικής. Ακολουθούν τα Μ.Μ.Ε ως πηγή ενημέρωσης, οι φίλοι και το διαδίκτυο με την ίδια περίπου συχνότητα, 32,7% και 26,5%, αντίστοιχα, και ένα μεγάλο ποσοστό, 36,&%, ενημερώνεται από άλλη πηγή. Οι περισσότεροι μαθητές στο σημείο αυτό ανέφεραν τους γονείς τους.

**Γράφημα 1**: Πηγές ενημέρωσης των μαθητών για τους κινδύνους του διαδικτύου




**Πίνακες**

Πόσο συχνά χρησιμοποιούν οι μαθητές το διαδίκτυο, τις Ιστοσελίδες κοινωνικής δικτύωσης (Facebook, Hi5, My space..), τα Chat Rooms (MSN, Yahoo) και πόσο συχνά παίζουν διαδικτυακά παιχνίδια, ανταλλάσσουν αρχεία ή ακούνε μουσική και παρακολουθούν ειδήσεις. Όπως φαίνεται παρακάτω οι μικροί μαθητές του δημοτικού σχολείου χρησιμοποιούν πολύ συχνά το διαδίκτυο, είτε ως πηγή ψυχαγωγίας είτε ως μέσο επικοινωνίας. Το σίγουρο είναι ότι οι ελεύθερες ώρες των παιδιών έχουν περιοριστεί στους τοίχους του σπιτιού τους κι όχι σε κάποια αλάνα ή στο γήπεδο του

σχολείου τις απογευματινές ώρες. Ελάχιστοι είναι οι μαθητές του δείγματος που δεν έχουν πρόσβαση στο διαδίκτυο.

**Πίνακας 1: Συχνότητα χρήσης του διαδικτύου (N=99)**

| | Συχνότητα | % |
|---|---|---|
| Κάθε Μέρα | 33 | 33,3 |
| Πάνω από 1 φορά την εβδομάδα | 43 | 43,4 |
| Μια φορά το Μήνα | 6 | 6,1 |
| Λιγότερο από μια φορά το Μήνα | 4 | 4,0 |
| Καθόλου | 13 | 13,1 |
| Σύνολο | 99 | 100,0 |

Οι μαθητές επικοινωνούν, παίζουν και ακούνε μουσική χρησιμοποιώντας τις υπηρεσίες που προσφέρει το διαδίκτυο. Τα ποσοστά είναι συγκλονιστικά στην καθημερινή σχεδόν χρήση των σελίδων κοινωνικής δικτύωσης. Οι κοινωνικές σχέσεις που αναπτύσσονται στην πραγματική ζωή, αντικαθίστανται ή γίνεται προσπάθεια αντικατάστασης από την ηλεκτρονική μορφή αυτών, που επιβάλλουν οι κανόνες του διαδικτύου. Φυσικά η ποιότητα των σχέσεων αυτών είναι πολύ χαμηλές και σε τελευταία ανάλυση οι λίστες των «φίλων» δείχνει τη μοναξιά της εποχής μας. Οι παραπάνω υπηρεσίες λειτουργούν ως «θήρες – θύρες» των επιτήδειων με διττό στόχο αφενός να διευρύνουν τον καταναλωτικό τους πληθυσμό και αφετέρου να θηρεύσουν υποψήφια θύματα.

**Πίνακας 2: Ποσοστά χρήσης υπηρεσιών διαδικτύου από τους μαθητές (N=99)**

| | Κάθε Μέρα | Πάνω από 1 φορά την εβδομάδα | Μια φορά την εβδομάδα | Μια φορά το Μήνα | Λιγότερο από μια φορά το Μήνα | Σύνολο |
|---|---|---|---|---|---|---|
| Chat | 13,6% | 15,3% | 18,6% | 16,9% | 35,6% | 100,0% |
| Κοινωνικής Δικτύωσης | **27,4%** | **29,0%** | 8,1% | 6,5% | 29,0% | 100,0% |
| Διαδικτυακά Παιχνίδια | **36,0%** | **37,2%** | 11,6% | 7,0% | 8,1% | 100,0% |
| Μουσική | **54,5%** | **22,7%** | 13,6% | 6,8% | 2,3% | 100,0% |
| Ανταλλαγή Αρχείων | 13,0% | 13,0% | 10,9% | 13,0% | 50,0% | 100,0% |
| Ειδήσεις | 9,1% | 9,1% | 16,4% | 12,7% | 52,7% | 100,0% |

Η πλειοψηφία των μαθητών, **78,4%,** συνδέεται στο διαδίκτυο από το σπίτι και μόνο ένας στους 4 συνδέεται από το σχολείο. Αυτό δείχνει ότι στο σχολείο υπάρχει έλεγχος και ορθολογική χρήση του διαδικτύου. Είναι θέμα ευθύνης των γονιών να ασχοληθούν και στο σπίτι σοβαρά με την ενημέρωση των παιδιών τους, ενημέρωση που αρκετές φορές δεν έχουν οι ίδιοι (Κέκκερης Γ., Δέλλας Σ., 2005).

| **Πίνακας 3:Σύνδεση μαθητών στο διαδίκτυο** | | Count | Column N % |
|---|---|---|---|
| q4.1 Σύνδεση στο διαδίκτυο από το Σπίτι | Ναι | 76 | **78,4%** |
| | Όχι | 21 | 21,6% |
| q4.2 Σύνδεση στο διαδίκτυο από το Σχολείο | Ναι | 25 | 25,8% |
| | Όχι | 72 | 74,2% |

| | | | |
|---|---|---|---|
| q4.3 Σύνδεση στο διαδίκτυο από το Internet Καφέ | Ναι | 8 | 8,2% |
| | Όχι | 89 | 91,8% |
| q4.4 Σύνδεση στο διαδίκτυο από το Αλλού | Ναι | 17 | 17,5% |
| | Όχι | 80 | 82,5% |

Είναι σημαντική η θέση του υπολογιστή μέσα στο σπίτι. Η πλειοψηφία των μαθητών όπως φαίνεται στον πίνακα 4 συνδέεται στο διαδίκτυο από τον υπολογιστή που βρίσκεται στο σαλόνι. Ωστόσο ένα επίσης μεγάλο ποσοστό μαθητών έχει τον υπολογιστή μέσα στο υπνοδωμάτιό τους. Στην πρώτη περίπτωση μπορούν οι γονείς εύκολα να ασκήσουν έλεγχο σχετικά με τις ιστοσελίδες αλλά και τη συχνότητα εισόδου στο διαδίκτυο (Λαμπροπούλου & Κολεΐδης 2010). Στην δεύτερη, στο υπνοδωμάτιο, ο έλεγχος είναι πλημμελής έως ανύπαρκτος και φανερώνει άγνοια ή και αδιαφορία για μια λελογισμένη χρήση. Οι περισσότερες έρευνες έχουν δείξει τη σημαντικότητα της θέσης του υπολογιστή μέσα στο σπίτι (Ασλανίδου Σ., Οικονόμου Α. 2006).

| **Πίνακας 4: Θέση του υπολογιστή στο σπίτι** | | Count | Column N % |
|---|---|---|---|
| q5.1 Ο υπολογιστής σύνδεσης βρίσκεται Σαλόνι | Ναι | 28 | 28,9% |
| | Όχι | 69 | **71,1%** |
| q5.2 Ο υπολογιστής σύνδεσης βρίσκεται Τραπεζαρία | Ναι | 12 | 12,4% |
| | Όχι | 85 | 87,6% |
| q5.3 Ο υπολογιστής | Ναι | 50 | **51,5%** |

| | | | |
|---|---|---|---|
| σύνδεσης βρίσκεται Υπνοδωμάτιο | Όχι | 47 | 48,5% |
| q5.4 Ο υπολογιστής σύνδεσης βρίσκεται Αλλού | Ναι | 15 | 15,5% |
| | Όχι | 82 | 84,5% |

Οι μαθητές επικοινωνούν με τους συμμαθητές και τους φίλους τους. Επικοινωνούν μαζί τους με σταθερό ή κινητό τηλέφωνο αλλά και μέσα από διάφορες υπηρεσίες του διαδικτύου. Στην πλειοψηφία τους διαθέτουν κινητό τηλέφωνο και το χρησιμοποιούν σε ποσοστό 45,5%. Ο φόρτος των μαθημάτων και οι υποχρεωτικές εξοντωτικές πολλές φορές εξωσχολικές δραστηριότητες, τους αναγκάζουν να μην έχουν τη ζωντανή επαφή που θα ήθελαν με τους φίλους τους στη διάρκεια της ημέρας και έτσι καταφεύγουν στην επικοινωνία μαζί τους μέσω τηλεφώνου, σταθερού ή κινητού.

Με ποιο τρόπο (σταθερό τηλέφωνο, κινητό ή υπολογιστή) επικοινωνούν με τους φίλους τους.

**Πίνακας 5: Τρόποι επικοινωνίας των μαθητών με τους φίλους τους (N=99)**

| | | Συχνότητα | Ποσοστό |
|---|---|---|---|
| SMS | Ναι | 16 | 16,2% |
| | Όχι | 83 | 83,8% |
| Σταθερό Τηλέφωνο | Ναι | 46 | **46,5%** |
| | Όχι | 53 | 53,5% |
| Κινητό Τηλέφωνο | Ναι | 45 | 45,5% |
| | Όχι | 54 | 54,5% |

| | | | |
|---|---|---|---|
| Email | Ναι | 19 | 19,2% |
| | Όχι | 80 | 80,8% |
| Chat Room/Instant Messenger | Ναι | 24 | **24,2%** |
| | Όχι | 75 | 75,8% |
| Άλλο | Ναι | 16 | 16,2% |
| | Όχι | 83 | 83,8% |

Αν έχουν δεχτεί κάποιου είδους παρενόχληση κατά τη χρήση του διαδικτύου και αν γνωρίζουν για την ασφάλεια και τους κινδύνους που κρύβει η χρήση του.

**Πίνακας 6: Επικίνδυνες ενέργειες των μαθητών κάνοντας χρήση του διαδικτύου (N=99)**

| | | Συχνότητα | Ποσοστό |
|---|---|---|---|
| Έχουν ενοχληθεί από κάποιον μέσω του διαδικτύου | Όχι | 90 | 91,8% |
| | Ναι | 8 | **8,2%** |
| Έχουν συναντήσει κάποιον που γνώρισαν μέσω του διαδικτύου | Όχι | 86 | 87,8% |
| | Ναι | 12 | **12,2%** |
| Έχουν δώσει κάποια προσωπικά στοιχεία σε κάποιον που γνώρισες στο διαδίκτυο | Όχι | 87 | 89,7% |
| | Ναι | 10 | **10,3%** |

Η πλειοψηφία των μαθητών δεν έχει δεχτεί κανενός είδους παρενόχληση από το διαδίκτυο, δεν έχουν δώσει τα προσωπικά τους στοιχεία σε κάποιον και δεν έχουν συναντήσει κάποιον που έχουν γνωρίσει από το διαδίκτυο. Από τους 12 μαθητές που δήλωσαν ότι έχουν συναντήσει κάποιον μέσω διαδικτύου μόνο οι τέσσερεις (4/12)

ανέφεραν ότι στην συνάντηση αυτή τους συνόδευε και κάποιος γνωστός. Οι υπόλοιποι συναντήθηκαν μόνοι τους και το πιο ανησυχητικό είναι η δήλωση ενός μαθητή ότι «ντράπηκε» να μιλήσει στους γονείς του για την παρενόχληση που δέχτηκε. Υπάρχει γόνιμο έδαφος από το σχολείο και τους γονείς στην κατεύθυνση της ενημέρωσης των παιδιών τους για το τι πραγματικά είναι και τι μπορεί να κρύβεται στο «σερφάρισμα» αθώων φαινομενικά σελίδων του διαδικτύου.

**Πίνακας 7: Πηγές ενημέρωσης των μαθητών για τους κινδύνους του διαδικτύου (N=99)**

| | | Συχνότητα | Ποσοστό |
|---|---|---|---|
| Σχολείο | Ναι | 69 | **70,4%** |
| | Όχι | 29 | 29,6% |
| Μ.Μ.Ε. | Ναι | 41 | 41,8% |
| | Όχι | 57 | 58,2% |
| Φίλους | Ναι | 32 | 32,7% |
| | Όχι | 66 | 67,3% |
| Διαδίκτυο | Ναι | 26 | 26,5% |
| | Όχι | 72 | 73,5% |
| Διαφωτιστικά Έντυπα | Ναι | 8 | 8,2% |
| | Όχι | 90 | 91,8% |
| Άλλη Ενημέρωση | Ναι | 36 | 36,7% |

| | | | |
|---|---|---|---|
| | Όχι | 62 | 63,3% |
| Δεν έχω ενημερωθεί | Ναι | 9 | 9,2% |
| | Όχι | 89 | 90,8% |

Τον κυρίαρχο ρόλο του σχολείου ως πηγή ενημέρωσης των μαθητών για τους κινδύνους του διαδικτύου, έρχεται να ενισχύσει και ο πίνακας 7. Οι εκπαιδευτικοί ενημερώνουν και υποδεικνύουν τρόπους ασφαλούς πλοήγησης στο διαδίκτυο. Αποδίδουν στον υπολογιστή και στο διαδίκτυο τον πραγματικό τους ρόλο, του γνωστικού εργαλείου το οποίο δρα υποβοηθητικά στην κατάκτηση της γνώσης.

**7. Συμπεράσματα**

Συνοψίζοντας την εργασία μας, θα αναφερθούμε στα κυριότερα σημεία της και στα συμπεράσματα τα οποία εξάχθηκαν.

Έτσι λοιπόν ορίζοντας εν συντομία το τι σημαίνει ασφάλεια στο διαδίκτυο εννοούμε την ορθή χρήση του με βάση κανόνες, γνώση και ενημέρωση των κίνδυνων και τρόπων αντιμετώπισης τους, καθώς και λήψη μέτρων προστασίας κατά την πλοήγηση. Είναι απαραίτητη η ασφαλής πλοήγηση στο διαδίκτυο διότι χρησιμοποιείται συχνά και πολύ τόσο από παιδιά όσο και από εφήβους, δηλαδή από ευαίσθητες ομάδες πληθυσμού, οι οποίοι εκτίθενται σε σοβαρούς κινδύνους και έρχονται σε επαφή ή εμφανίζουν οι ίδιοι ως συμπτώματα έντονη αντικοινωνική και βίαιη συμπεριφορά δηλαδή εκφοβισμό, παρενόχληση και απειλές. Αυτό που αξίζει να σημειωθεί είναι η άγνοια που έχουν τόσο οι γονείς όσο και τα παιδιά για τους κινδύνους που υπάρχουν στο διαδίκτυο.

Οι στάσεις απέναντι στη χρήση του διαδικτύου διαμορφώνονται σε τρεις άξονες: την στάση των παιδιών, των γονέων και των εκπαιδευτικών. Όσον αφορά στα παιδιά, αντιμετωπίζουν συχνά ακατάλληλο διαδικτυακό υλικό ενώ δεν ξέρουν να πλοηγηθούν ασφαλώς με αποτέλεσμα να αισθάνονται ανασφάλεια κατά την πλοήγησή τους. Από την άλλη πλευρά, σύμφωνα με έρευνες οι γονείς πιστεύουν ότι τα παιδιά τους είναι ανασφαλή στο διαδίκτυο ενώ ταυτόχρονα θέτουν ένα αυστηρό πλαίσιο ελέγχου προσπαθώντας να τα προστατέψουν. Η έλλειψη χρόνου καθώς και

το φοβικό σύνδρομο για την τεχνολογία που τους διακατέχει κάνουν το ψηφιακό χάσμα μεταξύ γονιών και παιδιών ακόμα μεγαλύτερο και την μεταξύ τους επικοινωνία δυσκολότερη. Τέλος, οι εκπαιδευτικοί αναφέρουν ότι δεν τους παρέχονται τα κατάλληλα εργαλεία για να προάγουν την ασφάλεια στο διαδίκτυο μέσα στη σχολική τάξη και να διδάξουν τους μαθητές να πλοηγούνται με ασφάλεια στο διαδίκτυο.

Μια άλλη μεγάλη ενότητα με την οποία ασχοληθήκαμε είναι οι κίνδυνοι του διαδικτύου. Κωδικοποιώντας τους σε κατηγορίες έχουμε τους κινδύνους κατά την ηλεκτρονική αλληλογραφία δηλαδή τα κακόβουλα λογισμικά, τους ιούς, τους δούρειους ίππους και τα «σκουλήκια». Ακόμα, όσον αφορά στην ηλεκτρονική αλληλογραφία, χαρακτηρίζεται ως απρόκλητη, εμπορική, μαζική ενώ οι ηλεκτρονικές απάτες μέσω της αλληλογραφίας που μπορεί να σημειωθούν, είναι η νιγηριανή επιστολή το ισπανικό λόττο και τα μηνύματα απατηλού περιεχομένου. Κίνδυνοι σημειώνονται και κατά την άμεση συνομιλία, με σοβαρότερους: την αποπλάνηση ανηλίκου και την ηλεκτρονική παρενόχληση. Ακόμα, τα βίαια ηλεκτρονικά παιχνίδια και η πολύωρη ενασχόληση των παικτών-χρηστών με αυτά έχουν ως αποτέλεσμα την εμφάνιση αντικοινωνικής συμπεριφοράς. Ακόμα ένας κίνδυνος είναι η παραπληροφόρηση που υπάρχει στο διαδίκτυο διότι οι πληροφορίες συνεχώς αυξάνονται και η ορθότητά τους παραμένει ανεξέλεγκτη. Μια άλλη παγίδα είναι ο ηλεκτρονικός τζόγος με τον οποίο όσοι ασχολούνται και πέφτουν θύματα, εμφανίζουν κατάθλιψη και εξαρτήσεις στη χρήση ουσιών και κατανάλωση αλκοόλ. Τέλος κατά το διαμοιρασμό αρχείων χρειάζεται ιδιαίτερη προσοχή διότι εγκυμονείται ο κίνδυνος τα προσωπικά δεδομένα (αριθμοί πιστωτικών καρτών, φορολογικά δεδομένα κ.α.) του καθενός να χρησιμοποιηθούν από αγνώστους.

Στα ελληνικά δεδομένα και σύμφωνα με έρευνα που έγινε σε μαθητές της Στ τάξης Δημοτικού Σχολείου στο Νομό Αχαΐας τα κυριότερα σημεία που εντοπίστηκαν είναι τα εξής: οι μαθητές συνδέονται στο ίντερνετ κατά κύριο λόγο από το σπίτι ενώ οι πηγές από τις οποίες ενημερώνονται για τους κινδύνους του διαδικτύου είναι καταρχάς το σχολείο και ακολουθούν τα Μέσα Μαζικής Ενημέρωσης. Οι κύριες υπηρεσίες που χρησιμοποιούν είναι περισσότερο η μουσική, μετά τα ηλεκτρονικά παιχνίδια και τέλος τα μέσα κοινωνικής δικτύωσης. Σχετικά με τη συχνότητα χρήσης του διαδικτύου, οι μισοί μαθητές μπαίνουν πάνω από μια φορά την εβδομάδα ενώ αρκετοί το επισκέπτονται καθημερινά. Το ευχάριστο που προκύπτει από την έρευνα

είναι ότι μικρό ποσοστό μαθητών προβαίνει σε επικίνδυνες ενέργειες κατά τη χρήση διαδικτύου.

Άρα, τα παιδιά αντιμετωπίζουν ποικίλους κινδύνους στο διαδίκτυο αλλά υπάρχουν τρόποι παρέμβασης που δομούνται σε τρεις άξονες. Υπάρχουν παιδαγωγικοί τρόποι παρέμβασης με τους οποίους γονείς και δάσκαλοι μπορούν να προστατεύσουν τα παιδιά. Οι γονείς μπορούν να συζητούν, να ενημερώνονται και να επαγρυπνούν διαρκώς, να παρακολουθούν σεμινάρια και να προσπαθούν να έχουν ουσιαστική επικοινωνία με τα παιδιά. Επίσης, οι εκπαιδευτικοί καλό θα είναι να συζητούν με τους μαθητές, να δίνουν λίστα με προτεινόμενες σελίδες, να τους επιβλέπουν κατά τη χρήση του διαδικτύου και να διδάσκουν τους βασικούς κανόνες ασφαλούς χρήσης διαδικτύου. Επίσης, μπορούν να χρησιμοποιούν τα παιχνίδια ρόλων και να αξιοποιούν διδακτικά σενάρια. Όσον αφορά τους τεχνολογικούς τρόπους παρέμβασης αυτοί είναι τα συστήματα φιλτραρίσματος και γονικού ελέγχου, οι μηχανές αναζήτησης και φυλλομετρητές για παιδιά, η εγκατάσταση προγραμμάτων προστασίας από ιούς και τειχών προστασίας (firewall) καθώς και τα λογισμικά αντικατασκοπίας, ηλεκτρονικού ψαρέματος και τα φίλτρα για ενοχλητική αλληλογραφία (spam) ενώ η χρήση υδατογραφήματος προστατεύει τα προσωπικά δεδομένα στα κοινωνικά δίκτυα. Τέλος, η παρέμβαση της πολιτείας μπορεί να γίνει με τη δίωξη ηλεκτρονικού εγκλήματος, τη γραμμή safeline , το δίκτυο inhope και την ιστοσελίδα saferinternet.

## 8. Πώς εργαστήκαμε;

Στην ενότητα αυτή θα παρουσιαστεί αναλυτικά ο τρόπος με τον οποίο εργαστήκαμε. Καταρχάς χρησιμοποιήσαμε την τεχνική του καταιγισμού ιδεών ώστε να διευκολυνθεί η έναρξη της εργασίας. Αναλυτικότερα λοιπόν, ο πρώτος μας στόχος ήταν να συλλέξουμε το υλικό με το οποίο θα ασχολούμασταν και θα αποτελούσε τον σκελετό της εργασίας μας δηλαδή άρθρα σε ελληνικά και ξένα περιοδικά, εργασίες και δημοσιεύσεις σε συνέδρια, διδακτορικές διατριβές, δημοσιεύσεις σε έγκυρες ιστοσελίδες αλλά και εποπτικό υλικό όπως εικόνες, βίντεο και παιχνίδια.

Στην συνέχεια, ακολούθησε ο καταμερισμός της εργασίας μεταξύ των μελών της ομάδας μας. Αρχικά αφού διαβάστηκε από όλους το θέμα σε διάστημα μιας

εβδομάδας, στην συνέχεια η εργασία μοιράστηκε με βασικό κριτήριο τα ενδιαφέροντα και τις ειδικές γνώσεις του καθενός από τα μέλη της ομάδας ενώ η συνεργασία πραγματοποιήθηκε με κοινή απόφαση και απόλυτα ελεύθερες και δημοκρατικές διαδικασίες.

Όσον αφορά στη διάρθρωση και τη συγγραφή της εργασίας, μελετήθηκε το υλικό σε μια προσπάθεια κατανόησης του θέματος μέσα από τη μελέτη της βιβλιογραφίας και ακολούθησε επεξεργασία και σύνθεση των πηγών. Στην συνέχεια, καταγράφηκαν τα κύρια σημεία της εργασίας μας και ακολούθησε η δημιουργία σχεδιαγράμματος. Αξίζει στο σημείο αυτό να αναφερθεί ότι ως εργαλεία χρησιμοποιήσαμε ένα έγγραφο google doc στο οποίο σημείωνε ο καθένας τα διάφορα τμήματα του σχεδιαγράμματος καθώς και οποιεσδήποτε αλλαγές ή απορίες προέκυπταν στην πορεία ενώ για τις συνεννοήσεις μεταξύ των μελών της ομάδας χρησιμοποιήθηκε κατά κόρον η ηλεκτρονική αλληλογραφία.

Τέλος για την παρουσίαση της εργασίας ακολουθήσαμε την εξής διαδικασία. Ο καθένας ετοίμασε το δικό του power point και τα διάφορα τμήματα τα ενώσαμε μεταξύ τους σχηματίζοντας μια σύνθεση όλων των επιμέρους σκελετών της εργασίας δημιουργώντας ένα ομαδικό power point. Στην συνέχεια, ακολούθησε συνάντηση και συζήτηση με τον επιβλέποντα καθηγητή για όποιες απορίες είχαν προκύψει και για ορισμένες διορθώσεις και τέλος κάναμε την τελική παρουσίαση της εργασίας μας στους συμφοιτητές μας.

Από τη μεταξύ μας συνεργασία και επικοινωνία αξίζει να αναφερθεί το γεγονός ότι το κλίμα της ομάδας ήταν θετικό και αυτό ενθάρρυνε την αποδοτικότητά μας και την ανάπτυξη πρωτοβουλιών ενώ στο κλείσιμο της εργασίας μας, ευχή όλων αποτέλεσε μια επόμενη συνεργασίας.

**Βιβλιογραφία**

Allen, B., & Lauterbach, D. (2007). Personality characteristics of adult survivors of childhood trauma. *Journal of Traumatic Stress*, 20, 587–595.

http://dx.doi.org/10.1002/jts.20195.

Anastasiades, P. S & Vitalaki, E. (2011), Promoting Internet Safety in Greek Primary Schools: the Teacher's Role, *Educational Technology & Society*, Volume 14 Number 2, pp. 71-80

Avgoulea, M., Bouras, C., Paraskevas, M. & Stathakopoulos, G., (2003) Policies for content filtering in educational networks: the case of Greece, *Telematics and Informatics*, 20, pp. 71–95,

Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology*, 31, pp. 439–447. http://dx.doi.org/10.1016/j.appdev.2010.07.005.

Bagley, C., & Mallick, K. (2000). Prediction of sexual, emotional and physical maltreatment and mental health outcomes in a longitudinal cohort of 290 adolescent women. *Child Maltreatment*, 5, pp. 218–226.

http://dx.doi.org/10.1177/1077559500005003002.

Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology*, 31, pp. 439–447. http://dx.doi.org/10.1016/j.appdev.2010.07.005.

Berger, L. M., Slack, K. S., Waldfogel, J., & Bruch, S. K. (2010). Caseworker-perceived caregiver substance abuse and child protective services outcomes. *Child Maltreatment*, 13, pp. 199–210.

Brå (The Swedish National Council for Crime Prevention) (2007). *Vuxnas Sexuella Kontakter med Barn via Internet* [Adults' sexual contacts with children online]. Brå-rapport 2007:11. Stockholm: Swedish National Council for Crime Prevention.

Bradley, R., Heim, A., &Westen, D. (2005). Personality constellations in patients with a history of childhood sexual abuse. *Journal of Traumatic Stress*, 18, pp. 769–780.http://dx.doi.org/10.1002/jts.20085

Can J. (2001) Children's Charities' Coalition for Internet Safety

Charlton, J.P., and Danforth, D.W., 2007, Distinguishing addiction and high engagement in the context of online game playing, *Computers in Human Behavior*, 23(3), pp. 1531–1548.

Children's Bureau and Department of Health and Human Services (2010). *Child maltreatment*. Retrieved July 3, 2012 via:

http://www.acf.hhs.gov.programs/cb/pubs/cm10/cm10.pdf

Child Exploitation and Online Protection Centre (2008). *An analysis of victim typologies and indicators of vulnerability*. Unpublished

Chou, C. & Peng, H. (2011), Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience, *The Internet and Higher Education*, Volume 14, Issue 1, January 2011, pp. 44–53

Dombrowski, S. C., LeMasney, J.W., Ahia, C. E., & Dickson, S. A. (2004). Protecting children from online sexual predators: Technological, psychoeducational, and legal considerations. *Professional Psychology: Research and Practice*, 35, pp. 65–73. http://dx.doi.org/10.1037/0735-7028.35.1.65.

Domon K., Yamazaki, N. (2004), Unauthorized file-sharing and the pricing of digital content, Economics Letters, 85, pp. 179–184

Elmore, G. M., & Huebner, E. S. (2010). Adolescents' satisfaction with school experiences:Relationships with demographics, attachment relationships, and school engagement behavior. *Psychology in the Schools*, 47, pp. 525–537. http://dx.doi.org/10.1002/pits.20488.

European Online Grooming ProjectWebster, S., Davidson, J., Bifulco, A., Gottschalk, P.,Caretti, V., Pham, T., & Grove-Hills, J. (2010). *European Online Grooming Project scoping report. European Union* (Retrieved on 5th May 2011, via: http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/EOGP-Projectscoping-report.pdf.)

Ey, L.-A. & Cupit, C. G. (2011). Exploring young children's understanding of risks associated with Internet usage and their concepts of management strategies, *Journal of Early Childhood Research*, 9, pp. 53-65

Finkelhor, D., Ormrod, R., Turner, H., & Hamby, S. L. (2005). The victimization of children and youth: A comprehensive, national survey. *Child Maltreatment*, 10, pp. 5–25. http://dx.doi.org/10.1177/1077559504271287.

Finkelhor, D., Ormrod, R., Turner, H., & Holt, M. (2009). Pathways to poly-victimization. *Child Maltreatment*, 14, pp. 316–329.

http://dx.doi.org/10.1177/1077559509347012.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A. & Morrison, S. (2006), Safety in Cyberspace: Adolescents' Safety and Exposure Online, *Youth Society*, 38 pp. 135-154

Helweg-Larsen, K., Schütt, N., & Larsen, H. B. (2011). Predictors and protective factors for adolescent internet victimization: Results from a 2008 nationwide Danish youth survey. Acta Paediatrica, 101, pp. 533–539. http://dx.doi.org/10.1111/j.1651-2227.2011.02587.x.

Lloyd, J., Doll H., Hawton, K., Dutton W. H., Geddes J. R., Goodwin G. M. & Rogers, R. D. (2010). How Psychological Symptoms Relate to Different Motivations for Gambling: An Online Study of Internet Gamblers, *BIOL PSYCHIATRY* 68: pp. 733–740

Kenny, M. C., &McEachern, A. G. (2000). Racial, ethnic and cultural factors of childhood sexual abuse: A selected review of the literature. *Clinical Psychology Review*, 20, pp. 905–922. http://dx.doi.org/10.1016/S0272-7358%2899%2900022-7.

Kyas, O. (1997). *Internet Security- Risk Analysis, Strategies and Firewalls*. Verlag: Coriolis Group.

Liau, A. K.& Khoo, A. & Ang, P. H. (2008), Parental Awareness and Monitoring of Adolescent Internet Use, *Current Psychology* (2008) 27, pp.217–233

Livingstone, S., & Bober, M. (2005). *UK children go online*. Swindon, UK: Economic and Social Research Council (ESRC).

Livingstone, S., Bober, M., & Helsper, E. J. (2005). Active participation or just more information? Young people's take up of opportunities to act and interact on the internet.Information, *Communication and Society*, 8, pp. 287–314.

http://dx.doi.org/10.1080/13691180500259103

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2011b). *EU kids online*, September 2011.Retrieved on 31st May 2012 via: www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20kids%2011%20(2009–11)/EUKidsOnlineIIIReports/Final%20report.pdf

Maykut, P. & Morehouse, R. (1994). *Beginning Qualitative Research: a Philosophic and Practical Guide*. London: The Falmer Press.

McGee, H., Garavan, R., Barra, M., Byrne, J., & Conroy, R. (2002). *The Savi Report: Sexual abuse and violence in Ireland. A national study of Irish experiences, beliefs and attitudes concerning sexual violence.* Dublin: Liffey Press.

Mitchell, K. J., Finkelhor, D. & Wolak, J. (2001), Risk Factors for and Impact of Online Sexual Solicitation of Youth, *JAMA*, June 20, 2001—Vol 285, No. 23, pp. 3011-3014

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Online requests for sexual pictures from youth: Risk factors and incident characteristics. *Journal of Adolescent Health*, 41, pp. 196–203. http://dx.doi.org/10.1016/j.jadohealth.2007.03.013.

O'Leary, P. J., & Barber, J. (2008). Gender differences in silencing following childhood sexual abuse. *Journal of Child Sexual Abuse*, 17, pp. 133–143. http://dx.doi.org/10.1080/10538710801916416.

Olson, L. N., Daggs, J. L., Ellevold, B. L., & Rogers, T. K. K. (2007). Entrapping the innocent: Toward a theory of child sexual predators' luring communication. *Communication Theory*, 17, pp. 231–251. http://dx.doi.org/10.1111/j.1468-2885.2007.00294.x.

Pereda, N., Guilera, G., Forns, M., & Gomez-Benito, J. (2009). The prevalence of child sexual abuse in community and student samples: A meta-analysis. *Clinical Psychology Review*, 29, pp. 328–338. http://dx.doi.org/10.1016/j.cpr.2009.02.007.

Peter, J., Valkenburg, P. M., & Schouten, A. P. (2005). Developing a model of adolescent friendship formation on internet. *Cyberpsychology & Behavior*, 8, pp. 423–430. http://dx.doi.org/10.1089/cpb.2005.8.423.

Söderström, S. (2009). The significance of ICT in disabled youth's identity negotiations.Scandinavian, *Journal of Disability Research*, 11, pp. 131–144. http://dx.doi.org/10.1080/15017410902830587.

Sorenson, K., & Bodanovskaya, Z. (2012). Children with disabilities. In M. Ainsaar, & L.Lööf (Eds.), *Online behaviour related to child sexual abuse: Literature report*.

Soo, D., & Bodanovskaya, Z. (2012). Risk factors of becoming a victim of internet related sexual abuse. In M. Ainsaar, & L. Lööf (Eds.), *Online behaviour related to child sexual abuse: Literature report. European Union and Council of the Baltic Sea States:ROBERT Project (*Risktaking Online Behaviour Empowerment Through Research and Training).

Spielhofer, T. (2010). *Children's online risks and safety: A review of the available evidence*. Prepared for the UK Council for Child Internet Safety. London: The National Foundation for Education Research.

Stahl, C. & Fritz, N. (2002), Internet safety: adolescents' self-report, *Journal of Adolescent Health*, Volume 31, Issue 1, July 2002, pp. 7–10

Stanley, J. (2001). Child abuse and the internet. *Child Abuse Prevention Issues*, 15, pp. 1–18.

Suldo, S. M., & Huebner, E. S. (2006). Is extremely high life satisfaction during adolescence advantageous? *Social Indicators Research*, 78, pp. 179–203. http://dx.doi.org/10.1007/s11205-005-8208-2.

Sun, P., Unger, J. B., Palmer, P. H., Gallaher, P., Chou, C., Baezconde-Garbanati, L., et al.(2005). Internet accessibility and usage among urban adolescents in Southern California: Implications for web-based health research. *CyberPscyhology and Behavior*, 8, pp. 441–453. http://dx.doi.org/10.1089/cpb.2005.8.441.

Susan Keith and Michelle E. Martin,(2005), Cyber-Bullying: Creating a Culture of Respect in a Cyber world.

Suseg, H., Skevik Grødem, A., Valset, K., & Mossige, S. (2008). *Seksuelle krenkelser via nettet hvor stort er problemet?* (Sexual harassment on the internet — How great is the problem?). Retrieved 30th May 2012 via: www.nova.no/asset/3525/1/ 3525_1.pdf

Valcke M., De Wever B., Van Keer H., Schellens T., (2011), Long-term study of safe Internet use of young children, *Computers & Education*, 57, pp. 1292–1305

Valcke, M., Bonte, S., De Wever, B., Rots, I. (2010), Internet parenting styles and the impact on Internet use of primary school Children, *Computers & Education*, 55, pp. 454-464

Valcke, M., Schellens, T., Van Keer, H., Gerarts, M. (2007), 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

Verheecke E. (2008) *Enquête auprès des jeunes scolarisés à Genève sur l'usage des nouvelles technologies*

(http://www.actioninnocence.org/suisse/Fichiers/ModeleContenu/294/Fichiers/Enqu%C3%AAte%20%20Usages%20et%20m%C3%A9susages%202008.pdf)

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P.,Caretti, V., Pham, T., & Grove-Hills, J. (2012). *European Online Grooming Project final report*. European Union (Retrieved on 21st April 2012 via: http://www.european-online-grooming-project.com/)

Wishart, J. (2004), Internet safety in emerging educational contexts, *Computers & Education*, 43, pp. 193–204

Wishart J.M., Oades C.E., Morris M., (2007) Using online role play to teach internet safety awareness, *Computers & Education*, 48 , pp. 460–473

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online "predators" and their victims: Myths, realities and implications for prevention and treatment. American Psychologist, 63, 111–1128. http://dx.doi.org/10.1037/0003-066X.63.2.111.

Yancey, C. T., & Hansen, D. J. (2010). Relationship of personal, familial, and abuse-specific factors with outcome following childhood sexual abuse. *Aggression and Violent Behavior*, 15, pp. 410–421. http://dx.doi.org/10.1016/j.avb.2010.07.003

Ybarra, M. (2004), Linkages between Depressive Symptomatology and Internet Harassment among Young Regular Internet Users, *CYBERPSYCHOLOGY & BEHAVIOR*, Volume 7, Number 2, 2004, pp. 247-257

Youn. S. (2008), Parental Influence and Teens' Attitude toward Online Privacy Protection, *Journal of Consumer Affairs*, Volume 42, Issue 3, pp. 362–388,

Zigomitros, A., Papageorgiou, A., & Patsakis, K. (n.d.). Social network content management through watermarking.

Ασλανίδου Σ., Οικονόμου Α. (2006). *Νέοι και διαδίκτυο: χρήση και πρακτικές στο σχολείο,* 5ο Συνέδριο ΕΤΠΕ αναρτήθηκε από

*http://www.etpe.gr/files/proceedings/22/1234434966_5%20etpe%2042,4-431.pdf*

Δημητρακάκης, Κ., Σοφός, Α., Βαλμάς, Θ. (2011), Η προστασία των μαθητών στο Διαδίκτυο από την οπτική των εκπαιδευτικών, *στα πρακτικά του 2ου πανελληνίου συνεδρίου για την ένταξη και χρήση των ΤΠΕ στην εκπαιδευτική διαδικασία*, σσ. 215-228, Πάτρα 28-30/4/2011

Ελληνικό Κέντρο Ασφαλούς διαδικτύου (2007)

Ηλιάδη Α., Ασφάλεια στο διαδίκτυο, 1ο Εκπαιδευτικό Συνέδριο «Ένταξη και Χρήση των ΤΠΕ στην Εκπαιδευτική Διαδικασία»

Κατερέλος Ι. & Παπαδόπουλος. Π. (*2009*) *Οι έφηβοι* και το *Ιντερνέτ*., Αθήνα: Εκδόσεις Καστανιώτης.

*Κέκκερης, Γ.& Δέλλας, Σ., (2003). Δράσεις για την ασφαλέστερη χρήση του Διαδικτύου στο διεθνή και ευρωπαϊκό χώρο σαν αναφορά για την ελληνική εκπαίδευση, 6ο Πανελλήνιο Συνέδριο με διεθνή συμμετοχή «Διδακτική των Μαθηματικών και Πληροφορική στην Εκπαίδευση» Πανεπιστήμιο Θεσσαλίας, Βόλος.*

Κέκκερης Γ., Δέλλας Σ. (2005). *Υπεύθυνη και Ασφαλής Χρήση του Διαδικτύου: μια Διδακτική Πρόταση,* Πρακτικά 3ου Συνεδρίου των εκπαιδευτικών για την *Αξιοποίηση των ΤΠΕ στη διδακτική πράξη*, Σύρος.

Λάζος, Γ. (2001). *Πληροφορική και Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.

Λαμπροπούλου & Κολεΐδης (2010). *Χρήση ιστοσελίδων κοινωνικής δικτύωσης από μαθητές Γυμνασίου,* Στο Β. Καλτσάκης, Γ. Σαλονικίδης, Μ. Δοδοντσής (επιμ.) Πρακτικά 2ου Πανελληνίου Εκπαιδευτικού Συνεδρίου Ημαθίας *«Ψηφιακές και Διαδικτυακές αφαρμογές στην εκπαίδευση»,* (σελ. 1688-1696), http://www.ekped.gr/praktika10/web/151.pdf

Μαναριώτης, Παπαγεωργίου, Λαβίδας, (2013). *Ασφάλεια στο διαδίκτυο: Έρευνα στην 4η Περιφέρεια Αχαΐας*, 3ο Συνέδριο ΕΕ, Πρακτικά Συνέδρων, Αθήνα.

Νικολαΐδης, Χ. (1999). *Η σκοτεινή πλευρά του Internet*. Αθήνα: Anubis.

Οδηγός ασφαλούς χρήσης διαδικτύου για γονείς και παιδιά, Microsoft

Πανσεληνάς, Γ. (2010). *Ασφαλής χρήση του Διαδικτύου – Αποτελεσματικές διδακτικές παρεμβάσεις και ο ρόλος του εκπαιδευτικού Πληροφορικής.* 4ο Πανελλήνιο Συνέδριο Καθηγητών Πληροφορικής. Σέρρες 2010.

Παπαλεωνίδας Α., Καλτσίδης Χ., Ναλμπάντη Θ. (2011), Στάσεις μαθητών της «ψηφιακής τάξης» σε θέματα Διαδικτυακής συμπεριφοράς I-TEACHER.GR με ISSN 1792-4146

http://users.sch.gr/papaleon/images/pdfs/i-teacher.gr.pdf

Παρασκευόπουλος (1993). *Μεθοδολογία Επιστημονικής Έρευνας. Τόμοι Α΄ & Β΄.* Αθήνα: Ιδίου.

Συκιώτου, Α. (2009). *Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης*. Αθήνα: Αντ. Ν. Σάκκουλας.

Τρυφιάτης Ι., Στιβακτάκη Μ. (2009). *Οι κίνδυνοι στο διαδίκτυο*: Μια συνεργατική δραστηριότητα στο πλαίσιο της δράσης «SaferInternet», 1ο Εκπαιδευτικό Συνέδριο *«Ένταξη και χρήση των ΤΠΕ στην εκπαιδευτική διαδικασία»*, Βόλος

Τσουραμάνης, Χ. (2005*). Ψηφιακή Εγκληματικότητα - Η (αν)ασφαλής όψη του διαδικτύου*. Αθήνα: Β.Ν. Κατσαρού.

**Διαδικτυακές πηγές**

*31ο Δημοτικό Σχολείο Περιστερίου-Ασφάλεια στο Διαδίκτυο*. (n.d.). Ανάκτηση από http://eclass31.weebly.com/alphasigmaphi940lambdaepsiloniotaalpha-sigmatauomicron-deltaiotaalphadelta943kappatauupsilonomicron-2.html#.UcaWoztM9Iy

Action Innocence (2009)

http://www.actioninnocence.org/suisse/Fichiers/ModeleContenu/824/Fichiers/ZMDN-2012-2013.pdf προσπελάστηκε στις 20/4/13

Belsey, Bill. (2004). Cybcrlmlhfiu^.ca. Retrieved July 31, 2004, from Web site: www.cyberbullying.ca

*Cyber Kids*. (n.d.). Ανάκτηση από http://www.cyberkid.gov.gr/

*SafeLine*. (n.d.). Ανάκτηση από http://www.safeline.gr/poioi-eimaste/inhope

*Safer Internet*. (n.d.). Ανάκτηση από http://www.saferinternet.gr/ (Περιοδικό,Τεύχος 11ο: Μάρτιος 2007).

*Δίκτυο INHOPE*. (n.d.). Ανάκτηση από http://www.inhope.org/gns/home.aspx

*Δίωξη ηλεκτρονικού εγκλήματος*. (n.d.). Ανάκτηση από http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1763&Itemid=378

*Δωρεάν λογισμικά - sxoleio.eu*. (n.d.). Ανάκτηση από http://sxoleio.eu/

Συνθήκη των Ηνωμένων Εθνών για τα Δικαιώματα του Παιδιού www.unicef.gr/symbs.php, (N.243/1990)

http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (Νόμος του 2004 (22(III)/2004): Ο περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου (Κυρωτικός).Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου, Βουδαπέστη 23.11.2001). (Convention on Cybercrime)

http://eprints.lse.ac.uk/39351/1/EU_kids_online_final_report_%5BLSERO%5D.pdf

http://europa.eu.int/information_society/activities/sip/docs/pdf/reports/eurobarometer_EU25_highlights.pdf.

http://europa.eu.int/saferinternet

(Ευρωπαϊκή Επιτροπή, Ευρωβαρόμετρο, 2005).

http://www.appdata.com

http://ist.mit.edu/security/malware (πρόσβαση στις 9/4/2013)

http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_content&perform=view (πρόσβαση στις 9/4/2013)

http://www.ekato.org/gr/

http://www.emeraldinsight.com/journals.htm?articleid=17038666&show=abstract

http://www.mlsi.gov.cy/mlsi/sws/sws.nsf/dmllegislation_gr/dmllegislation_gr?OpenDocument&Start=1&Count=1000&Expand=1 (N.3064/2002: Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου, Βουδαπέστη Ο περί Καταπολέμησης της Εμπορίας Προσώπων και περί Σεξουαλικής Εκμετάλλευσης Ανηλίκων, Νόμος του 2000.)

http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104 (πρόσβαση στις 9/4/2013)

http://www.observatory.gr/page/default.asp?la=1&id=183&pl=110&pk=294&ap=101 (Παρατηρητήριο για την Κοινωνία της Πληροφορίας: (2007). Ετήσια μέτρηση των δεικτών των σχεδίων δράσης eEurope & i2010, για το 2006)

http://www.paidorama.com

http://www.pi.ac.cy/InternetSafety

http://www.pi.ac.cy/InternetSafety/drastiriotites_simsafety.html

www.safeline.gr

http://www.safeweb.org.cy

http://www.sciencedirect.com/science/article/pii/S0360131510000436

http://www.sch.gr/, (Πανελλήνιο Σχολικό Δίκτυο)

www.sch.gr/safe. (Ασφαλής πλοήγηση στο διαδίκτυο).

http://www.securitymanager.gr/it_security/protection_article.php?id=5&set=1&title=%C3%E5%ED%E9%EA%DC (πρόσβαση στις 9/4/2013)

http://www.spamlaws.com/what-is-spam.html (πρόσβαση στις 9/4/2013)

http://www2.e-yliko.gr/htmls/safety/sfshare.aspx

http://www2.e-yliko.gr/htmls/safety/smail5.aspx (πρόσβαση στις 9/4/2013)