ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

«INTERNET SAFETY»

Ονοματεπώνυμο Σπουδαστή: Κουτσοσπύρος Σπυρίδων

ΑΜ: 134

Εποπτεύων Καθηγητής: Ζαφειρόπουλος Σπυρίδων

Αμαλιάδα – 2011

Πίνακας Περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

ΠΕΡΙΛΗΨΗ

Στις αρχές της δεκαετίας του ’90, το Διαδίκτυο μπήκε σε μια νέα εποχή και πήρε την μορφή που το γνωρίζουμε μέχρι σήμερα, χάρη στην εμφάνιση του παγκόσμιου ιστού (World Wide Web). Το γραφικό του περιβάλλον έκανε την εξερεύνηση του Διαδικτύου πιο προσιτή και προσέλκυσε τον απλό χρήστη.

Μέσα σε είκοσι χρόνια το Διαδίκτυο με την βοήθεια της τεχνολογίας, κατάφερε μια μεγάλη και απότομη εξάπλωση. Εδραιώθηκε στις ζωές των ανθρώπων, επηρέασε και άλλαξε την καθημερινότητα τους. Έγινε ένα από τα πιο δημοφιλή μέσα επικοινωνίας, πληροφόρησης, ψυχαγωγίας και έφερε επανάσταση στους επαγγελματικούς τομείς, στην ιατρική και την εκπαίδευση. Έχει συναρπάσει εκατομμύρια χρήστες σε όλο τον κόσμο, ενώ για πολλούς είναι πλέον ένα αναπόσπαστο και πολύτιμο εργαλείο στην ζωή τους.

Ωστόσο το Διαδίκτυο έχει αμφισβητηθεί και κατηγορηθεί αρκετές φορές. Η μεγάλη ελευθερία κινήσεων που διαθέτει, ο τεράστιος όγκος προσωπικών δεδομένων που διακινούνται μέσα σε αυτό, η ανωνυμία που μπορεί να παρέχει, καθώς και το γεγονός ότι όλα αυτά είναι μη ελεγχόμενα, έχει δημιουργήσει σοβαρούς κινδύνους από άτομα που εκμεταλλεύονται τις αδυναμίες του Διαδικτύου για να πετύχουν τις προθέσεις τους. Λόγω της φύσης του, οι κίνδυνοι μπορούν να κρύβονται εύκολα και να μην είναι άμεσα ορατοί. Πολλές φορές η πλοήγηση στο Διαδίκτυο καταλήγει μοιραία και γίνεται άσχημη εμπειρία για τον χρήστη που δεν γνωρίζει, ότι πίσω από τον χαοτικό εικονικό κόσμο, τα πράγματα πολλές φορές δεν είναι έτσι όπως φαίνονται.

Σκοπός του εν λόγω συγγράμματος είναι η καταγραφή των κινδύνων που ενέχουν στην πλοήγηση του Διαδικτύου, η πληροφόρηση των χρηστών για τους τρόπους πρόληψης και αντιμετώπισης και η ανάλυση του Διαδικτύου

ως κοινωνικό φαινόμενο στην Ελλάδα. Η προσοχή στρέφεται στον πιο ευάλωτο και επιρρεπή χρήστη, τον ανήλικο, οπού οι κίνδυνοι που κρύβονται για αυτόν, είναι περισσότεροι και πολύ πιο σοβαροί. Παράλληλα καταγράφεται και αναδεικνύεται η σχέση των ενηλίκων με τις Τεχνολογίες Πληροφορικής και Επικοινωνίας (Τ.Π.Ε.) και παρουσιάζονται προτάσεις προς του γονείς για την προστασία και την ασφαλή πλοήγηση των παιδιών στο Διαδίκτυο.

ABSTRACT

In the early '90s, Internet entered a new era and took the form we all know it today, thanks to the emerge of the World Wide Web (WWW). Its Graphical User Interface (GUI) made the exploration of the Internet more accessible and attractive for the simple user.

Within twenty years, Internet with the help of technology, managed a large and rapid expansion. It was established in the lives of people, affected and changed their daily routine. It became one of the most popular means of communication, information, entertainment and brought revolution in business, medicine and education. It has taking over millions of users around the world and for many is considered to be an important and valuable tool in their life.

Is spite of its contribution Internet has been questioned and criticized several times. Due to the considerable available freedom, to the vast amount of personal data moving through it, the anonymity that can be provided, and the fact that all these are not controlled, it pose serious risks for people taking advantage of the weaknesses of the Internet to achieve their intentions. Because of its nature, risks can be easily concealed and are not visible directly. Sometimes surfing the Internet inevitably leads and becomes a bad experience for the user who does not know that behind the chaotic virtual world, things are often not as they seem.

The purpose of this dissertation is to record the risks when navigating the Internet, to inform users about ways of prevention and control of the risks and an analysis of Internet as a social phenomenon in Greece. The attention is drawn upon the most vulnerable and prone users, the minors, where the risks are very serious and more damaging. At the same time the relationship of adults with Information and Communication Technologies (ICT) is presented along with proposals to parents for the protection and safe navigation of children.

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω από καρδιάς τον επιβλέποντα καθηγητή μου κ. Ζαφειρόπουλο Σπύρο, για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Η καθοδήγηση που μου παρείχε, η εμπιστοσύνη που έδειξε στο πρόσωπό μου, η ελευθερία κινήσεων και πρωτοβουλιών που μου χάρισε, ήταν καταλυτικοί παράγοντες στην ολοκλήρωση την πτυχιακής εργασίας. Η βοήθεια του ήταν ανεκτίμητη καθ' όλα τα χρόνια της φοιτητικής μου ζωής.

Επιπλέον, θα ήθελα να ευχαριστήσω τον ραδιοφωνικό σταθμό «Εν Λευκώ» για την όμορφη παρέα που μου κράτησε τις ώρες συγγραφής της πτυχιακής εργασίας, αποδεικνύοντας για μια ακόμα φορά, ότι όλα τα πράγματα γίνονται καλύτερα με λίγη μουσική.

Τέλος, η παρούσα πτυχιακή εργασία είναι αφιερωμένη στην μνήμη του Κώστα, του ανθρώπου στον οποίο χρωστάω την εισαγωγή μου στην σχολή.

“Try again, fail again. Fail better.”

Samuel Beckett

ΕΙΣΑΓΩΓΗ[1]

Τα τελευταία χρόνια οι τεχνολογικές εξελίξεις είναι ραγδαίες. Η παγκόσμια κοινωνία των πληροφοριών αποτελεί σήμερα μια απτή πραγματικότητα, η οποία μας ανήκει και στην οποία ανήκουμε κατά τρόπο αδιαμφισβήτητο, μας περιβάλλει από παντού, μας γεμίζει με την αφθονία της, μας σαγηνεύει με τις υποσχέσεις της και μας τρομάζει με τις εκπλήξεις της.

Όταν στις αρχές της δεκαετίας του ’90 ο Tim Berners Lee σχεδίασε τον παγκόσμιο ιστό, ελάχιστοι μπορούσαν να προβλέψουν την τεράστια εξάπλωσή του και τον τρόπο με τον οποίο θα έμπαινε στην καθημερινότητά μας. Αρχικά, χρησιμοποιήθηκε κυρίως από ακαδημαϊκούς, στρατιωτικούς και κρατικούς οργανισμούς των πλέον προηγμένων χωρών, με αποτέλεσμα οι διακινούμενες πληροφορίες να είναι ασφαλείς ως προς το ύφος τους και να διακινούνται ελεύθερα και χωρίς ιδιαίτερες προφυλάξεις. Ωστόσο, καθώς το νέο μέσο άρχισε να διαδίδεται σε πιο πλατιές μάζες ανθρώπων, το περιεχόμενο που διακινούνταν απέκτησε μεγαλύτερη ποικιλία. Ο εκσυγχρονισμός του παγκόσμιου ιστού έκανε το Διαδίκτυο ένα ιδιαίτερα αποτελεσματικό μέσο επικοινωνίας και δημιούργησε ολοένα και περισσότερους χρήστες που το εκμεταλλεύονται είτε για επαγγελματικούς λόγους, είτε για διασκέδαση, είτε για οποιονδήποτε άλλο σκοπό. Σήμερα μπορούμε να πούμε με βεβαιότητα ότι το Διαδίκτυο είναι ένας ολόκληρος κόσμος με ό,τι αυτό συνεπάγεται.

Οι συνέπειες της επιταχυνόμενης εφαρμογής του Διαδικτύου γίνονται αισθητές σε όλα της τα πεδία: στις οικογενειακές σχέσεις, στην ψυχολογική συμπεριφορά των ανθρώπων, στην πολιτική οργάνωση, στον κόσμο των επιχειρήσεων και του εμπορίου, στην εκπαίδευση, στον τρόπο που δουλεύουμε και διασκεδάζουμε. Μας προσφέρει αφθονία πληροφοριών, γκρεμίζει τα γεωγραφικά σύνορα της γνώσης, συνενώνει τις εμπειρίες των ανθρώπων παγκοσμιοποιώντας τους μύθους τους.

[1] http://ediadiktio.blogspot.com/2009/02/10-2009.html
http://www.e-yliko.gr/htmls/pc_use/safety.aspx
http://epapanis.blogspot.com/2009_03_01_archive.html

Τα αναμφισβήτητα οφέλη του Διαδικτύου πολλές φόρες επισκιάζονται από τις αρνητικές συνέπειες της παρατεταμένης ή λανθασμένης χρήσης του, καθώς και το πλήθος των παραβατικών συμπεριφορών που βρίθουν στον εικονικό του κόσμο. Το Διαδίκτυο είναι ένας ολόκληρος κόσμος. Αν κάποιος γνωρίζει που βαδίζει και τι κάνει, επωφελείται από τα πλεονεκτήματα του, διαφορετικά μπορεί να έρθει αντιμέτωπος με διαφόρων ειδών κακοτοπιές και κινδύνους, ακριβώς όπως συμβαίνει και στον πραγματικό κόσμο.

Η παρούσα πτυχιακή εργασία εξετάζει τους κινδύνους που κρύβονται κατά τη χρήση του Διαδικτύου, καθώς επίσης και τους τρόπους με τους οποίους μπορεί να επιτευχθεί η ασφαλής πλοήγηση.

Στο κεφάλαιο 1, παρουσιάζονται η εξέλιξη του Διαδικτύου στην Ελλάδα και έρευνες που αφορούν την χρήση του.

Στο κεφάλαιο 2, αναλύονται οι κίνδυνοι που καλείται να αντιμετωπίσει ένας ενήλικας κατά την πλοήγηση του στο Διαδίκτυο, καθώς και οι τρόποι εξάλειψης τους.

Στο κεφάλαιο 3, εξετάζονται οι κίνδυνοι κατά τη χρήση Διαδικτύου από παιδιά και οι τρόποι αντιμετώπισής τους.

Στο κεφάλαιο 4, μελετάται ο ρόλος που έχουν οι ενήλικες στην προστασία των παιδιών από τους κινδύνους του Διαδικτύου.

Στο κεφάλαιο 5, παρουσιάζεται το λογισμικό προστασίας που ενισχύει την ασφάλεια του υπολογιστή, όπως επίσης και το λογισμικό γονικού ελέγχου που βοηθά του γονείς να δημιουργήσουν σωστή και ασφαλή πλοήγηση για τα παιδιά.

Στο κεφάλαιο 6, παρουσιάζονται δράσεις, υπηρεσίες και ομάδες που έχουν δημιουργηθεί από διάφορους φορείς, με σκοπό να ενημερώσουν, να προφυλάξουν και γενικότερα να βοηθήσουν τους χρήστες τους Διαδικτύου σε τυχόν προβλήματα που μπορούν να προκύψουν.

1. ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΤΗΝ ΕΛΛΑΔΑ

1.1 Στοιχεία χρήσης Διαδικτύου [2]

Ένας νέος κόσμος επικοινωνίας προσγειώθηκε και τάραξε συθέμελα την καθημερινότητα των Ελλήνων τη δεκαετία που πέρασε, υποσχόμενος περισσότερη ελευθερία και νέες δυνατότητες επιλογών στην ενημέρωση, στην κατανάλωση και στην ψυχαγωγία.

Το Διαδίκτυο στην Ελλάδα ξεκίνησε στις αρχές της δεκαετίας του ’90 (1992-1993), αρχικά αρκετά περιορισμένα από 2-3 εταιρείες που παρείχαν κυρίως υπηρεσίες online πληροφόρησης. Στα μέσα της δεκαετίας του ’90 άρχισε η περισσότερο ουσιαστική διάδοση του Διαδικτύου στην Ελλάδα. Από τότε έχουν γίνει σημαντικά βήματα στη διείσδυση και χρήση του Διαδικτύου, ωστόσο τα ποσοστά χρήσης παραμένουν ακόμη σε χαμηλά επίπεδα.

Σύμφωνα με το Παρατηρητήριο της Κοινωνίας της Πληροφορίας, τον οργανισμό που μετρά τους Έλληνες χρήστες του Διαδικτύου και τις συνήθειές τους, οι Έλληνες δεν έχουν την καλύτερη σχέση με το Διαδίκτυο και οι επιδόσεις τους είναι αρκετά χαμηλότερες από του ευρωπαϊκού μέσου όρου.

Παρόλα αυτά η διείσδυση του Διαδικτύου στα Ελληνικά νοικοκυριά σημειώνει σταθερή ανοδική πορεία τα τελευταία έτη. Έρευνα που πραγματοποιήθηκε από το Παρατηρητήριο της Κοινωνίας της Πληροφορίας το 2008, στο πλαίσιο της μελέτης για τη μέτρηση των δεικτών των ευρωπαϊκών σχεδίων δράσης «i2010» και «eEurope», έδειξε ότι:

- Σχεδόν 4 στα 10 νοικοκυριά ήταν στα τέλη του 2008 συνδεδεμένα στο Διαδίκτυο (39,4%).

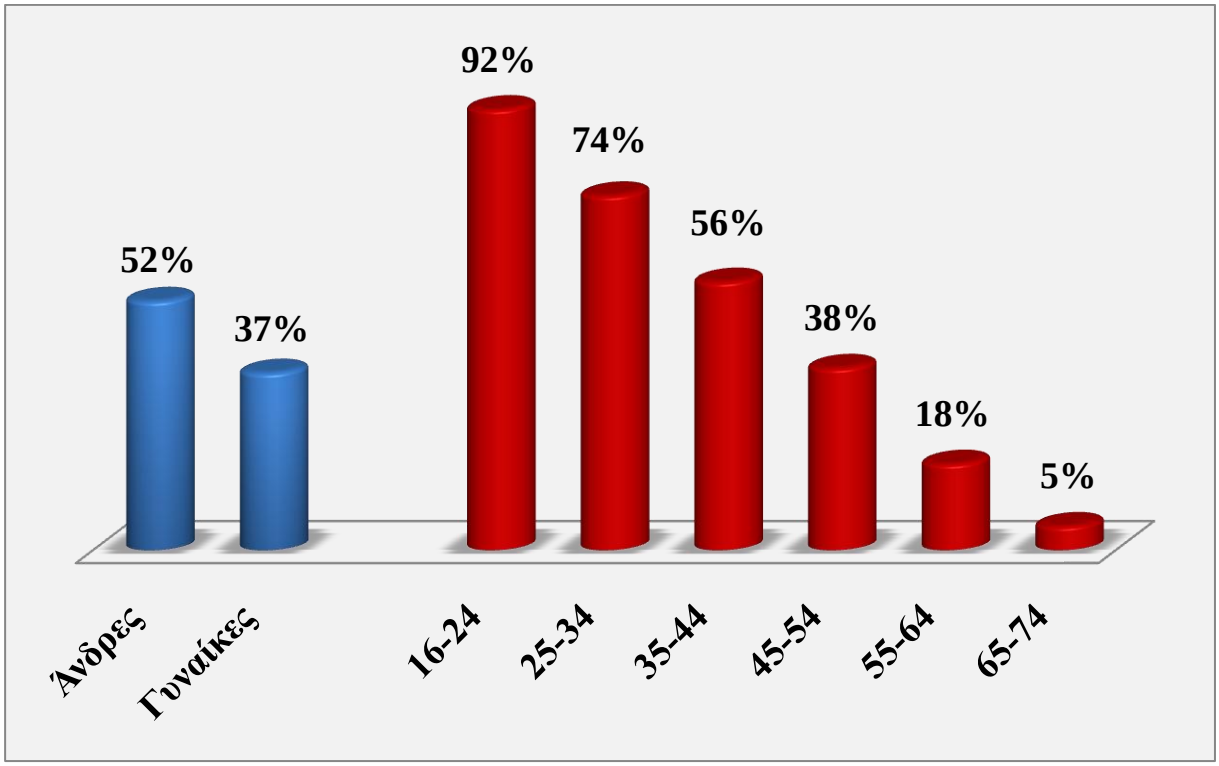
[2] http://www.imerisia.gr/article.asp?catid=12319&subid=2&pubid=10867156#
http://www.sepe.gr/files/news/SEPE_Meleti_Internet.pdf
http://www.politonsymaxia.gr/?p=511
«Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.4, 7, 9

- Ο μέσος ετήσιος ρυθμός αύξησης της πρόσβασης για την τετραετία 2005-2008 διαμορφώνεται στο 17,6%.

Εξετάζοντας τα ποσοστά πρόσβασης στο Διαδίκτυο με βάση τα δημογραφικά χαρακτηριστικά του δείγματος, προκύπτει ότι τα πρωτεία στη χρήση κατέχουν:

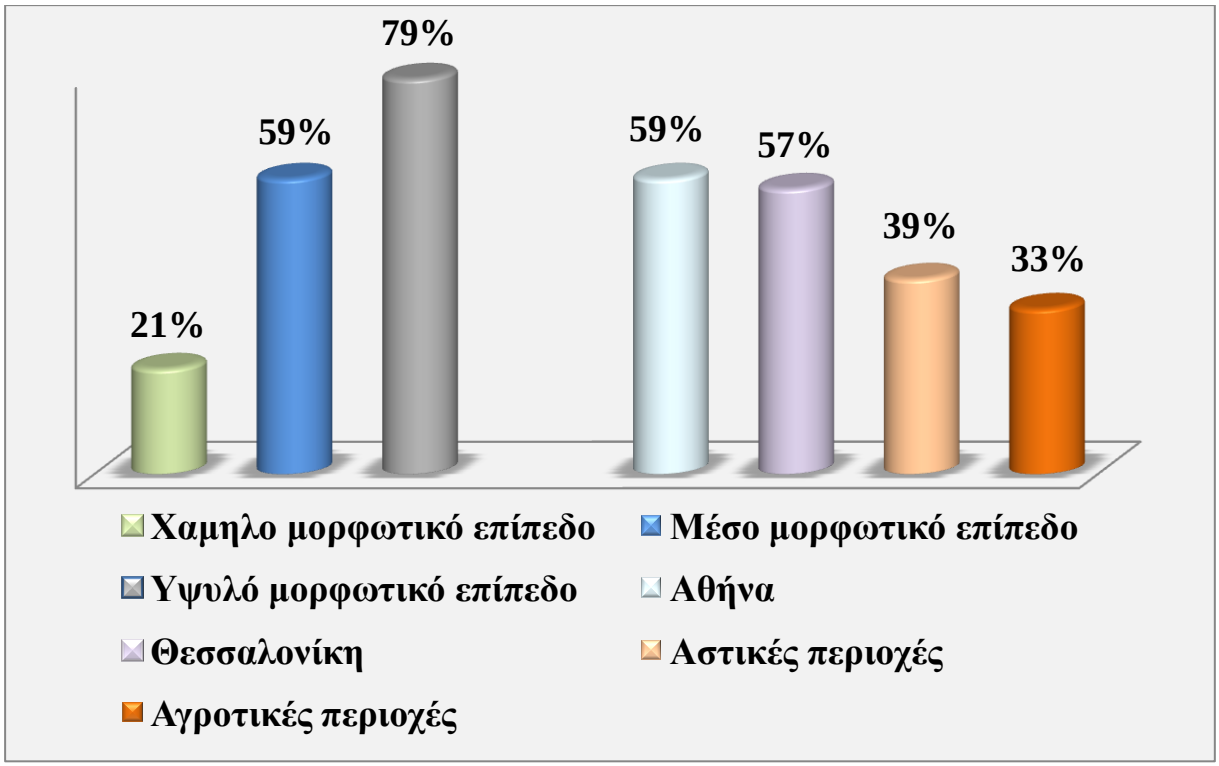
- οι άνδρες
- οι νέοι, ιδιαίτερα των ηλικιών 16-24
- τα άτομα υψηλού μορφωτικού επιπέδου
- οι κάτοικοι των μεγάλων αστικών κέντρων

Στα σχήματα που ακολουθούν παρουσιάζονται μερικά από τα πιο σημαντικά αποτελέσματα, αναφορικά με τη διείσδυση του Διαδικτύου, σύμφωνα με την ετήσια έρευνα του Παρατηρητηρίου της Κοινωνίας της Πληροφορίας.



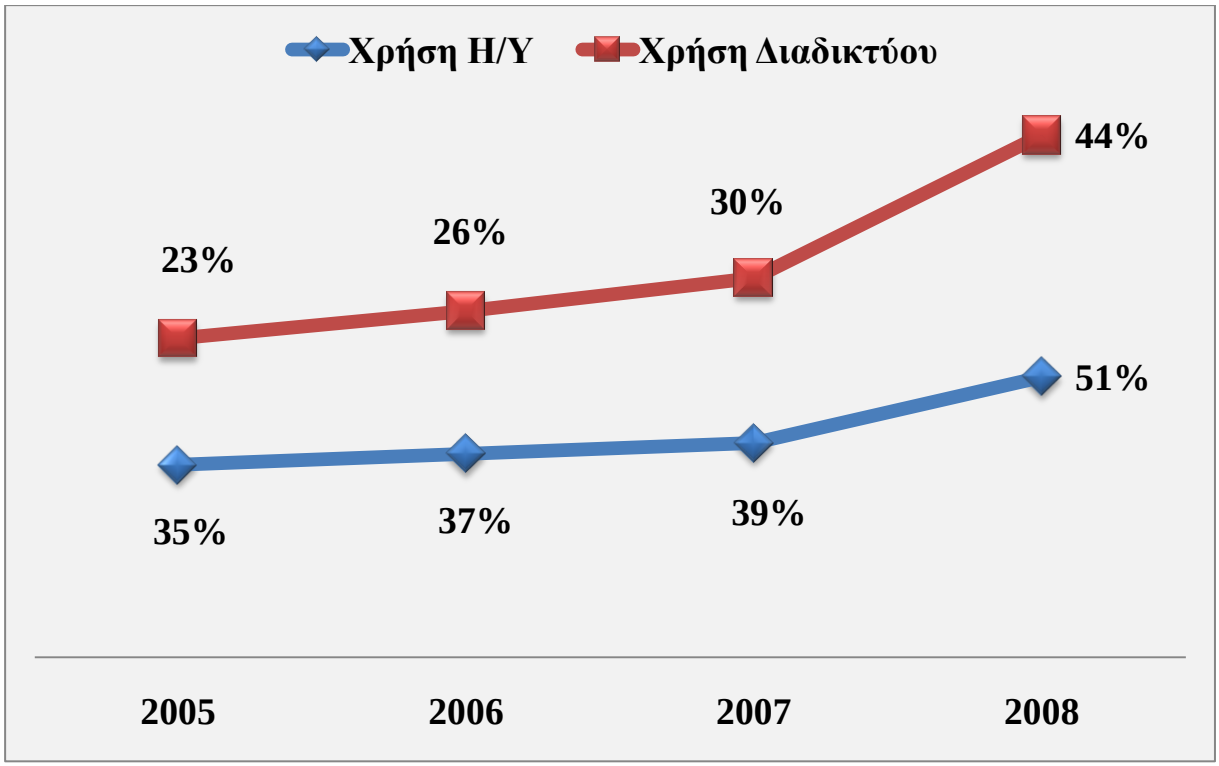
Σχήμα 1 – Χρήση του Διαδικτύου από τον Ελληνικό πληθυσμό (2008)[3]

[3] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.5



Σχήμα 2 – Χρήση του Διαδικτύου από τον Ελληνικό πληθυσμό(β) (2008)[4]

[4] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.5



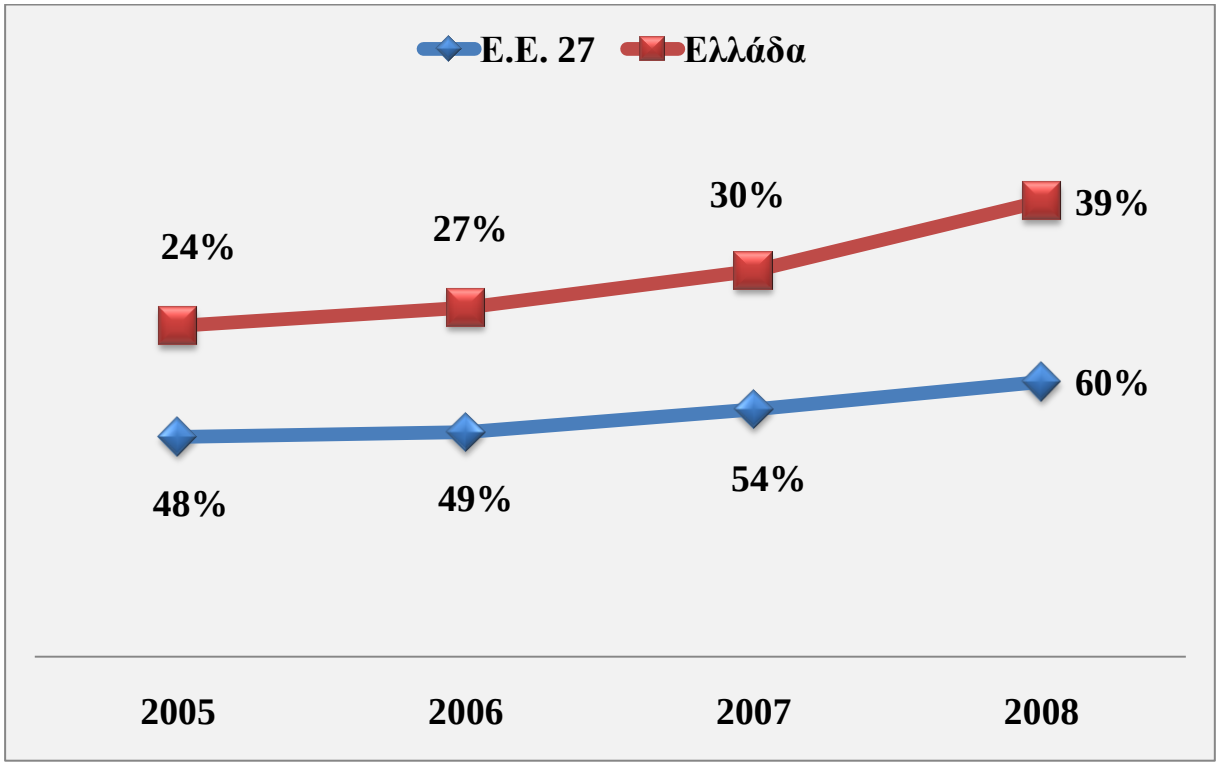
Σχήμα 3 – Χρήση Η/Υ και Διαδικτύου[5]

Χρήση Η/Υ: Όσοι έχουν / χρησιμοποιούν Η/Υ.

Χρήση Διαδικτύου: Όσοι έχουν πρόσβαση στο Διαδίκτυο, ανεξάρτητα από το αν έχουν προσωπική σύνδεση ή όχι.

[5] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.7

Περίπου 4 στα 10 Ελληνικά νοικοκυριά είναι συνδεδεμένα στο Διαδίκτυο (39,4%), ενώ αξίζει να σημειωθεί ότι το 2008 καταγράφηκε η μεγαλύτερη άνοδος μέσα στην τετραετία 2005-2008, της τάξης των 9 ποσοστιαίων μονάδων. Σε επίπεδο Ε.Ε. το αντίστοιχο ποσοστό εξακολουθεί να είναι αρκετά πιο υψηλό (60% για την Ε.Ε.27) αν και ιδιαίτερα θετικά αξιολογείται το γεγονός ότι ο μέσος ετήσιος ρυθμός αύξησης των νοικοκυριών με πρόσβαση στο Διαδίκτυο στο διάστημα 2005-2008 εκτιμάται σε 17,6%, τη στιγμή που ο μέσος ετήσιος ρυθμός της Ευρώπης (Ε.Ε.27) είναι στο 7,7%.



Σχήμα 4 – Νοικοκυριά με σύνδεση στο Διαδίκτυο[6]

[6] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.5

Διερευνώντας τους λόγους που αποφεύγουν να αποκτήσουν σύνδεση στο σπίτι τους οι Έλληνες, στο μεγαλύτερό τους ποσοστό δηλώνουν:

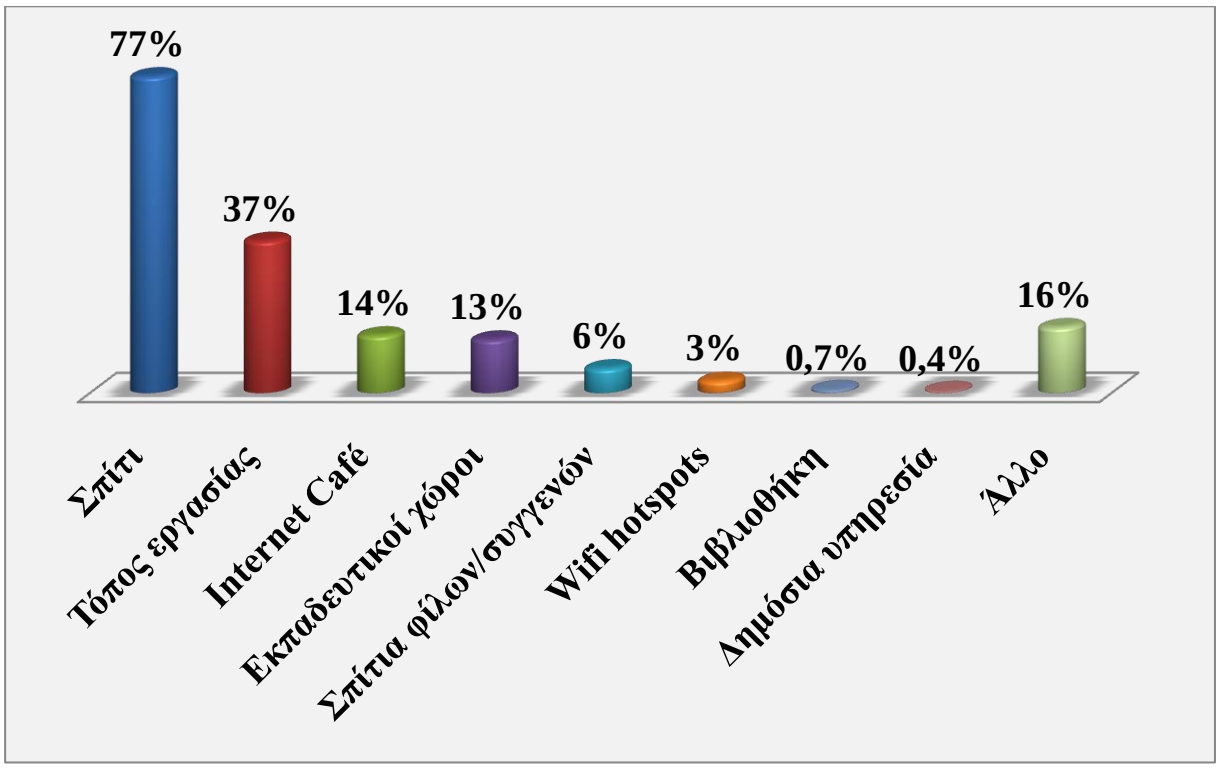
- ότι δεν θέλουν καθώς θεωρούν το περιεχόμενο επιζήμιο (28%).
- ότι δε διαθέτουν τις κατάλληλες δεξιότητες για τη χρήση του Διαδικτύου (27%).
- ότι το κόστος για την απόκτηση του σχετικού εξοπλισμού είναι υψηλό (11%).

Συνοψίζοντας, το 2008 σημειώνεται η μεγαλύτερη άνοδος στη χρήση του Διαδικτύου σε σχέση με τα προηγούμενα έτη ενώ, εκτός από την αυξητική τάξη, σημειώνεται και εντατικοποίηση ως προς τη συχνότητα χρήσης, τόσο των τακτικών όσο και των πιο δυναμικών χρηστών.

Όλα αυτά δείχνουν ότι το Διαδίκτυο είναι ένα νεανικό μέσο και ότι οι μεγαλύτερες ηλικίες υστερούν της χρήσης του, παρ' όλα αυτά, φαίνεται ότι η κατάσταση βελτιώνεται. Αυτό υποστηρίζει η Έλλη Παπουρτζή, πρόεδρος του Παρατηρητηρίου για την ΚτΠ, και υπερθεματίζει: «Η σχέση των Ελλήνων με τις νέες τεχνολογίες την τριετία 2005-2007 έχει καλυτερεύσει, ενώ κερδίζει όλο και μεγαλύτερο έδαφος στις νεότερες ηλικίες, σε τέτοιο βαθμό μάλιστα που τα σημερινά Ελληνόπουλα δεν έχουν να ζηλέψουν τίποτα από τους υπόλοιπους νέους της Ευρώπης». Στη συνέχεια η ίδια στέκεται στις επιδόσεις του ασθενούς φύλου: «Όλο και περισσότερες Ελληνίδες κατακτούν τον κυβερνοχώρο, με τον μέσο ετήσιο ρυθμό αύξησής τους να φθάνει στο 20% σε σχέση με 6% στις Ευρωπαίες των 27 χωρών-μελών».

1.2 Τόπος πρόσβασης[7]

Περίπου 8 στους 10 τακτικούς χρήστες του Διαδικτύου δηλώνουν ότι έχουν πρόσβαση από το σπίτι, ενώ ακολουθεί σε πολύ χαμηλότερο ποσοστό ο χώρος εργασίας, που αφορά κυρίως εργαζομένους γραφείου, όπως διοικητικά / διευθυντικά στελέχη (66%), επιστήμονες (62%) ή υπαλλήλους γραφείου (70%) και άτομα ανώτατης εκπαίδευσης έως 45 ετών (55%).



Σχήμα 5 – Τόπος πρόσβαση στο Διαδίκτυο (2008)[8]

Η πρόσβαση στο Διαδίκτυο από Internet café, εκπαιδευτικούς χώρους και σημεία ασύρματης ευρυζωνικής πρόσβασης (wifi hotspots), πραγματοποιείται κυρίως από νέους έως 25 ετών. Ειδικά ο δείκτης των wifi hotspots, που διαμορφώνεται μόλις στο 3%, αναμένεται να αυξηθεί σημαντικά τα αμέσως επόμενα χρόνια, για τους εξής λόγους:

- Οι φορητές συσκευές που επιτρέπουν πρόσβαση στο Διαδίκτυο, όπως τα κινητά τηλέφωνα, τα palmtops και τα netbooks αρχίζουν να αποκτούν

[7,8] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.9-10

σημαντικό μερίδιο στην Ελληνική αγορά. Η σχέση των ατόμων με το Διαδίκτυο γίνεται ολοένα και πιο ευέλικτη, αποδεσμεύοντας τους σταδιακά από τους ηλεκτρονικούς υπολογιστές και επιτρέποντας την πρόσβαση από οπουδήποτε.

- Δημιουργούνται πολλά νέα σημεία δωρεάν ασύρματης ευρυζωνικής πρόσβασης. Χαρακτηριστικό παράδειγμα η πρωτοβουλία της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού του Υπουργείου Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, η οποία μετά την ανάπτυξη wi-fi hotspots στο Σύνταγμα, το Θησείο, την Πλατεία Κοτζιά και το Εθνικό Ίδρυμα Ερευνών στην Αθήνα, ανακοίνωσε τη χρηματοδότηση της δημιουργίας 279 νέων σημείων δωρεάν ασύρματης πρόσβασης (WiFi hotspots) σε Δήμους, Νομαρχίες, Περιφέρειες, Τ.Ε.Δ.Κ. και άλλους φορείς σε ολόκληρη τη χώρα.

Συγκρίνοντας τα στοιχεία που αφορούν τον τόπο πρόσβασης στο Διαδίκτυο με τα αντίστοιχα της Ε.Ε.27 παρατηρείται ότι οι συνήθειες των Ελλήνων συμβαδίζουν με αυτές του ευρωπαίου πολίτη. Το 86% του πληθυσμού της Ε.Ε.27 συνδέεται στο Διαδίκτυο από το σπίτι, το 42% από το χώρο εργασίας και το 13% από εκπαιδευτικούς χώρους.

1.3 Λόγοι χρήσης[9]

Όσον αφορά τους λόγους χρήσης του Διαδικτύου, τα στοιχεία του 2008 παρουσιάζουν ορισμένες μεταβολές σε σχέση με την ομοιόμορφη εικόνα της προηγούμενης τριετίας (2005-2007).

Παράλληλα με τις «παραδοσιακές» δραστηριότητες ενός χρήστη του Διαδικτύου, όπως είναι η αναζήτηση πληροφοριών και η αποστολή / λήψη e-mail, οι Έλληνες χρήστες φαίνεται να στρέφονται πλέον και να αξιοποιούν τις

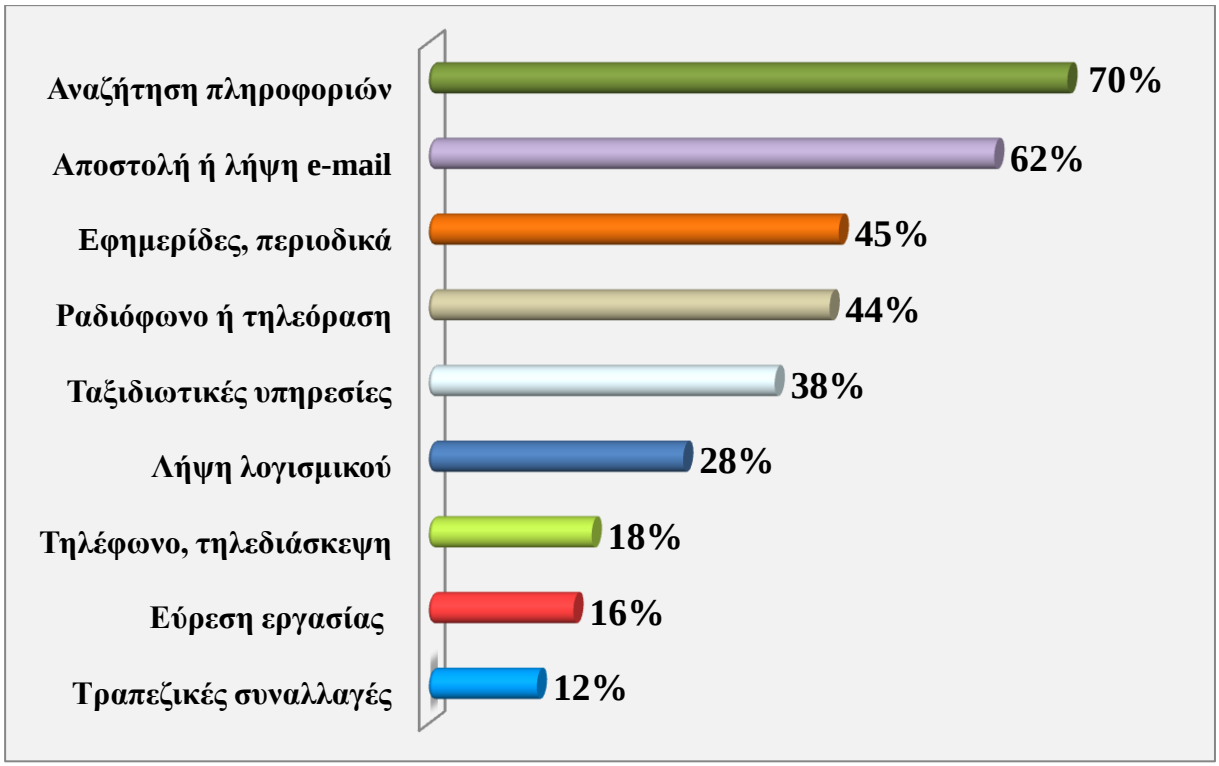
[9] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.10, 31-32

νέες δυνατότητες επικοινωνίας και ψυχαγωγίας που προσφέρονται μέσω Διαδικτύου.

Σημαντική μεταβολή σε σχέση με τα προηγούμενα έτη έχει σημειωθεί στο ποσοστό των Ελλήνων που χρησιμοποιούν το Διαδίκτυο για να διαβάσουν ηλεκτρονικές εφημερίδες και περιοδικά (45%). Η ακρόαση ραδιοφώνου και η παρακολούθηση τηλεόρασης μέσω του Διαδικτύου αξιοποιείται από το 44% των χρηστών, παρουσιάζοντας επίσης μεγάλη αύξηση σε σχέση με το 2007 (28%).

Περίπου 4 στους 10 χρήστες του Διαδικτύου το αξιοποιούν για χρήση υπηρεσιών σχετικά με ταξίδια, 3 στους 10 για την απόκτηση λογισμικού και περίπου 2 στους 10 χρήστες για την πραγματοποίηση τηλεφωνικών κλήσεων μέσω Διαδικτύου και αναζήτηση εργασίας.

Στην τελευταία θέση της κατάταξης έρχονται οι υπηρεσίες ηλεκτρονικής τραπεζικής με διείσδυση μόλις 12%, παρόλο που αποτελούν έναν ιδιαίτερα προσιτό και αποτελεσματικό τρόπο για την πραγματοποίηση ηλεκτρονικών συναλλαγών με τράπεζες και σειρά λοιπών φορέων. Στο προφίλ των χρηστών e-banking υπερτερούν οι άνδρες, τα άτομα ανώτατης μόρφωσης, τα ανώτατα διοικητικά / διευθυντικά στελέχη, οι επιστήμονες, ενώ με βάση τη γεωγραφική περιοχή η κρίσιμη μάζα χρηστών εντοπίζεται στην Αθήνα. Καθώς πρόκειται για τη μοναδική κατηγορία του Σχήματος 6 που περιλαμβάνει χρηματικές συναλλαγές, η κατάταξη στην τελευταία θέση είναι ενδεικτική της έλλειψης εμπιστοσύνης των χρηστών στο Διαδίκτυο σχετικά με την ασφάλεια των συναλλαγών. Επιπλέον, δεδομένου ότι ο αντίστοιχος ευρωπαϊκός μέσος όρος διαμορφώνεται στο κατά πολύ υψηλότερο 47%, γίνεται φανερό ότι πρέπει να εντατικοποιηθούν οι προσπάθειες πλήρους και ορθής ενημέρωσης των Ελλήνων σχετικά με τη διεξαγωγή ηλεκτρονικών συναλλαγών, ενδεχομένως και σε συνδυασμό με παροχή κινήτρων για τη χρήση τους έναντι των παραδοσιακών συναλλαγών.



Σχήμα 6 – Λόγοι χρήσης Διαδικτύου (2008)[10]

Ενδιαφέρον παρουσιάζει και η μεταβολή των συνηθειών των χρηστών του Διαδικτύου, καθώς μεταβάλλεται η ηλικία τους.

Τα νεαρότερα άτομα χρησιμοποιούν κυρίως το Διαδίκτυο για λόγους επικοινωνίας με άλλους χρήστες (μέσω e-mail, instant messaging) και ψυχαγωγίας (πρόσβαση σε ηλεκτρονικά Μ.Μ.Ε. και ηλεκτρονική λήψη οπτικοακουστικού υλικού), ενώ δεν παύει να χρησιμοποιείται και για τον εντοπισμό χρήσιμων πληροφοριών.

Στην ηλικιακή κατηγορία 35-44 παρατηρείται υψηλότερη ιεράρχηση του πληροφοριακού χαρακτήρα του Διαδικτύου, ενώ γίνεται είσοδος – και μάλιστα σε υψηλή θέση – της κατηγορίας που αφορά σε υπηρεσίες σχετικές με ταξίδια και διαμονή.

Διερευνώντας τις συνήθειες μεγαλύτερων σε ηλικία χρηστών του Διαδικτύου, δεν παρατηρούνται σημαντικές αλλαγές σε σχέση με το γκρουπ 35-44. Ιδιαίτερο

[10] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.11

ενδιαφέρον, ωστόσο, παρουσιάζει το γεγονός ότι έρχονται δεύτεροι σε ανάγνωση ιστολογίων (blogs), με ποσοστό 33,9% μετά τους νέους 16-24 (37%).

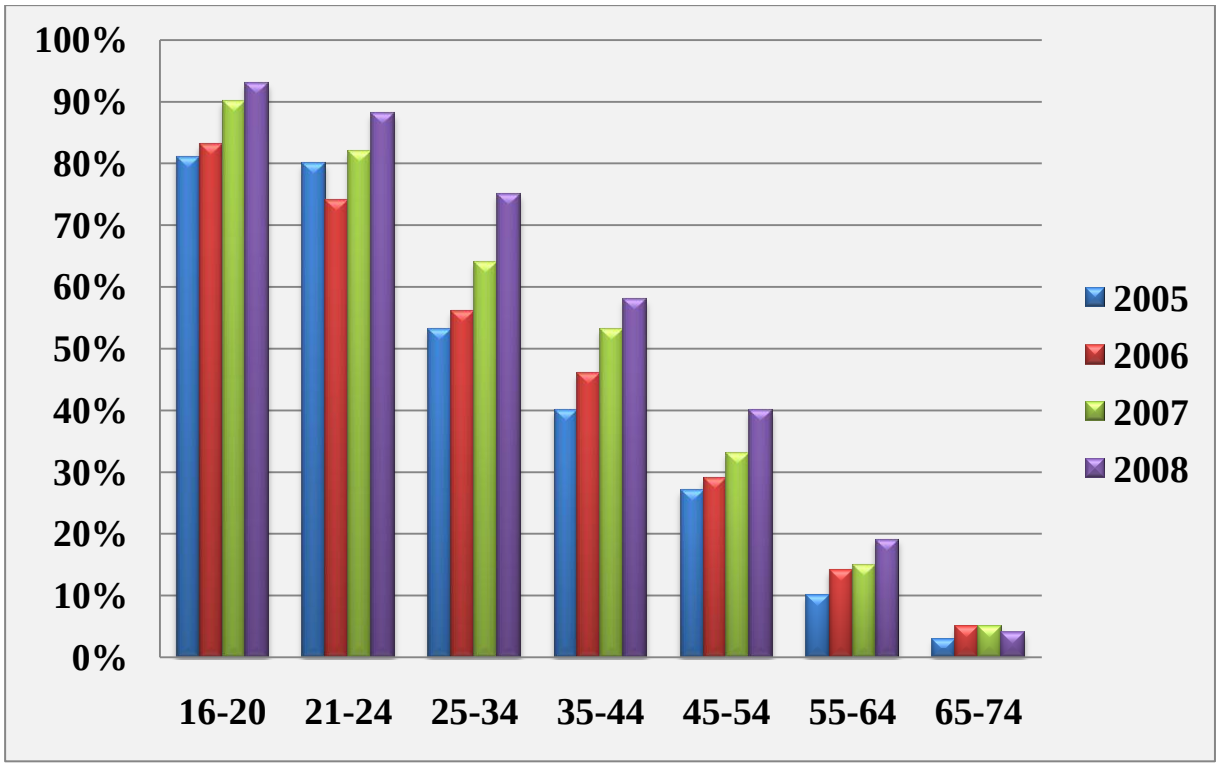
1.4 Ψηφιακό χάσμα[11]

Αναλύοντας τα αποτελέσματα της έρευνας με βάση την ηλικία των ερωτώμενων, παρατηρούνται μεγάλες αποκλίσεις μεταξύ των διαφόρων ηλικιακών ομάδων. Συγκρίνοντας, για παράδειγμα, έναν έφηβο με έναν 40άρη και έναν 70άρη, βλέπουμε τη χρήση Η/Υ και Διαδικτύου να κινείται από την τάξη του 95% στο 60% και 5% αντίστοιχα. Εξαίρεση του κανόνα, τα κινητά τηλέφωνα, που χρησιμοποιούνται από όλους σχεδόν του πολίτες έως 55 ετών, ενώ μικρή πτώση παρατηρείται στις μεγαλύτερες ηλικίες συγκρινόμενη με την αντίστοιχη πτώση στη χρήση του Η/Υ και του Διαδικτύου.

Στα παρακάτω γραφήματα παρουσιάζονται αναλυτικά τα ποσοστά χρήσης του Η/Υ και του Διαδικτύου για όλες τις ηλικιακές ομάδες και για την τετραετία 2005-2008. Τα βασικά συμπεράσματα από τη διαχρονική παρακολούθηση των δεικτών συνοψίζονται στα εξής:

- Η χρήση των τεχνολογιών πληροφορικής κυμαίνεται σε πολύ υψηλά επίπεδα στους νέους 16-24 ετών, με ακόμη πιο έντονη διείσδυση να παρατηρείται στην υποκατηγορία 16-20 ετών.
- Καθώς αυξάνεται η ηλικία των ατόμων, μειώνεται ο βαθμός εξοικείωσής τους με τις νέες τεχνολογίες.
- Σχεδόν 2 στα 10 άτομα ηλικίας 55-64 ετών χρησιμοποιούν τον Η/Υ και το Διαδίκτυο, ποσοστό ιδιαίτερα χαμηλό για παραγωγικές ηλικίες.
- Τα άτομα ηλικιών 65 και άνω είναι αποκομμένα από τη χρήση νέων τεχνολογιών (Η/Υ 4%, Διαδίκτυο 5%).
- Υπάρχει ξεκάθαρη αυξητική τάση για το διάστημα 2005-2008, η οποία είναι ιδιαίτερα έντονη στις ηλικιακές κατηγορίες 25-34 και 35-44.

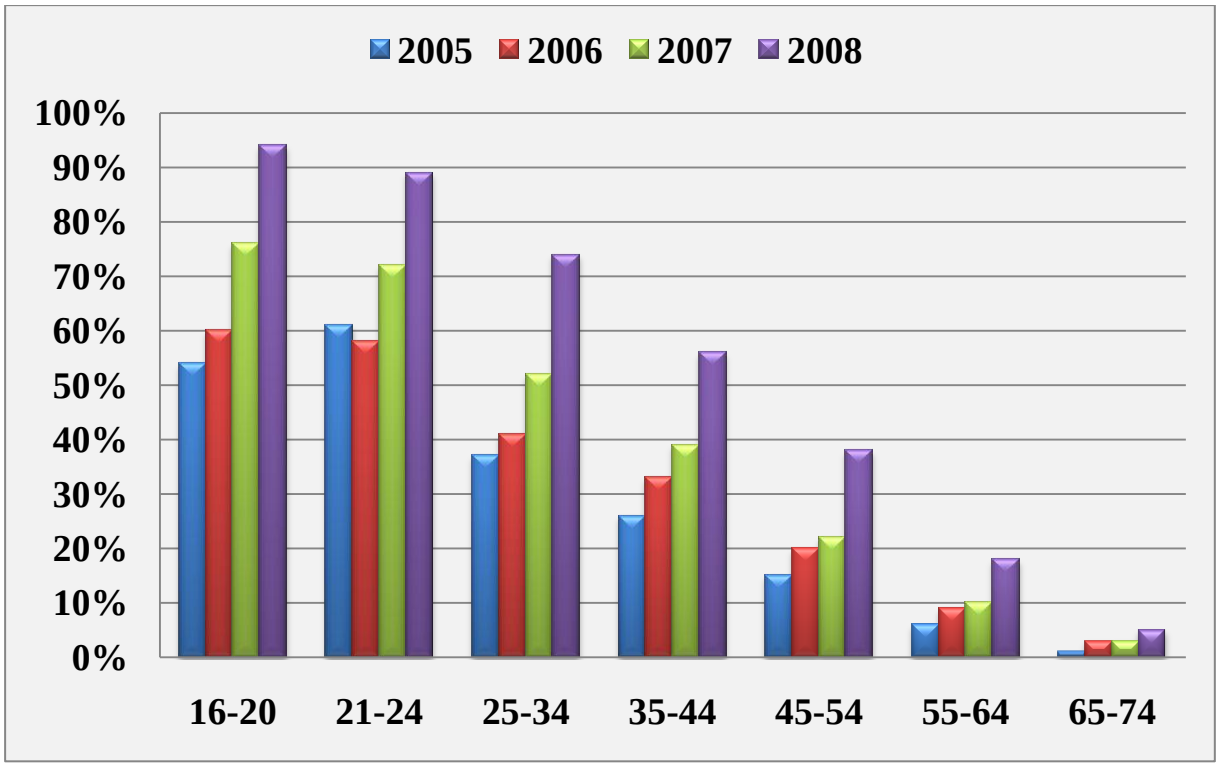
[11]«Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.28



Σχήμα 7 – Χρήση Η/Υ ανά ηλικιακή κατηγορία[12]

Σύνολο δείγματος: 2005 n=8330, 2006 n=8025, 2007 n=8245, 2008 n=5966

[12] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.29



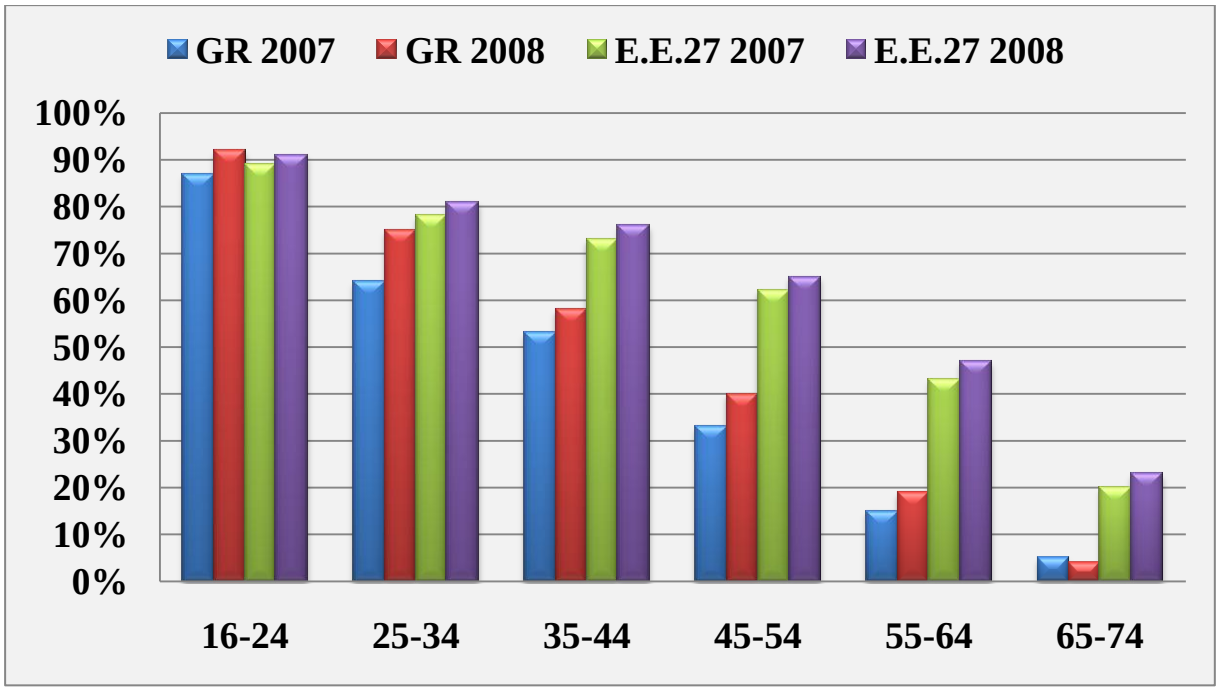
Σχήμα 8 – Χρήση Διαδικτύου ανά ηλικιακή κατηγορία[13]

Σύνολο δείγματος: 2005 n=8330, 2006 n=8025, 2007 n=8245, 2008 n=5966

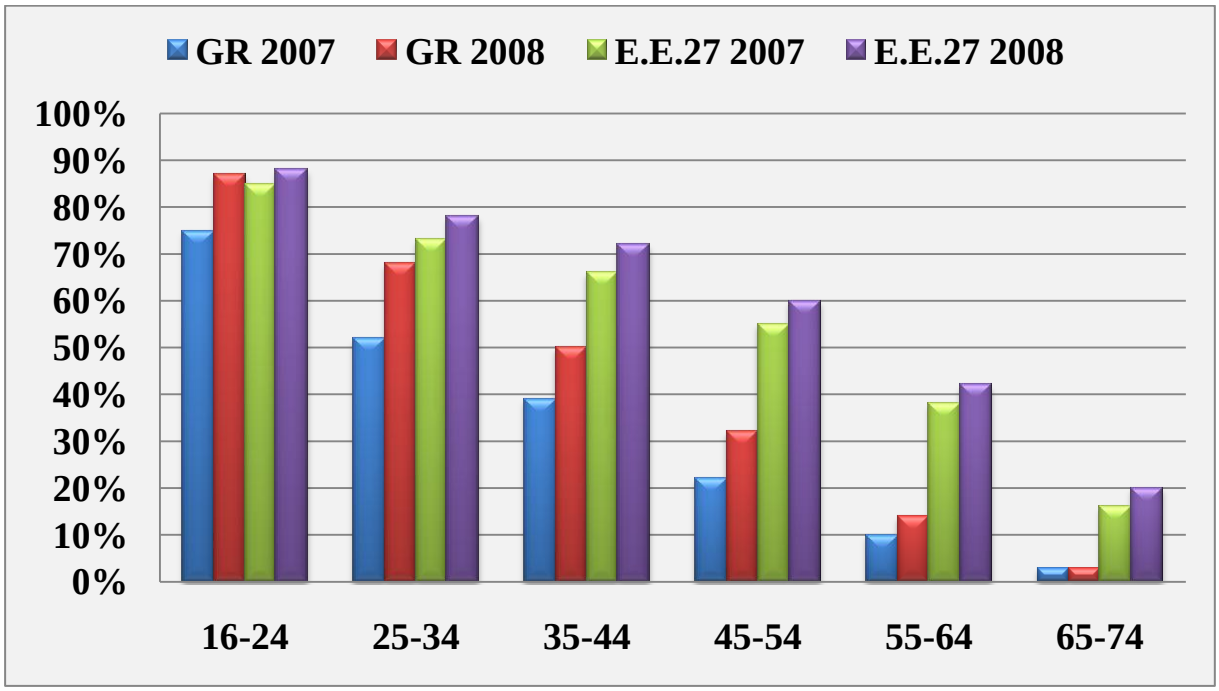
Λαμβάνοντας υπόψη και τους ευρωπαϊκούς μέσους όρους στους υπό εξέταση δείκτες, παρατηρείται ότι και στην Ευρώπη υπάρχει συσχέτιση της χρήσης τεχνολογιών πληροφορικής με την ηλικία.

Ωστόσο, όσο αυξάνεται η ηλικία των ατόμων αυξάνεται και το χάσμα μεταξύ Ελλάδας και Ευρώπης, φτάνοντας σχεδόν τις 20 ποσοστιαίες μονάδες για τις ηλικίες 65-74. Αυτό είναι εμφανές και στα παρακάτω γραφήματα, ειδικά για τις ηλικίες άνω των 45 ετών. Παρά το γεγονός ότι τα ποσοστά της Ελλάδας έχουν αυξηθεί σημαντικά κατά το έτος 2007-2008, αποδεικνύεται ότι χρειάζεται να καταβληθεί μεγάλη προσπάθεια προκειμένου οι πιο μεγάλοι σε ηλικία Έλληνες να είναι ανταγωνιστικοί «ψηφιακά» έναντι των Ευρωπαίων.

[13] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.29-31



Σχήμα 9 – Ελλάδα vs E.E.27, Χρήση Η/Υ ανά ηλικιακή κατηγορία[14]



Σχήμα 10 – Ελλάδα vs E.E.27, Χρήση Διαδικτύου ανά ηλικιακή κατηγορία[15]

[14,15] «Ταυτότητα χρηστών Internet στην Ελλάδα», Μάρτιος 2010, Παρατηρητήριο για την Κοινωνίας της Πληροφορίας, σελ.30

Το ιδιαίτερα θετικό μήνυμα που προκύπτει είναι ότι υπάρχει πλέον σύγκλιση μεταξύ των νέων της Ελλάδας ηλικίας 16-24 και των συνομήλικών τους στην Ε.Ε.27, η οποία επιτεύχθηκε με εντυπωσιακή άνοδο στη χρήση Η/Υ και Διαδικτύου μεταξύ 2007 και 2008 (87% σε 92% και 75% σε 87% αντίστοιχα).

1.5 Οφέλη από την ανάπτυξη του Διαδικτύου[16]

Τα οφέλη από την ανάπτυξη του Διαδικτύου έχουν απήχηση τόσο στην Ελληνική οικονομία, στην απασχόληση και στην παραγωγικότητα όσο και στο σύνολο του Ελληνικού πληθυσμού (ιδιώτες, επιχειρήσεις, κράτος).

1.5.1 Οικονομία-Απασχόληση-Παραγωγικότητα

Η χρήση της τεχνολογίας και του Διαδικτύου μπορεί να συνεισφέρει σημαντικά στη δημιουργία απασχόλησης και εσόδων. Δίνει τη δυνατότητα σε άτομα και επιχειρήσεις να εκμεταλλευτούν οικονομικές ευκαιρίες που απορρέουν από αποδοτικότερες διαδικασίες, τη συμμετοχή σε ευρύτερα οικονομικά δίκτυα και τη δημιουργία νέων ευκαιριών για απασχόληση.

Με πολλούς τρόπους το Διαδίκτυο βοηθά στη ανάπτυξη της παραγωγικότητας όπως π.χ. με τη διάδοση πληροφοριών και λύσεων για κάποιο συγκεκριμένο πρόβλημα σε όλους τους ενδιαφερομένους της αγοράς ή με την έγκαιρη πρόσβαση σε στοιχεία, είτε μέσα από το Διαδίκτυο είτε από κλειστά δίκτυα, που βοηθούν στη λήψη σωστών αποφάσεων.

Οι επιχειρήσεις και γενικότερα η αγορά μπορούν με τη χρήση του Διαδικτύου και της τεχνολογίας να μειώσουν κόστη για αγορά υλικών, προμήθειες συναλλαγών ή και λειτουργικά κόστη γεγονός που τους δίνει τη δυνατότητα να μειώσουν τις τιμές των προϊόντων τους και να γίνουν πιο ανταγωνιστικοί. Επιπλέον πέρα από τη μείωση των τιμών μπορούν να χρησιμοποιήσουν την καλύτερη και περισσότερη πληροφόρηση που έχουν για να βελτιώσουν την αξία του προϊόντος τους και να αποκτήσουν ανταγωνιστικό πλεονέκτημα.

[16] http://www.sepe.gr/files/news/SEPE_Meleti_Internet.pdf

Η παγκόσμια αυτή δικτύωση έχει σαν αποτέλεσμα νέους τρόπους δημιουργίας και παράδοσης προϊόντων και υπηρεσιών σε παγκόσμιο επίπεδο. Δημιουργούνται νέα επιχειρηματικά μοντέλα και νέες συνθήκες αγοράς καθώς και νέοι κλάδοι απασχόλησης (απασχόληση που μπορεί να γίνεται και μέσω Διαδικτύου - τηλε-εργασία). Παράλληλα η πρόσβαση σε νέες αγορές και πηγές που μπορούν να δώσουν ευκαιρίες για απόκτηση ανταγωνιστικού πλεονεκτήματος, δίνει σημαντικές ευκαιρίες για περαιτέρω ανάπτυξης της οικονομίας.

1.5.2 Ιδιώτες

1.5.2.1 Καλύτερη ποιότητα ζωής

Η ανάπτυξη του Διαδικτύου συμβάλλει σημαντικά στη βελτίωση του βιοτικού επίπεδου του πολίτη μέσα από εφαρμογές που τον βοηθούν:

- Στην διεκπεραίωση των εργασιών του σε σχέση με το κράτος πιο εύκολα και πιο γρήγορα με εφαρμογές e-government όπως την υποβολή της φορολογικής του δήλωσης, της δήλωσης Φ.Π.Α., την απόκτηση πιστοποιητικών κ.α.
- Στην αύξηση των γνώσεών του χρησιμοποιώντας ηλεκτρονικές βιβλιοθήκες, forums, online εγκυκλοπαίδειες, ηλεκτρονικά μουσεία κ.α.
- Στην ολοκληρωμένη και διαδραστική ενημέρωσή του μέσα από ειδησεογραφικά web sites, portals, ηλεκτρονικό τύπο κ.λπ.
- Στην ψυχαγωγία του δίνοντάς του την δυνατότητα να επισκεφτεί δικτυακούς τόπους με μουσική (music on demand), ταινίες (video on demand), online games κ.λπ. Στην από απόσταση αγορά προϊόντων και υπηρεσιών χωρίς να βγει από το χώρο του (e-shops)
- Στον προγραμματισμό των διακοπών του με επίσκεψη σε τουριστικά, περιγητικά, online κρατήσεων εισιτηρίων και καταλυμάτων web sites
- Στην διαχείριση των χρημάτων του μέσω εφαρμογών e-banking, e-trading κ.λπ.

- Στην παρακολούθηση θεμάτων που αφορούν την υγεία του μέσω του ηλεκτρονικού φακέλου υγείας και γενικά του προγράμματος e-health
- Στην παρακολούθηση online μαθημάτων μέσω πλατφορμών e-learning

1.5.2.2 Ενίσχυση της Επικοινωνίας σε όλα τα επίπεδα

- Ένα ισχυρό μέσο επικοινωνίας ουσιαστικά απελευθερώνεται.
- Αμεσότερη επικοινωνία, ευκολότερα, ταχύτερα και οικονομικότερα.
- Επικοινωνία σε όλα τα επίπεδα χωρίς χρονικούς και γεωγραφικούς περιορισμούς.

1.5.2.3 Εξοικονόμηση χρόνου

- Καλύτερη διαχείριση του χρόνου τόσο σε προσωπικό, όσο και επαγγελματικό επίπεδο.
- Ταχύτερη πρόσβαση στην πληροφορία.
- Ταχύτερη επικοινωνία και μεταφορά μεγαλύτερου όγκου δεδομένων δια μέσου της ευρυζωνικής πρόσβασης και των υπηρεσιών της.

1.5.2.4 Νέοι ορίζοντες στην εκπαίδευση

- Νέα μέσα διδασκαλίας.
- Εμπλουτισμός διδακτέας ύλης με διαδραστικό τρόπο.
- Αλλαγή τρόπου μετάδοσης της γνώσης.
- Παροχή εξατομικευμένων εκπαιδευτικών λύσεων.
- Αναβάθμιση και εκσυγχρονισμός μορφωτικού επιπέδου.
- Αναβάθμιση της εκπαίδευσης ομάδων πολιτών που δεν μπορούν να απολαύσουν το αναφαίρετο δικαίωμα της μάθησης και της εκπαίδευσης (π.χ. άτομα με ειδικές ανάγκες).

1.5.2.5 Βελτίωση της σχέση του ατόμου με το κράτος

- Καλύτερη παροχή υπηρεσιών στον πολίτη ο οποίος αποδεσμεύεται από γραφειοκρατικές, χρονοβόρες διαδικασίες.

- Χρησιμοποίηση του κρατικού μηχανισμού ως αρωγό στην αναβάθμιση της ποιότητας ζωής του πολίτη με εφαρμογές όπως η ηλεκτρονική υποβολή φορολογικής δήλωσης, η ηλεκτρονική έκδοση φορολογικής ενημερότητας, πιστοποιητικών, η ηλεκτρονική πληρωμή φόρων, η ενημέρωση μέσα από ειδικές πύλες για προγράμματα, επιδοτήσεις κ.α.

1.5.2.6 Ποιοτικότερες και οικονομικότερες υπηρεσίες Διαδικτύου

Η αναβάθμιση της ποιότητας αφορά το επίπεδο, τους τρόπους, την ταχύτητα, την αξιοπιστία, την υποστήριξη της πρόσβασης και τις ηλεκτρονικές υπηρεσίες περιεχόμενου που καλύπτει τους χρηστές σε όλους τους τομείς και τους προσφέρει αυξημένες δυνατότητες, όπως ευρεία επικοινωνία και άμεση πρόσβαση στην πληροφορία. Η δυνατότητα για οικονομικότερη υπηρεσία είναι εύκολο να γίνει κατανοητή. Από την στιγμή που το Διαδίκτυο αναπτύσσεται και διεισδύει περισσότερο στην Ελληνική πραγματικότητα, οι εταιρείες παροχής υπηρεσιών Διαδικτύου είναι σε θέση να προσφέρουν και μεγαλύτερο εύρος υπηρεσιών σε χαμηλότερες τιμές λόγω της υγιούς ανάπτυξης του ανταγωνισμού.

1.5.3 Επιχειρήσεις

1.5.3.1 Επέκταση επιχειρηματικών δραστηριοτήτων

- Διεύρυνση των αγορών.
- Αύξηση των κερδών.
- Δημιουργία νέων τρόπων προώθησης των προϊόντων / υπηρεσιών.
- Αναβάθμιση της εξυπηρέτησης των πελατών.
- Περιορισμός των μειονεκτημάτων του μικρού μεγέθους, της απόστασης από τα κέντρα αποφάσεων και τις αγορές
- Πρόσβαση και ένταξη στην παγκόσμια αγορά, μέσα από εφαρμογές ηλεκτρονικού εμπορίου, help desk, e-market places κ.λπ.

1.5.3.2 Αύξηση της ανταγωνιστικότητας

- Βελτίωση της εικόνας.
- Αναβάθμιση των προϊόντων / υπηρεσιών.
- Βελτίωση της εξυπηρέτησης των πελατών.
- Χρησιμοποιώντας το μέσο για την προώθηση (interactive marketing) και διάθεση των προϊόντων / υπηρεσιών (e-commerce, interactive web sites), αλλά και κατ' επέκταση για άλλους τομείς όπως την εξυπηρέτηση, την επικοινωνία με τους πελάτες μέσω online help desks, chat servers, forums κ.α., η επιχείρηση οδηγείται στην επίτευξη στρατηγικών πλεονεκτημάτων που έχει ως αποτέλεσμα την αύξηση της ανταγωνιστικότητας της επιχείρησης στις δύσκολες οικονομικές συνθήκες της αγοράς.

1.5.3.3 Διεύρυνση του πελατολογίου

Χρησιμοποιώντας το Διαδίκτυο για έρευνες αγοράς, micro-marketing, προώθηση προϊόντων, διανομή, επικοινωνία με το κοινό / πελάτες και προμηθευτές, ενημέρωση για νέα προϊόντα, ακόμα και για αναζήτηση πληροφοριών από εξωτερικούς αναλυτές (έρευνες, μελέτες, άρθρα), οι εταιρείες έχουν την ευκαιρία να διευρύνουν το πελατολόγιο τους.

1.5.3.4 Αναβαθμισμένη και αμεσότερη επικοινωνία με πελάτες προμηθευτές.

Με την ανάπτυξη του Διαδικτύου, των τεχνολογιών επικοινωνίας, και των δικτύων υπολογιστών, corporate web sites, Internet based extranets, εφαρμογές VPN, mobile WAN, multimedia e-messaging κ.λπ., προμηθευτές και πελάτες έρχονται πιο κοντά και η επικοινωνία τους γίνεται αποτελεσματικότερη και αποδοτικότερη.

1.5.3.5 Αύξηση της παραγωγικότητας - μείωση των λειτουργικών εξόδων

- Ουσιαστική εξοικονόμηση πολύτιμου χρόνου μέσω των ευρυζωνικών υπηρεσιών και εφαρμογών
- Αύξηση της παραγωγικότητας της επιχείρησης
- Μείωση των λειτουργικών εξόδων εφόσον οι παραπάνω εργασίες εκτελούνται ηλεκτρονικά.

1.5.3.6 Ποιοτικότερες και οικονομικότερες υπηρεσίες Διαδικτύου

Η αναβάθμιση της ποιότητας αφορά το επίπεδο της πρόσβασης, τους τρόπους, την ταχύτητα, την αξιοπιστία, την υποστήριξη, την ανάπτυξη εφαρμογών και περιεχομένου που καλύπτει τους χρηστές σε όλους τους τομείς και τους προσφέρει αυξημένες δυνατότητες όπως ευρεία και εύκολη επικοινωνία και άμεση πρόσβαση στην πληροφορία. Η δυνατότητα για οικονομικότερη υπηρεσία είναι εύκολο να γίνει κατανοητή. Από την στιγμή που το Διαδίκτυο αναπτύσσεται και διεισδύει όλο και περισσότερο στην Ελληνική πραγματικότητα, οι εταιρείες παροχής υπηρεσιών Διαδικτύου είναι σε θέση να προσφέρουν μεγαλύτερο εύρος υπηρεσιών και σε πιο προσιτές τιμές.

1.5.4 Κράτος

1.5.4.1 Εκσυγχρονισμός του κράτους - βελτίωση των υπηρεσιών προς τον πολίτη

- Οργάνωση των πληροφοριών.
- Αυτοματοποίηση των διαδικασιών.
- Η δημόσια διοίκηση εκσυγχρονίζεται, αναδιοργανώνεται, εναρμονίζεται με τα ευρωπαϊκά δεδομένα, αποκτά διαφάνεια και εξελίσσεται σε αποτελεσματικό φορέα.

1.5.4.2 Προστασία και προβολή της Ελληνικής πολιτιστικής ταυτότητας

- Προώθηση του Ελληνικού πολιτισμού παγκόσμια.

- Προστασία της πολιτιστικής κληρονομιάς και της σύγχρονης δημιουργίας.
- Αξιοποίηση πολιτιστικού περιεχόμενου.
- Ο Ελληνικός πολιτισμός τεκμηριώνεται, προβάλλεται και διαφυλάσσεται μέσα από εφαρμογές ηλεκτρονικών μουσείων, βιβλιοθηκών, πινακοθηκών κ.λπ.

1.5.4.3 Προώθηση του Ελληνικού τουρισμού

- Προβολή και ανάπτυξη του Ελληνικού τουρισμού μέσα από πύλες ενημέρωσης, εφαρμογές ηλεκτρονικών κρατήσεων καταλυμάτων, εισιτηρίων κ.λπ.
- Ο τουρισμός, ένα από τα ισχυρότερα εθνικά προϊόντα αποκτά μεγαλύτερη προβολή παγκοσμίως.

1.5.4.4 Συμβολή στην αναβάθμιση της παιδείας

Η ενσωμάτωση του Διαδικτύου στην εκπαιδευτική διαδικασία διαμορφώνει νέα δεδομένα στο σύνολο του εκπαιδευτικού συστήματος και συμβάλλει ουσιαστικά στην ανάπτυξη του μέσου στην Ελλάδα. Η αξιοποίησή του ως εργαλείο για την εκπαίδευση, συμβάλει ουσιαστικά στον εκσυγχρονισμό του Ελληνικού εκπαιδευτικού συστήματος.

1.5.4.5 Συμβολή στην οικονομική ανάπτυξη

Σε παγκόσμιο επίπεδο κρατικοί και δημόσιοι φορείς είναι ο μεγαλύτερος πελάτης των τηλεπικοινωνιακών οργανισμών καταβάλλοντας τεράστια τέλη. Με την ανάπτυξη του Διαδικτύου και των ευρυζωνικών υπηρεσιών παρέχεται η δυνατότητα μείωσης του κόστους και η σημαντική βελτίωση των νέων επιχειρηματικών σχημάτων μεταξύ των ιδιωτικών και δημόσιων φορέων. Η ανάπτυξη υποδομών και υπηρεσιών Διαδικτύου είναι στρατηγικής σημασίας για την Ελλάδα εφόσον μπορεί να προσδώσει σημαντική ώθηση στις οικονομικές δραστηριότητες της χώρα.

1.5.4.6 Βελτίωση της εικόνας του κράτους και εθνική ανταγωνιστικότητα

- Βελτίωση της εικόνας της κρατικής μηχανής τόσο ως προς τον πολίτη όσο και ως προς τις υπόλοιπες χώρες.
- Ενίσχυση της ανταγωνιστικότητας της χώρας και κατά συνέπεια οικονομική ανάπτυξη.

1.5.4.7 Διεύρυνση δυνατοτήτων στην έρευνα και στην ανάπτυξη

Η επιστημονική έρευνα αποτελεί βασικό παράγοντα για την πρόοδο και ευημερία της χώρας. Η ανάπτυξη του Διαδικτύου βοηθά στην αξιοποίηση των νέων τεχνολογιών στην επιστημονική έρευνα και στην διάχυση των αποτελεσμάτων της μέσω της ενοποίησης των επιστημονικών φορέων, της βελτίωσης των υποδομών και των δικτύων επικοινωνίας μεταξύ τους.

1.5.4.8 Ενίσχυση της περιφέρειας

Για τις επιχειρήσεις και τον πολίτη που δραστηριοποιούνται στην περιφέρεια, η ανάπτυξη του Διαδικτύου μπορεί να συμβάλλει καταλυτικά στην εξέλιξή τους σε όλους τους τομείς δραστηριότητας. Το Διαδίκτυο αποτελεί κινητήρια δύναμη της περιφέρειας τόσο στους τομείς οικονομικής ανάπτυξης και ανταγωνιστικότητας όσο και στην καθημερινότητα και στον δημόσιο βίο. Ο στόχος της μεγαλύτερης ανάπτυξης του Διαδικτύου στην Ελληνική περιφέρεια αποτελεί ουσιαστικό μέτρο κατά του οικονομικού και κοινωνικού αποκλεισμού των περιφερειών και της δημιουργίας τοπικών και εθνικών ανισοτήτων.

2. ΚΙΝΔΥΝΟΙ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΑΠΟ ΕΝΗΛΙΚΕΣ

2.1 Κακόβουλο λογισμικό[17]

Το κακόβουλο λογισμικό (malware) είναι λογισμικό που αναπτύχθηκε με σκοπό την επίθεση σε ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να περιλαμβάνει, ιούς, σκουλήκια, λογισμικό υποκλοπής και άλλα καταστρεπτικά προγράμματα που μπορούν να κρυφτούν στον υπολογιστή και να δημιουργήσουν προβλήματα. Περισσότερο επικίνδυνο είναι το γεγονός ότι το κακόβουλο λογισμικό μπορεί να παρακολουθήσει τις συνήθειες περιήγησης, να αποσπάσει κωδικούς πρόσβασης, καθώς επίσης και να επιτρέψει σε κάποιον εισβολέα να πάρει τον έλεγχο του υπολογιστή.

Το κακόβουλο λογισμικό μπορεί είτε να εγκατασταθεί από μόνο του στον υπολογιστή χωρίς να το γνωρίζει ο χρήστης, είτε να εγκατασταθεί μαζί με κάποιο άλλο πρόγραμμα. Για παράδειγμα, ο χρήστης μπορεί να νόμισε ότι κατέβασε κάποιο βιντεοπαιχνίδι στο οποίο να κρύβεται κάποιο είδος κακόβουλου λογισμικού.

2.1.1 Τρόποι μόλυνσης[18]

Η διαδικασία της μόλυνσης / μετάδοσης συνήθως εκτελείται με έναν από τους ακόλουθους τρόπους:

Μέσω ηλεκτρονικής αλληλογραφίας: Το κακόβουλο λογισμικό βρίσκεται συνημμένο σε ένα μήνυμα ηλεκτρονικής αλληλογραφίας. Η αποστολή του μηνύματος μπορεί να είναι είτε ηθελημένη από κάποιον τρίτο, είτε ως αποτέλεσμα αυτόματης μετάδοσης (π.χ. mail worm).

Μέσω αφαιρούμενων αποθηκευτικών μέσων: (floppy, CD, DVD, USB disks, zip,). Ο τρόπος αυτός μόλυνσης ήταν και είναι ο πλέον δημοφιλής στην κατηγορία των κλασσικών ιών.

[17] http://www.microsoft.com/hellas/
[18] http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf

Μέσω Web: Εκτελέσιμος κώδικας ενσωματωμένος σε σελίδες html.

Μέσω άλλων υπηρεσιών διαδικτυακής επικοινωνίας: Υπηρεσίες συνομιλίας σε πραγματικό χρόνο (Instant messengers, Internet telephony, video conferencing, IRC clients) υπηρεσίες ομάδων συζήτησης (newsgroups), προγράμματα ανταλλαγής αρχείων (peer to peer) κ.λ.π

Μέσω Δικτύων (LAN, WAN): Το κακόβουλο λογισμικό (π.χ. τύπου worm) εκμεταλλεύεται ευπάθειες δικτυακών πρωτοκόλλων, υπηρεσιών, εφαρμογών και δικτυακών λειτουργικών συστημάτων ώστε να μεταδίδεται αυτόματα μέσω τοπικών δικτύων ή Δικτύων Ευρείας Περιοχής που εκτελούν την οικογένεια πρωτοκόλλων TCP/IP. Παραδείγματα αποτελούν οι επιθέσεις υπερχείλισης καταχωρητή (buffer overflow) τις οποίες χρησιμοποιούν αρκετά worms για να εξαπλωθούν. Επίσης, η κοινή χρήση αρχείων, εγγράφων και φακέλων σε τοπικά δίκτυα, διευκολύνει την εξάπλωση του κακόβουλου λογισμικού (όλων των κατηγοριών). Σε ένα παρεμφερές σενάριο, το κακόβουλο λογισμικό αντιγράφει τον εαυτό του στους φακέλους με τα διαμοιραζόμενα αρχεία που χρησιμοποιούν οι εφαρμογές ανταλλαγής αρχείων (P2P).

2.1.2 Παρενέργειες[19]

Οι παρενέργειες ενός κακόβουλου λογισμικού ποικίλλουν:

- Ενοχλητικά μηνύματα, διαφημίσεις κ.λπ. (adware)
- Επιθέσεις υποκλοπής δεδομένων και πληροφοριών
    - Επιθέσεις διακοπής, αλλοίωσης, εισαγωγής
    - Διαγραφή ή αλλοίωση δεδομένων, εφαρμογών και αρχείων συστήματος
    - Αντιγραφή αρχείων στο τοπικό δίκτυο (μετάδοση μέσω κοινής χρήσης αρχείων) ή στο Διαδίκτυο (για μετάδοση μέσω των προγραμμάτων P2P)

[19] http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf

- Αναστολή λειτουργίας ή δυσλειτουργία του λειτουργικού συστήματος
- Καταστροφή των τομέων εκκίνησης (boot sectors), πινάκων καταχώρησης αρχείων (FAT), και πινάκων κατατμήσεων (partition tables)

- Δημιουργία «κερκόπορτας» (back door) με σκοπό την (μετέπειτα) παραβίαση της ασφάλειας του συστήματος
- Επιθέσεις εναντίον της διαθεσιμότητας συστημάτων
  - Κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος)
  - Κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος)
  - Κατανάλωση της χωρητικότητας (bandwidth) του δικτύου
  - Χρήση των ξενιστών για συγχρονισμένη επίθεση σε κάποιον τρίτο, στα πλαίσια μιας επίθεσης DDOS (Distributed DOS).

2.1.3 Ιός[20]

Ένας ιός (virus) υπολογιστή είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του, ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό.

Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB.

Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα «σκουλήκια» υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα σκουλήκι μπορεί να

[20] http://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_(%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82)

διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του.

Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο, την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του, είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές φορές μάλιστα, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι «καλοκάγαθοι» ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.

Έως σήμερα έχουν δημιουργηθεί και κυκλοφορήσει χιλιάδες ιοί, αρκετοί από τους οποίους είναι πολύ επικίνδυνοι, όταν προσβάλλουν κάποιο υπολογιστικό σύστημα ή δίκτυο. Εκτιμάται ότι το έτος 2000 υπήρχαν περίπου 50.000 γνωστοί ιοί, ενώ σήμερα ο αριθμός τους έχει υπερβεί τις 60.000. Οι περισσότεροι είναι γραμμένοι για υπολογιστές με λειτουργικά συστήματα MS-DOS και/ή

Windows. Αυτό πιστεύεται ότι οφείλεται είτε στην αυξημένη διάδοση των συστημάτων αυτών, είτε στα κενά ασφάλειας που παρουσιάζουν και κάνουν ευκολότερη τη μόλυνση του συστήματος και τη διάδοσή τους.

2.1.3.1 Τρόπος δράσης και διάδοσης

Ανεξάρτητα από το τι και πώς μολύνει σε ένα σύστημα, ο ιός πρέπει να εξασφαλίσει ορισμένες βασικές συνθήκες, προκειμένου να δράσει. Συγκεκριμένα, πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (στο σκληρό δίσκο, αλλά όχι μόνο). Γι' αυτό το λόγο πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος, είτε του κανονικού λογισμικού ενός συστήματος. Εξασφαλίζουν έτσι δύο πράγματα: Πρώτον, ότι θα μπορούν να αυτοαντιγραφούν και δεύτερον ότι θα μπορέσουν να εκτελέσουν τον κώδικά τους.

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης, είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιϊκό πρόγραμμα, πριν επιτρέψουν στο χρήστη να τα λάβει.

2.1.3.2 Τύποι ιών

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

- Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:
    - Τομείς σκληρού δίσκου συστήματος (system sectors)
    - Αρχεία
    - Ιοί μακροεντολών (macros)
    - Ιοί πηγαίου κώδικα (source code viruses)

- Ιοί συμπλεγμάτων σκληρού δίσκου (hard disk clusters)

- Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:
  - Πολυμορφικοί ιοί
  - Αόρατοι ιοί (stealth viruses)
  - Θωρακισμένοι ιοί (armored viruses)
  - Πολυτμηματικοί ιοί (multipartite viruses)
  - Ιοί πλήρωσης κενών (spacefiller viruses)
  - Ιοί παραλλαγής (camouflage viruses)

2.1.3.3 Τρόποι αντιμετώπισης

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη. Ορισμένοι μάλιστα, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία.

Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους πρόσφατα δημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να «καθαρίσουν» τυχόν μολυσμένα αρχεία που εντοπίζουν.

Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας

τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι χρηματικού ποσού (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα).

Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του «προϊόντος» τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του, αλλά και να δημιουργεί τις ειδικές δισκέτες (τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους), ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

2.1.4 Δούρειος ίππος[21]

Στην επιστήμη υπολογιστών, ο δούρειος ίππος (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία, ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.

Συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί.

Συνήθως, αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να

[21] http://el.wikipedia.org

έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του Διαδικτύου.

Άλλες επιπτώσεις από την εκτέλεση ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του, απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή, απενεργοποίηση προγραμμάτων firewall ή αντιϊκών.

Γενικά οι δούρειοι ίπποι δεν μπορούν να πολλαπλασιαστούν όπως οι ιοί. Ένας δούρειος ίππος μπορεί να δράσει και ως κατάσκοπος, δηλαδή να ξεκινήσει να καταγράφει οτιδήποτε πληκτρολογείται στο πληκτρολόγιο. Έτσι θα συλλέξει πληροφορίες κωδικών πρόσβασης, λογαριασμών, πιθανών τραπεζικών συναλλαγών και άλλα προσωπικά δεδομένα.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι χρήστες πάντα προτρέπονται να μην ανοίγουν ύποπτα αρχεία επισυναπτόμενα σε e-mail. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη μέσω e-mail. Υπάρχει περίπτωση να το έχει κατεβάσει από μια ιστοσελίδα, μέσω προγραμμάτων Instant Messaging, ή από CD και DVD.

Τέλος, στην επιστήμη της αρχιτεκτονικής υπολογιστών, η λέξη «δούρειος ίππος» μπορεί επίσης να αναφέρεται και σε κενά ασφαλείας που επιτρέπουν σε διάφορα προγράμματα να διαβάσουν αρχεία χωρίς εξουσιοδότηση.

2.1.4.1 Τύποι δούρειων ίππων

Υπάρχουν δύο είδη δούρειων ίππων:

- Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι χάκερς μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer-to-peer), προγράμματα ανακοίνωσης καιρικών συνθηκών, κ.λπ.
- Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Οι τύποι δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω στις εξής κατηγορίες ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή:

- Απομακρυσμένη πρόσβαση.
- Αποστολή e-mail.
- Καταστροφή αρχείων.
- Κατέβασμα αρχείων.
- Proxy trojan.
- FTP trojan (προσθήκη, διαγραφή ή μεταφορά αρχείων από τον μολυσμένο υπολογιστή).
- Απενεργοποίηση λογισμικού ασφαλείας (firewall, αντιϊκά κ.λπ.).
- Denial of Service (DoS).
- URL trojan (επιτρέπει στον υπολογιστή να συνδεθεί στο Διαδίκτυο μόνο μέσω μίας πολύ ακριβής σύνδεσης).

2.1.5 Σκουλήκι[22]

Το σκουλήκι (worm) είναι ένα πρόγραμμα το οποίο έχει δυνατότητες πολλαπλασιασμού του εαυτού του και εξαπλώνεται από υπολογιστή σε υπολογιστή χωρίς να το γνωρίζει ο χρήστης. Λόγω του ότι τα σκουλήκια χρησιμοποιούν τις δικτυακές συνδέσεις για να εξαπλωθούν, μπορούν να έχουν υπερβολικά γρήγορη εξάπλωση και να δημιουργήσουν μεγάλη δικτυακή κίνηση, μειώνοντας την ταχύτητα ή μη επιτρέποντας τη νόμιμη πρόσβαση στο δίκτυο.

Τα σκουλήκια δεν είναι τόσο καταστροφικά όσο οι ιοί γιατί δεν σβήνουν αρχεία, όμως κάνουν τη σύνδεση στο Διαδίκτυο πιο αργή επειδή στέλνουν τα αντίγραφα τους σε άλλους ηλεκτρονικούς υπολογιστές. Επίσης κάνουν το σύστημα του υπολογιστή πιο αργό χρησιμοποιώντας πολύ μνήμη με το να αντιγράφουν τον εαυτό τους άπειρες φορές και γεμίζοντας τον ελεύθερο χώρο του σκληρού δίσκου. Υπάρχουν όμως και ορισμένα σκουλήκια που έχουν ταυτόχρονα ιδιότητες ιών, πράγμα που τα καθιστά πιο επικίνδυνα από τα συνηθισμένα σκουλήκια.

2.1.6 Λογισμικό υποκλοπής[23]

Το λογισμικό υποκλοπής (spyware) είναι λογισμικό το οποίο εκτελεί συγκεκριμένες ενέργειες, όπως υποκλοπή και συγκέντρωση προσωπικών δεδομένων, αλλαγή των ρυθμίσεων του υπολογιστή χωρίς τη συγκατάθεσή του χρήστη. Οι πληροφορίες αυτές περιλαμβάνουν (χωρίς να περιορίζονται από) προσωπικά στοιχεία, ονόματα χρήστη (usernames), κωδικούς πρόσβασης (passwords), κωδικούς TAN (Transaction Authorization Number), κλειδιά, αριθμούς πιστωτικής κάρτας, λεπτομέρειες συναλλαγών. Στη χείριστη του μορφή παίρνει τη μορφή λογισμικού keylogger που υποκλέπτει κάθε χαρακτήρα

[22] http://www.dart.gov.gr/
http://www.itsecurity.gr
[23] http://www.dart.gov.gr
http://www.microsoft.com/

που πληκτρολογεί ο χρήστης και τα προωθεί (στο παρασκήνιο) π.χ. μέσω e-mail σε τρίτους.

Το λογισμικό υποκλοπής συχνά σχετίζεται με λογισμικό που προβάλλει ανεπιθύμητες διαφημίσεις (adware) ή λογισμικό που ανιχνεύει προσωπικά ή ευαίσθητα δεδομένα. Αυτό δεν σημαίνει ότι κάθε διαφημιστικό λογισμικό ή λογισμικό που παρακολουθεί τις ενέργειές του χρήστη στο Διαδίκτυο είναι επιζήμιο. Για παράδειγμα, μπορεί ο χρήστης να εγγραφεί σε μια δωρεάν υπηρεσία λήψης μουσικής και να δεχτεί, αντί για την καταβολή κάποιας συνδρομής, να λαμβάνει διαφημιστικά μηνύματα. Εάν κατανοεί τους όρους και συμφωνεί, μπορεί να αποφασίσει ότι πρόκειται για δίκαιη συναλλαγή. Μπορεί, επίσης, να συμφωνήσει η εταιρεία να παρακολουθεί τη δραστηριότητά του στο Διαδίκτυο, προκειμένου να προσδιορίζει ποιες διαφημίσεις θα προβάλλονται. Κάποια άλλα είδη λογισμικού υποκλοπής ενδέχεται να προκαλέσουν αλλαγές στον υπολογιστή που είναι ενοχλητικές και μπορεί να μειώσουν την ταχύτητά του ή να τον κάνουν να «κολλάει».

Όταν το λογισμικό υποκλοπής εγκατασταθεί στον υπολογιστή, το πρώτο πράγμα που κάνει είναι να ενημερώσει τον αποστολέα του ότι έχει πλέον τον έλεγχο του υπολογιστή. Έτσι, ο απομακρυσμένος χάκερ μπορεί να χειριστεί τον υπολογιστή του χρήστη, ο οποίος δεν γνωρίζει καν τι συμβαίνει. Με τον τρόπο αυτό, δημιουργούνται ολόκληρα δίκτυα από «υπολογιστές-ζόμπι» που χρησιμοποιούνται για επιθέσεις DOS (Denial of Service) σε servers μεγάλων συνήθως εταιρειών.

Το λογισμικό υποκλοπής δεν έχει άμεση εξάπλωση όπως οι ιοί ή τα σκουλήκια. Γενικά, ένα μολυσμένο σύστημα δεν επιχειρεί να μεταδώσει την μόλυνση σε άλλους υπολογιστές. Αντ' αυτού, το λογισμικό υποκλοπής εισχωρεί στο σύστημα μέσω της εξαπάτησης του χρήστη ή μέσω της εκμετάλλευσης των τρωτών σημείων του λογισμικού.

Όταν ο χρήστης εγκαθιστά κάποιο πρόγραμμα στον υπολογιστή, πρέπει να φροντίζει να διαβάζει προσεκτικά όλους τους όρους, συμπεριλαμβανομένης της

σύμβασης άδειας χρήσης και της δήλωσης σχετικά με την προστασία προσωπικών δεδομένων. Μερικές φορές η χρήση ανεπιθύμητου λογισμικού στην εγκατάσταση κάποιου λογισμικού τεκμηριώνεται, αλλά μπορεί να εμφανίζεται στο τέλος της σύμβασης άδειας χρήσης ή της δήλωσης σχετικά με την προστασία προσωπικών δεδομένων.

2.1.7 Ανεπιθύμητη διαφήμιση[24]

Ως ανεπιθύμητη διαφήμιση (adware) θεωρείται κάθε είδους λογισμικού το οποίο με αυτόματο τρόπο, εκτελεί, επιδεικνύει, ή λαμβάνει διαφημιστικό υλικό μέσω Διαδικτύου. Η εκτέλεση αυτού του λογισμικού μπορεί να γίνεται νόμιμα, στα πλαίσια μιας εφαρμογής που το ορίζει ρητώς στους όρους χρήσης της, ή με τρόπο μη φανερό. Στη δεύτερη περίπτωση τα λογισμικά τύπου adware θεωρούνται κακόβουλο λογισμικό. Το λογισμικό adware συνήθως συνεργάζεται με λογισμικό spyware (η λειτουργία του βασίζεται στα αποτελέσματα της λειτουργίας του spyware). Αν και μερικά adware θεωρούνται ακίνδυνα και αφορούν τεχνικές εμπορίας, θα πρέπει να είναι δικαίωμα του χρήστη να αποφασίσει ποιος μπορεί να παρακολουθεί προσωπικές και εμπιστευτικές πληροφορίες.

Οι παρενέργειες ενός λογισμικού adware ποικίλουν:

- εμφάνιση ανεπιθύμητων μηνυμάτων στον φυλλομετρητή (browser), ή στην επιφάνεια εργασίας
- αλλαγή της αρχικής σελίδας του φυλλομετρητή (μια επίθεση γνωστή και ως browser hijacking)
- αλλαγή της αρχικής σελίδας αναζήτησης στο Διαδίκτυο.
- αναδρομολόγηση σε λανθασμένο (πλαστό) δικτυακό τόπο (web spoofing)
- αργοπορία δικτύου και υπολογιστή

[24] http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf
http://noc.chania.teicrete.gr/docs/security.pdf

- ενοχλητικά διαφημιστικά παράθυρα (pop-ups)

2.1.8 Dialers[25]

Οι dialers είναι μικρά προγράμματα (συνήθως μόνο 50 με 80 kb σε μέγεθος) τα οποία έχουν τη δυνατότητα να αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Διαδικτύου (ISP) και να καλούν αυτόματα ένα υψηλής χρέωσης αριθμό (π.χ. 901 ή αριθμούς εξωτερικού π.χ. 00xx) για πρόσβαση σε συγκεκριμένες υπηρεσίες χωρίς την συνειδητή συγκατάθεση του χρήστη.

Τα προγράμματα αυτά, αρχικά δημιουργήθηκαν για την εξυπηρέτηση πληρωμών μικρών ποσών, δίνοντας τη δυνατότητα στο χρήστη να εισέρχεται σε συγκεκριμένες ιστοσελίδες (pay per view websites) και να χρεώνεται στον τηλεφωνικό του λογαριασμό για το περιεχόμενο που λαμβάνει. Δυστυχώς όμως, λόγω του «εύκολου χρήματος» τα προγράμματα αυτά αποτελούν μία σημαντική απειλή στο χώρο του Διαδικτύου.

Οι δύο συνηθέστεροι τρόποι που μπορούν να δράσουν οι dialers είναι οι εξής:

- Μπορούν να αλλάξουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (Dial Up Networking) έτσι ώστε να υποχρεώσουν το χρήστη να καλέσει έναν συγκεκριμένο αριθμό (συνήθως διεθνή κλήση σε αριθμό υψηλού κόστους) άγνωστο στο χρήστη. Διαγράφουν τον αριθμό του παρόχου υπηρεσιών Internet (ISP) που χρησιμοποιεί ο χρήστης και αντικαθιστούν αυτόν τον αριθμό με τον δικό τους. Κατόπιν, αυτός ο αριθμός χρησιμοποιείται κάθε φορά που συνδέεται ο χρήστης στο Διαδίκτυο αντί για τον αριθμό του παρόχου υπηρεσιών Internet (ISP).
- Μπορούν να αναγκάσουν τον υπολογιστή να παρακάμψει τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (Dial Up Networking) και να καλέσει ένα συγκεκριμένο αριθμό. Παρόλο που μπορεί να εμφανίζονται οι

[25] http://www.forthnet.gr/templates/viewcontentTmArt.aspx?p=102396
http://www.otenet.gr/hd/abuse/abuse_xrewseis.htm
http://support.hol.gr/uploads/pdf/dialers_info.pdf

προεπιλεγμένες ρυθμίσεις του χρήστη όταν συνδέεται στο Διαδίκτυο, θα καλείται ένας άλλος αριθμός που θα έχει οριστεί από τον dialer (συνήθως διεθνή κλήση σε αριθμό υψηλής χρέωσης).

2.1.8.1 Τρόποι μόλυνσης

Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Αυτές μπορεί να είναι ιστοσελίδες που παρέχουν πειρατικό λογισμικό, ιστοσελίδες με πορνογραφικό περιεχόμενο, ή ιστοσελίδες με αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των ιστοσελίδων έχουν το dialer λογισμικό ενσωματωμένο στον κώδικα της ιστοσελίδας τους ώστε να γίνεται download και να εγκαθίσταται αυτόματα στο σύστημα του χρήστη, χωρίς να γίνεται αντιληπτό και χωρίς να ζητάει απαραίτητα την συγκατάθεση του. Ένας άλλος τρόπος εμφάνισης αυτών των προγραμμάτων είναι με τη μορφή συνημμένων αρχείων σε ηλεκτρονικά μηνύματα αλληλογραφίας, που παρουσιάζονται ως δημοφιλή προγράμματα όπου εάν ο χρήστης τα αποθηκεύσει και τα εγκαταστήσει, εγκαθιστά εν αγνοία του την εφαρμογή dialer.

Η ιδέα πίσω από αυτά τα προγράμματα είναι ότι οι άνθρωποι που τα παράγουν μπορούν να αποκομίσουν έσοδα από τους χρήστες που καλούν τον αριθμό που είναι εγκατεστημένος στην ιστοσελίδα τους. Ο χρήστης αντιμετωπίζει αναπάντεχα αυξημένους λογαριασμούς τηλεφώνου, καθώς οι κλήσεις που κατευθύνουν τα προγράμματα αυτά μπορεί να φτάνουν και τα 2€ το λεπτό, αντί των 0,0058€ το λεπτό για ώρες αιχμής και 0,0029€ το λεπτό για ώρες μη αιχμής που είναι η χρέωση του Ενιαίου Πανελλαδικού Αριθμού Κλήσης (Ε.Π.Α.Κ.). Βάσει αυτών, διαφαίνεται ότι η χρέωση των κλήσεων σε αριθμούς υψηλής χρέωσης είναι κατά 689 φορές ακριβότερη από τη χρέωση Ε.Π.Α.Κ.

Πρέπει να σημειωθεί ότι τα προγράμματα dialer απειλούν κατά κύριο λόγο τους συνδρομητές υπηρεσιών PSTN ή ISDN και τα συστήματα που έχουν εγκατεστημένο modem (PSTN / ISDN) το οποίο είναι συνδεδεμένο σε τηλεφωνική γραμμή, ενώ οι συνδρομητές υπηρεσιών ADSL δεν διατρέχουν

κίνδυνο καθώς εξ' ορισμού δεν έχουν τη δυνατότητα να πραγματοποιήσουν τηλεφωνική κλήση μέσω modem και συνδέονται άμεσα με την υπηρεσία Διαδικτύου. Ωστόσο στην περίπτωση που ο υπολογιστής εκτός της ADSL σύνδεσης έχει εγκατεστημένο και κάποιο ISDN ή PSTN modem το οποίο είναι συνδεδεμένο σε τηλεφωνική γραμμή, τότε το σύστημα του είναι εξίσου τρωτό στους dialers.

2.1.8.2 Χαρακτηριστικά των dialers

Οι dialers συνήθως έχουν τις ακόλουθες παρενέργειες:

- Σπάνια υπάρχει κάποια ένδειξη στην ιστοσελίδα που να αναφέρεται στο «download» του dialer και σε μεμονωμένες περιπτώσεις ο χρήστης το αντιλαμβάνεται, καθώς δεν υπάρχει καμία ενημέρωση σχετικά με το κόστος της κλήσης.
- Το download σε πολλές περιπτώσεις ολοκληρώνεται ακόμη και αν ο χρήστης το ακυρώσει. Επίσης πολλές φορές αρχίζει χωρίς καν να το γνωρίζει / επιλέξει ο χρήστης.
- Υπάρχει παράκαμψη πολλές φορές της προεπιλεγμένης (default) σύνδεσης του χρήστη και ορίζεται ο dialer ως προεπιλεγμένη σύνδεση, χωρίς ειδοποίηση.
- Αν ο χρήστης είναι ήδη συνδεδεμένος, γίνεται αυτόματα διακοπή της πραγματοποιηθείσας σύνδεσης με τον ISP του χρήστη και ύστερα γίνεται πραγματοποίηση κλήσης, μέσω του εγκατεστημένου στον Η/Υ dialup modem, στο νούμερο ειδικής χρέωσης.
- Ο dialer πραγματοποιεί συνδέσεις από μόνος του.
- Οι χρεώσεις της σύνδεσης δεν εμφανίζονται πουθενά και ο λογαριασμός τηλεφώνου θα περιέχει κλήσεις σε διεθνείς προορισμούς και θα είναι υψηλότερος σε σχέση με τους προηγούμενους.

- Ένας dialer μπορεί να συνοδεύει και κάποια άλλη εφαρμογή. Επιπλέον, διάφορα trojans έχουν την δυνατότητα να κατεβάσουν και να εγκαταστήσουν dialer.
- Η ταχύτητα της σύνδεσή, πιθανόν να είναι μικρότερη από ότι συνήθως.
- Πολλές φορές ανοίγουν αυτόματα σελίδες «αμφιλεγόμενου περιεχομένου», χωρίς να έχει ζητηθεί κάτι τέτοιο από τον χρήστη.

2.1.8.3 Διάγνωση και αντιμετώπιση

Υπάρχουν συμπτώματα τα οποία μαρτυρούν την εγκατάσταση και λειτουργία ενός dialer στον υπολογιστή του χρήστη:

- Εμφάνιση άγνωστων/περίεργων εικονιδίων, είτε στην επιφάνεια εργασίας του υπολογιστή, είτε στον πίνακα ελέγχου.
- Ο χρήστης θα ακούσει το modem να αποσυνδέεται και να πραγματοποιεί νέα κλήση (εκτός εάν ο dialer έχει σιγήσει τους ήχους κλήσης).
- Είναι πιθανόν, η ταχύτητα της σύνδεσής να είναι πολύ χαμηλότερη από ότι συνήθως.
- Ο χρήστης θα λάβει έναν απρόσμενα υψηλό λογαριασμό τηλεφώνου, στον οποίο θα βρει κλήσεις σε άγνωστους αριθμούς υψηλής χρέωσης ή εξωτερικού.
- Είναι πιθανόν, παρά το γεγονός ότι ο χρήστης είναι συνδεμένος στο Διαδίκτυο, να μην μπορεί να στείλει ηλεκτρονικά μηνύματα (e-mails).

Υπάρχουν όμως τρόποι προστασίας από τους dialers:

- Μία λύση είναι η φραγή διεθνών κλήσεων στην γραμμή του τηλεφώνου. Βέβαια αυτός ο τρόπος για ορισμένους ανθρώπους μπορεί να αποτελεί και εμπόδιο, αλλά αποτελεί τη μοναδική, προς στιγμήν, σίγουρη λύση.
- Αποφυγή επισκέψεων σε ιστοσελίδες αμφιλεγόμενου περιεχομένου.

- Εάν κατά λάθος ο χρήστης βρεθεί σε μία τέτοια ιστοσελίδα, θα πρέπει να κλείσει όλα τα παράθυρα που «πετάγονται» (pop up).
- Αποφυγή download ή εγκατάσταση οποιονδήποτε προγραμμάτων από τέτοιες ιστοσελίδες.
- Απενεργοποίηση του υπολογιστή και του modem όταν δεν χρησιμοποιούνται.
- Βεβαίωση ότι έχει ρυθμιστεί ο ήχος του modem έτσι ώστε να ακούγεται όταν πραγματοποιεί κλήση. Πολλοί χρήστες χαμηλώνουν την ένταση ήχου κλήσης του modem και με αυτόν τον τρόπο δεν μπορούν να το ακούσουν όταν κάνει επανάκληση.
- Ο χρήστης θα πρέπει να μην ανοίγει συνημμένα αρχεία που λαμβάνει μέσω e-mail από άγνωστους αποστολείς.

2.1.9 Ανεπιθύμητη αλληλογραφία[26]

Η ραγδαία εξάπλωση του Διαδικτύου είχε ως άμεσο αποτέλεσμα τη χρησιμοποίηση της υπηρεσίας ηλεκτρονικού ταχυδρομείου (e-mail) για διαφημιστικούς και όχι μόνο σκοπούς. Το αρχικό πλεονέκτημα της ελεύθερης μετάδοσης των δεδομένων, μέσα σε ελάχιστο χρόνο μετατράπηκε στο μεγαλύτερο σύγχρονο πρόβλημα της διεθνούς online κοινότητας: την ανεπιθύμητη αλληλογραφία (spam mail). Η έννοια του spamming ορίζεται ως οποιοσδήποτε τύπος ανεπιθύμητου εμπορικού e-mail (unsolicited commercial e-mail ή unsolicited bulk e-mail) με οποιονδήποτε σκοπό.

Τα κυριότερα χαρακτηριστικά του spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

[26] http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?_list=whatis
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/PUBLICATIONS/ENTYPO_EKDILOSIS_LOW_1.PDF
http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10007627
http://www.dart.gov.gr/NewsInner.aspx?new_id=139&nwc_id=20

- **Απρόκλητο**: Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.
- **Εμπορικό**: Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών, με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.
- **Μαζικό**: Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών.

2.1.9.1 Επιπτώσεις

Μεγάλο ποσοστό χρηστών του ηλεκτρονικού ταχυδρομείου σίγουρα έχουν νιώσει την ενόχληση από την αποστολή τέτοιων απρόκλητων και ενοχλητικών μηνυμάτων. Ιδιαίτερο πρόβλημα αντιμετωπίζουν οι χρήστες που χρησιμοποιούν μεγάλα διαστήματα της μέρας το ηλεκτρονικό ταχυδρομείο και είναι αναγκασμένοι να σβήνουν όλη αυτή την ανεπιθύμητη αλληλογραφία.

Η αναγκαιότητα για την αντιμετώπιση του spam εντοπίζεται στα ακόλουθα σημεία:

- Είναι φαινόμενο δυσάρεστο και ενοχλητικό για τους παραλήπτες. Πολλές φορές προβάλει αμφίβολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων κ.λπ. Άλλα μηνύματα περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.
- Οδηγεί σε κατάχρηση πόρων του Διαδικτύου. Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με κατανάλωση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στα κεντρικά συστήματα διανομής

αλληλογραφίας (e-mai servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και στα συστήματα των χρηστών.

- Θέτει σε κίνδυνο την ασφάλεια και την αξιοπιστία του Διαδικτύου: Οι spammers βρίσκονται σε συνεχή αναζήτηση συστημάτων τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους. Πολλά μηνύματα αυτής της κατηγορίας μεταφέρουν επισυναπτόμενα τα οποία μπορεί να είναι ιοί ή δούρειοι ίπποι, οι οποίοι θέτουν σε κίνδυνο την ασφάλεια των συστημάτων.

2.1.9.2 Πρόληψη

Κάποια μέτρα που μπορεί να λάβει ο χρήστης για την αποφυγή του spam είναι:

- Να προσπαθεί να δίνει την διεύθυνση ηλεκτρονικού ταχυδρομείου του, κατά το δυνατόν μόνο σε πρόσωπα ή οργανισμούς που γνωρίζει και εμπιστεύεται.
- Αν χρειαστεί να δώσει την διεύθυνση του, π.χ. για εγγραφή σε κάποιο ηλεκτρονικό περιοδικό ή για τη χρήση κάποιας υπηρεσίας στο Διαδίκτυο, να βεβαιωθεί ότι παρέχεται η δυνατότητα να δηλώσει ότι δεν επιθυμεί την αποστολή διαφημιστικών μηνυμάτων.
- Να ελέγχει την πολιτική ιδιωτικότητας (privacy policy) των ιστοσελίδων που επισκέπτεται πριν αποκαλύψει τα προσωπικά του δεδομένα.
- Να βεβαιωθεί ότι υπάρχει δέσμευση της εταιρείας ή του οργανισμού να μην διαβιβάζουν τα προσωπικά δεδομένα σε τρίτους.
- Να αποφεύγει την δημοσιοποίηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου του σε ιστοσελίδες που δεν εμπιστεύεται, μηχανές αναζήτησης, ηλεκτρονικές λίστες, blogs ή chat rooms.

2.1.9.3 Αντιμετώπιση

Αν παρόλα αυτά ο χρήστης πέσει θύμα του spam, κάποια μέτρα που μπορεί να λάβει για την αντιμετώπιση του είναι:

- Να μην απαντάει ποτέ σε spam mail. Όταν κάποιος απαντάει σε μηνύματα spam, ουσιαστικά επαληθεύει την εγκυρότητα της διεύθυνσης ηλεκτρονικού ταχυδρομείου και ενθαρρύνει τους spammers να στέλνουν περισσότερα μηνύματα.
- Να μην ακολουθεί ποτέ συνδέσμους (links) που ενδεχομένως αναφέρονται στο μήνυμα, ακόμα και αν πρόκειται για συνδέσμους διαγραφής της διεύθυνσης του από την λίστα του αποστολέα (unsubscribe links).
- Να μην γράφεται ποτέ σε ιστοσελίδες που υπόσχονται να αφαιρέσουν το όνομά του από spam λίστες. Παρόλο που μερικά από αυτές τις ιστοσελίδες είναι νόμιμες, το πιθανότερο είναι ότι πρόκειται για συλλέκτες ηλεκτρονικών διευθύνσεων.
- Να σβήσει όλα τα e-mail που εμφανίζονται να πωλούν κάτι για το οποίο δεν έχει ζητήσει πληροφορίες. Τέτοιου είδους e-mail πιθανώς ανήκουν στην κατηγορία spam ή junk mail. Μερικές εταιρίες αποστέλλουν ένα μεγάλο αριθμό ηλεκτρονικών μηνυμάτων, με σκοπό την προσέλκυση νέων πελατών, τα οποία όμως είναι ενοχλητικά και η διαγραφή τους χρονοβόρα.
- Να αναφέρει προβλήματα spam στον πάροχο υπηρεσιών Διαδικτύου του, ζητώντας ενδεχομένως τη φραγή συγκεκριμένων διευθύνσεων από τις οποίες του αποστέλλονται μηνύματα spam. Επιπλέον, ο πάροχος μπορεί να τον βοηθήσει σχετικά με τη χρήση ειδικού λογισμικού φιλτραρίσματος ή άλλων μέτρων ασφαλείας για την αποφυγή λήψης μηνυμάτων spam.
- Να μην προωθεί τα spam mail σε γνωστούς του.
- Να καταγγείλει περιστατικά spam στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα μέσω της υπηρεσίας ηλεκτρονικής υποβολής καταγγελιών στην ιστοσελίδα http:\\www.dpa.gr ή μέσω ηλεκτρονικού ταχυδρομείου στο contact@dpa.gr.

- Να δηλώσει την εναντίωση του για την λήψη μηνυμάτων προς τον αποστολέα, στην οποία μπορεί να ζητάει την διαγραφή του από την λίστα.
- Να μην αφήνει ελκυστικούς τίτλους μηνυμάτων, όπως π.χ. «urgent and confidential» ή «I have money for you», να τον δελεάσουν.
- Να χρησιμοποιήσει τις λειτουργίες αυτόματης διαγραφής του λογισμικού διαχείρισης ηλεκτρονικής αλληλογραφίας. Αρκετά e-mail προγράμματα επιτρέπουν στον χρήστη να δημιουργήσει κανόνες αυτόματης διαγραφής. Χρησιμοποιώντας αυτήν την λειτουργία, θα μειώσει το χρόνο που ξοδεύει στη διαγραφή των spam mail.
- Να πληκτρολογήσει την ηλεκτρονική του διεύθυνση σε μία μηχανή αναζήτησης, για να βρει ιστοσελίδες που τυχόν διαθέτουν τη διεύθυνσή του και να ζητήσει από τους υπεύθυνους να την αφαιρέσουν.
- Να κρατήσει κρυφά τα στοιχεία που έχει δώσει σε υπηρεσίες όπως Instant Messenger, ICQ κ.λπ. Και αυτά αποτελούν μια περιοχή που εκμεταλλεύονται οι spammers. Να βεβαιωθεί ότι κάνει block το προφίλ του από όλους τους χρήστες όταν χρησιμοποιεί υπηρεσίες instant messaging.

2.1.9.4 Θεσμικό πλαίσιο

Στην Ελλάδα η μη ζητηθείσα επικοινωνία ρυθμίζεται από το αρ.11 του νόμου 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Αντίστοιχοι νόμοι υπάρχουν και στις λοιπές χώρες της Ε.Ε. βάσει της Οδηγίας 2002/58/ΕΚ.

Σύμφωνα με τον παραπάνω νόμο η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας επιτρέπεται μόνο αν ο παραλήπτης έχει συγκατατεθεί εκ των προτέρων ρητώς, ανεξάρτητα αν ο παραλήπτης είναι φυσικό ή νομικό πρόσωπο. Επομένως, κάθε ηλεκτρονικό μήνυμα (π.χ. e-mail, SMS, MMS, IM) που αποστέλλεται χωρίς ο χρήστης να

έχει προηγουμένως δώσει ρητά την συγκατάθεση του, δηλαδή κάθε μήνυμα spam, είναι παράνομο.

Εξαίρεση αποτελεί η περίπτωση κατά την οποία αποστέλλονται διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου από κάποιον με τον οποίο ο χρήστης είχε ήδη προηγούμενη συναλλαγή και είχε δηλώσει την ηλεκτρονική του διεύθυνση (π.χ. κατά την αγορά κάποιου προϊόντος ή υπηρεσίας). Σε αυτή την περίπτωση, η αποστολή των μηνυμάτων μπορεί να γίνεται για παρόμοια προϊόντα η υπηρεσίας, μέχρι ο χρήστης να δηλώσει ότι δεν επιθυμεί να λαμβάνει πλέον αυτά τα μηνύματα. Ο αποστολέας των μηνυμάτων οφείλει να παρέχει στον χρήστη την δυνατότητα εναντίωσης στην λήψη των μηνυμάτων με απλό και εύκολο τρόπο (π.χ. μέσω του διαδικτυακού του τόπου ή μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου).

2.1.9.5 Πάροχοι υπηρεσιών Διαδικτύου

Οι πάροχοι υπηρεσιών Διαδικτύου (Π.Υ.Δ.) παίζουν κεντρικό ρόλο στην διακίνηση των μηνυμάτων spam. Αν και δεν δεσμεύονται θεσμικά στη λήψη μέτρων καταπολέμησης του, έχουν εμπορικό ενδιαφέρον στην προστασία των συνδρομητών τους από τη λήψη εισερχόμενων μηνυμάτων spam, καθώς η μαζική αποστολή spam μπορεί να γίνει επιβλαβής για τις υπηρεσίες που προσφέρουν, επηρεάζοντας αρνητικά την διαθεσιμότητα και την αξιοπιστία τους. Ενδεικτικό του παραπάνω ενδιαφέροντος είναι το γεγονός ότι οι περισσότεροι Π.Υ.Δ. χρησιμοποιούν ως εμπορικό τους πλεονέκτημα την παροχή υπηρεσιών φιλτραρίσματος προς τους συνδρομητές τους. Επίσης, το εξερχόμενο spam (το spam δηλαδή που προέρχεται από συνδρομητές ενός Π.Υ.Δ.) μπορεί επίσης να μειώσει τη γενικότερη ποιότητα της υπηρεσίας και το συνολικό χρόνο απόκρισης του δικτύου, έχοντας αντίστοιχες αρνητικές επιπτώσεις και σε όλους τους υπόλοιπους συνδρομητές του. Επίσης, υπάρχει πάντα και ο κίνδυνος πλήξης της φήμης του Π.Υ.Δ. (όπως π.χ. με την καταχώρηση του σε δημόσιες μαύρες λίστες), σε περιπτώσεις όπου τα

συστήματα τους χρησιμοποιούνται από spammers ή υπολογιστές στα δίκτυα τους έχουν καταληφθεί από spammers.

Η Ε.Ε. προωθεί ιδιαίτερα τη συνεργασία με τους Π.Υ.Δ. και την υιοθέτηση σχετικών μέτρων αυτορύθμισης, όπως κώδικες δεοντολογίας και βέλτιστες πρακτικές που στοχεύουν στην λήψη από τους Π.Υ.Δ. κοινά αποδεκτών τεχνικών και οργανωτικών μέτρων για την καταπολέμηση του spam.

Η Ελληνική Αρχή Προστασίας Δεδομένων, ακολουθώντας την παραπάνω τάση, σύστησε από το 2004 ομάδα εργασίας με εκπροσώπους των κύριων ιδιωτικών και δημόσιων Ελληνικών Π.Υ.Δ., διαπίστωσε την κοινή βούληση για τον περιορισμό του spam και συζήτησε την υιοθέτηση κώδικα δεοντολογίας των παρόχων για την καταπολέμησή του. Ο κώδικας δεν υιοθετήθηκε, καθώς δεν υπήρξε συναίνεση μεταξύ των μελών της ομάδας σχετικά με την ενσωμάτωση των τεχνικών μέτρων κατά του spam.

Η Αρχή, σε συνέχεια των εργασιών της ομάδας, εξετάζει το ενδεχόμενο να εκδώσει οδηγίες και συστάσεις προς τους Π.Υ.Δ. σε τέσσερις άξονες:

- Μέτρα γενικής πολιτικής και ενημέρωσης πελατών
- Μέτρα κατά του εξερχόμενου spam
- Μέτρα κατά του εισερχόμενου spam
- Μέτρα συνεργασίας των Π.Υ.Δ.

2.1.10 Phishing[27]

Όπως το ίδιο το όνομά του υπονοεί -παραλλαγή του αγγλικού «fishing» (ψάρεμα)- το phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

[27] http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043
http://www.dart.gov.gr/NewsInner.aspx?new_id=139&nwc_id=20

Το phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam e-mail, το οποίο ισχυρίζεται -ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κ.λπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση παράνομων οικονομικών συναλλαγών.

Τα e-mail αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας και τον οδηγούν μέσω συνδέσμων σε πλαστές ιστοσελίδες, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή, που και ο ίδιος ο φυλλομετρητής «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου και σύντομου χρονικού διαστήματος, ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος. Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω phishing. Τα e-mail που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά τους.

2.1.10.1 Συμπτώματα phising

Ενδείξεις πως ένα ηλεκτρονικό μήνυμα είναι πιθανόν πλαστό:

- Ως spam μηνύματα, χρησιμοποιούν συνήθως γενικές προσφωνήσεις, όπως «Αγαπητέ πελάτη», αντί για το πραγματικό όνομα του παραλήπτη.
- Η πλειοψηφία των phising μηνυμάτων επικαλείται κάποιο δήθεν πρόβλημα ή κάποια «μοναδική ευκαιρία» και χρησιμοποιώντας φρασεολογία που δημιουργεί την αίσθηση του επείγοντος, ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα, είτε για να επωφεληθεί της ευκαιρίας.
- Συνήθως ζητούν την παραχώρηση απορρήτων προσωπικών στοιχείων οικονομικού χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, όπως το όνομα χρήστη (username) και τον κωδικό πρόσβασης (password).

2.1.10.2 Τρόποι προστασίας από το phising

Οι χρήστες πρέπει να είναι γενικά καχύποπτοι και να μην απαντάνε σε μηνύματα ηλεκτρονικού ταχυδρομείου που τους ζητούν να αποκαλύψουν αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό e-mail.

Ακόμη και σε περιπτώσεις που όλα δείχνουν ότι το μήνυμα είναι γνήσιο, είναι προτιμότερο να επικοινωνήσουν με την εταιρία που παρουσιάζεται ως αποστολέας, για να επιβεβαιώσουν ότι πράγματι αυτή τους έστειλε το μήνυμα και ότι δεν πρόκειται για περίπτωση απάτης. Φυσικά, η επικοινωνία με την εταιρεία, δεν θα πρέπει να γίνεται σύμφωνα με τις οδηγίες που περιέχει το e-mail ή απαντώντας σε αυτό.

Πριν οι χρηστές προβούν στην παραχώρηση ευαίσθητων προσωπικών πληροφοριών μέσω του Διαδικτύου θα πρέπει να προσέχουν την ηλεκτρονική διεύθυνση στην οποία βρίσκονται. Αντί για το απλό «http://», θα πρέπει να

αρχίζει με «https://». Έτσι διασφαλίζουν ότι χρησιμοποιούν ασφαλή σύνδεση web (http secure).

Γενικότερα, καλό είναι οι χρηστές να αγνοούν τα ηλεκτρονικά μηνύματα που λαμβάνουν από άγνωστες πηγές και να αποφεύγουν να συμπληρώνουν ηλεκτρονικές φόρμες που λαμβάνουν μέσω του ηλεκτρονικού ταχυδρομείου.

Τέλος, στο Διαδίκτυο κυκλοφορούν δωρεάν εφαρμογές που ενσωματώνονται ως πρόσθετες λειτουργίες στον φυλλομετρητή, ενημερώνοντας τον χρήστη για την φερεγγυότητα κάθε ιστοσελίδας, την βαθμολογία της από τους άλλους χρήστες, και την ασφάλεια των προσωπικών δεδομένων.

2.2 Διαμοιρασμός αρχείων[28]

Μία από τις βασικότερες δυνατότητες που προσφέρει το Διαδίκτυο στους χρήστες είναι η μεταξύ τους αποστολή αρχείων κάθε είδους (κείμενα, προγράμματα, φωτογραφίες, μουσική και ταινίες). Αυτή η διαδικασία ονομάζεται ανταλλαγή αρχείων (file sharing) και πραγματοποιείται μέσω διαφόρων προγραμμάτων τα οποία διατίθενται στο Διαδίκτυο είτε ελεύθερα είτε με πληρωμή. Η λήψη ενός αρχείου από το Διαδίκτυο στον υπολογιστή ονομάζεται «κατέβασμα» (downloading), ενώ η αποστολή «ανέβασμα» (uploading).

Καθένα από τα προγράμματα αυτά λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή του χρήστη, σε όλους τους χρήστες, οι οποίοι είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως, κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία, στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας, σύγχρονη επικοινωνία μεταξύ των υπολογιστών, γι αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης προγράμματα (peer-to-peer). Η ευρύτατη χρήση της δυνατότητας

[28] http://www.saferinternet.gr/

αυτής του Διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου με μηδαμινό κόστος για τον χρήστη.
Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

Από την αλόγιστη χρήση την ανταλλαγής αρχείων στο Διαδίκτυο μπορούν να προκύψουν προβλήματα όπως:
Ασφάλεια: Η χρήση των προγραμμάτων διαμοιρασμού αρχείων παραβιάζει τους κανόνες «υγιεινής» του υπολογιστή. Η ανταλλαγή αρχείων με άγνωστους χρήστες, μπορεί να δημιουργήσει πρόβλημα στην «υγεία» του υπολογιστή μολύνοντας τον από ιούς και άλλα καταστροφικά προγράμματα. Άλλα προγράμματα (π.χ. spyware) μπορούν να καταγράψουν τις δραστηριότητες στο Διαδίκτυο και να στείλουν αυτή την πληροφορία σε τρίτους ή να προκαλούν εμφάνιση διαφημιστικών μηνυμάτων ακόμη και όταν ο υπολογιστής δεν είναι συνδεμένος στο Διαδίκτυο.
Πορνογραφικό υλικό: Τα περισσότερα από τα προγράμματα διαμοιρασμού αρχείων στο Διαδίκτυο επιτρέπουν την πρόσβαση ανήλικων σε ακατάλληλα βίντεο ή εικόνες. Καθώς τα παιδιά αναζητούν την αγαπημένη τους μουσική μπορεί αθέλητα να γίνουν παραλήπτες πορνογραφικού υλικού, απλά επειδή αυτό περιέχει τις ίδιες λέξεις-κλειδιά με τις οποίες γίνεται η αναζήτηση. Πολλά από τα προγράμματα ελέγχου της πλοήγησης δεν είναι καθόλου αποτελεσματικά, όταν η διακίνηση του ακατάλληλου υλικού γίνεται μέσα από προγράμματα διαμοιρασμού.
Νομικά προβλήματα: Τα περισσότερα αρχεία που είναι διαθέσιμα μέσα από τα προγράμματα διαμοιρασμού (βίντεο, μουσική, τραγούδια, βιντεοπαιχνίδια), έχουν προστατευμένα δικαιώματα. Αυτό σημαίνει ότι ο νόμος προστατεύει το δικαίωμα του ιδιοκτήτη να επιβάλλει περιορισμούς στην αντιγραφή και την

διακίνηση του προϊόντος. Η απόκτηση και η διάθεση προϊόντων χωρίς την άδεια του ιδιοκτήτη μπορεί να προκαλέσει νομικά προβλήματα. Η ανωνυμία δεν είναι ποτέ απόλυτα δεδομένη στο Διαδίκτυο. Σε αρκετές περιπτώσεις υπήρξαν διώξεις «πειρατών», που διακινούσαν παράνομα αρχεία μουσικής.

Προσωπικά δεδομένα: Αν από λάθος ρυθμίσεις ενός προγράμματος διαμοιρασμού αρχείων, γίνει κοινόχρηστος ολόκληρος ο σκληρός δίσκος του τοπικού υπολογιστή, τότε προσωπικά δεδομένα που πιθανόν είναι αποθηκευμένα στον υπολογιστή, όπως αριθμοί πιστωτικών καρτών ή φορολογικά δεδομένα, θα εκτεθούν σε όλους τους χρήστες που χρησιμοποιούν το πρόγραμμα αυτό.

3. ΚΙΝΔΥΝΟΙ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΑΠΟ ΠΑΙΔΙΑ

Στο παρόν κεφάλαιο παρουσιάζονται και αναλύονται οι κίνδυνοι που ενδέχεται να αντιμετωπίσουν οι ανήλικοι χρήστες της σχολικής (6-12 ετών) και εφηβικής (12-18) ηλικίας, κατά την πλοήγηση τους στο Διαδίκτυο.

3.1 Παιδιά στο Διαδίκτυο[29]

Αναμφίβολα το Διαδίκτυο ασκεί μεγάλη σαγήνη σε άτομα νεαρής ηλικίας και οι λόγοι είναι κατανοητοί. Αρκεί να αναλογιστεί κανείς ότι τα παιδιά και κυρίως οι έφηβοι, απαλλαγμένοι από τις απαγορεύσεις και τους περιορισμούς που βιώνουν καθημερινά στην πραγματική τους ζωή, νιώθουν, αλλά και ουσιαστικά, είναι ελεύθεροι να επικοινωνήσουν με όποιον επιθυμούν, να δοκιμάσουν διαδικτυακές εμπειρίες που τους φαίνονται δελεαστικές, προκλητικές και ενδιαφέρουσες, να εξερευνήσουν το άγνωστο, να ενταχθούν σε ομάδες, να διευρύνουν τον κοινωνικό τους κύκλο συνομιλώντας με άτομα που ίσως να μην συναντήσουν ποτέ, να ξεχαστούν με πολύωρες μοναχικές περιηγήσεις στον κυβερνοχώρο και να νιώσουν την αδρεναλίνη τους να κορυφώνεται παίζοντας παιχνίδια, χωρίς καν να χρειάζεται να μετακινηθούν από την καρέκλα τους.

Τα παιδιά μπορούν να αντλήσουν από το Διαδίκτυο πολλά ευχάριστα και χρήσιμα πράγματα. Όμως ο αχανής αυτός ιδεατός κόσμος, ο οποίος στην ουσία δεν ελέγχεται από κανέναν, έχει και τις σκοτεινές του πλευρές. Πάμπολλα περιστατικά εξαπάτησης ή και κακοποίησης παιδιών έχουν καταγραφεί παγκοσμίως, από επιτήδειους οι οποίοι χρησιμοποιούν την ανωνυμία του Διαδικτύου προκειμένου να επιτύχουν τους στόχους τους. Ένας ενήλικας είναι σε θέση να κρίνει και να αποφύγει τους κινδύνους που θα συναντήσει κατά την πλοήγησή του στο Διαδίκτυο, για ένα παιδί όμως, τα πράγματα είναι τελείως διαφορετικά. Η προστασία των παιδιών όμως δεν είναι κάτι απλό. Το επιθυμητό δεν είναι ούτε η πλήρης απαγόρευση της πρόσβασης στο Διαδίκτυο, που στερεί

[29] Καλμαντή Μ., Μαρκάκη Ε.Α. (2010), «Ο εθισμός στο Διαδίκτυο», περιοδικό «Γιατρεύω», τεύχος 15, σελ. 14-21

το παιδί από ένα ανεκτίμητο εργαλείο, αλλά ούτε και η απουσία οποιασδήποτε επίβλεψης.

3.1.1 Έλληνες χρήστες 9-16 ετών[30]

Με καθυστέρηση 3-4 χρόνων σε σχέση με τους συνομηλίκους τους σε άλλες χώρες της Ευρωπαϊκής Ένωσης μπαίνουν τα ελληνόπουλα στον κόσμο του Διαδικτύου, ωστόσο εμφανίζονται πιο «ώριμα» σε ότι αφορά την ασφαλή πλοήγηση. Αυτό δείχνουν τα αποτελέσματα της πρόσφατης έρευνας «EU Kids Online II», η οποία ξεκίνησε και ολοκληρώθηκε στο τέλος του καλοκαιριού του 2010 σε 25 χώρες της Ευρώπης, σε δείγμα 23.000 παιδιών ηλικίας 9 έως 16 ετών.

Οι υπεύθυνοι της έρευνας μάλιστα σημειώνουν, πως σημαντικό ρόλο στην ψηφιακή ωριμότητα των παιδιών, παίζει ως ένα βαθμό η πιο εντατική χρήση του Διαδικτύου, καθώς μπορεί μεν να αυξάνει τις πιθανότητες έκθεσης σε κάποιον κίνδυνο, αλλά παράλληλα τα «θωρακίζει» ώστε να τον αντιμετωπίσουν. «Η αυξανόμενη χρήση του Διαδικτύου βελτιώνει τον ψηφιακό αλφαβητισμό των παιδιών και τις ικανότητες ασφαλούς πλοήγησης», αναφέρεται χαρακτηριστικά στην έρευνα.

Στη Σουηδία και τις υπόλοιπες βόρειες χώρες η πρώτη επαφή με το Διαδίκτυο γίνεται στις ηλικίες των 7-8 χρόνων, ενώ στην Ελλάδα στην ηλικία των έντεκα ετών, που είναι και ο μεγαλύτερος μέσος όρος στην Ευρώπη. Ειδικότερα, όσον αφορά τη συχνότητα χρήσης, το 1/3 των παιδιών ηλικίας 9-10 ετών χρησιμοποιεί το Διαδίκτυο καθημερινά, ενώ στα μεγαλύτερα παιδιά το αντίστοιχο ποσοστό φτάνει το 77%.

Ο πλέον δημοφιλής χώρος πρόσβασης είναι το σπίτι και ακολουθεί το σχολείο. Ωστόσο, στην Ελλάδα διαπιστώνεται ότι το 11% των παιδιών είναι τόσο εξοικειωμένα με την τεχνολογία ώστε να πλοηγούνται με συσκευή παλάμης και

[30] Κώστας Ντελέζος, 28 Οκτωβρίου 2010, Τα Νέα online
http://www.tanea.gr/default.asp?pid=2&ct=1&artid=4601360

το 68% με κινητό τηλέφωνο, όταν ο ευρωπαϊκός μέσος όρος δεν ξεπερνά το 31%.

Η Ελλάδα, όπως αναφέρεται στην έρευνα, θεωρείται χώρα «χαμηλού διαδικτυακού κινδύνου» για τα παιδιά, καθώς από τις απαντήσεις των ανηλίκων ηλικίας 9 έως 16 ετών προκύπτει, ότι μόνο το 1/3 των παιδιών αισθάνθηκε κάποια στιγμή να απειλείται κατά την πλοήγηση στο Διαδίκτυο. Αντίθετα, σε χώρες όπως η Λιθουανία, η Εσθονία, η Τσεχία και η Σουηδία, αντίστοιχες απαντήσεις περί απειλών έδωσαν τα 2/3 των παιδιών.

Σημαντικό ρόλο στα θέματα της προστασίας από τους διαδικτυακούς κινδύνους, φαίνεται ότι παίζουν και οι Έλληνες γονείς. «Ο γονικός έλεγχος στην Ελλάδα είναι αποτελεσματικός, ανεξαρτήτως του επιπέδου εκπαίδευσης των γονέων, ενώ η περιορισμένη έκθεση των μικρών παιδιών σε σεξουαλικό περιεχόμενο, είναι συναφής με την αποτελεσματικότητα του ελέγχου», τονίζει η λέκτορας του τμήματος Επικοινωνίας και Μέσων Μαζικής Ενημέρωσης του Πανεπιστημίου Αθηνών, κ. Λίζα Τσαλίκη. Η ίδια, ως υπεύθυνη της Ελληνικής ομάδας της έρευνας «EU Kids Online II», προσθέτει ότι «τα μικρά παιδιά δεν ενδιαφέρονται να δουν πορνογραφικό υλικό, ειδικά όπως αυτό ορίζεται από τους ενήλικες».

Πάντως, οι Έλληνες γονείς εξακολουθούν να μην έχουν επαρκή εικόνα για τους κινδύνους που αντιμετώπισαν τα παιδιά τους, κατά την πλοήγηση τους στο Διαδίκτυο. Σχεδόν το 83% των γονέων, των οποίων τα παιδιά ανέφεραν ότι είχαν εκτεθεί σε κίνδυνο, δεν είχαν επίγνωση του γεγονότος. Σύμφωνα με την έρευνα, στην υπόλοιπη Ευρώπη το 52% των γονέων δεν γνώριζε ότι το παιδί του είχε λάβει μηνύματα σεξουαλικού περιεχομένου, ενώ το 61% των γονέων αγνοούσε ότι το παιδί του συνάντησε από κοντά πρόσωπο που γνώρισε μέσω του Διαδικτύου.

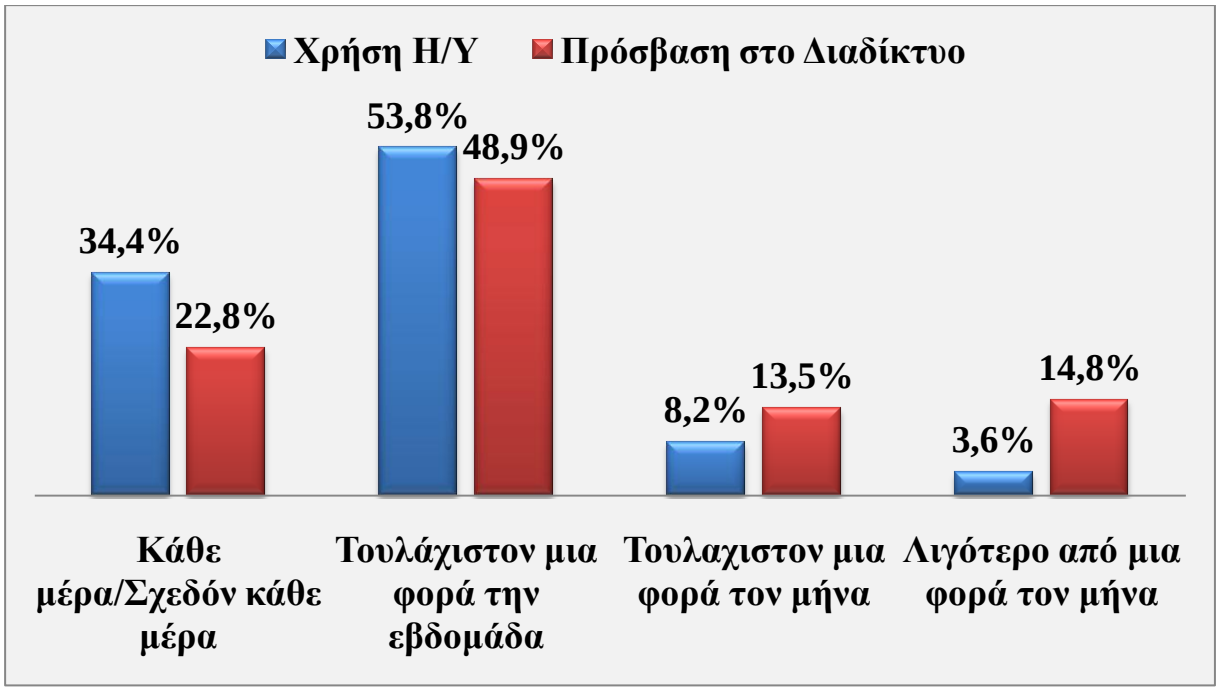
Όσον αφορά τα υπόλοιπα στοιχεία της έρευνας, το 63% των παιδιών στην Ελλάδα απάντησε ότι «υπάρχουν πολλά καλά πράγματα στο Διαδίκτυο», ενώ το 2% παραδέχτηκε ότι έχει ανταλλάξει μηνύματα ή εικόνες σεξουαλικού

περιεχομένου. Ακόμα, η Ελλάδα μαζί με την Πορτογαλία, την Ιταλία και την Τουρκία, εμφανίζει τα χαμηλότερα ποσοστά (3%) και στα κρούσματα εξύβρισης-εκβιασμών (bullying) μέσω Διαδικτύου.

Το 2008 πραγματοποιήθηκε η «Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας από τα νοικοκυριά, έτους 2008» από τη Γενική Γραμματεία της Εθνικής Στατιστικής Υπηρεσίας της Ελλάδος. Η έρευνα διενεργήθηκε σε τελικό δείγμα 5.045 ιδιωτικών νοικοκυριών και σε ισάριθμα μέλη αυτών, σε ολόκληρη την Ελλάδα, με κριτήριο την ύπαρξη ενός, τουλάχιστον, μέλους ηλικίας 16-74 ετών σε κάθε νοικοκυριό και περίοδο αναφοράς το πρώτο τρίμηνο του 2008. Επιπλέον, ερευνήθηκαν 289 παιδιά ηλικίας 12-15 ετών.

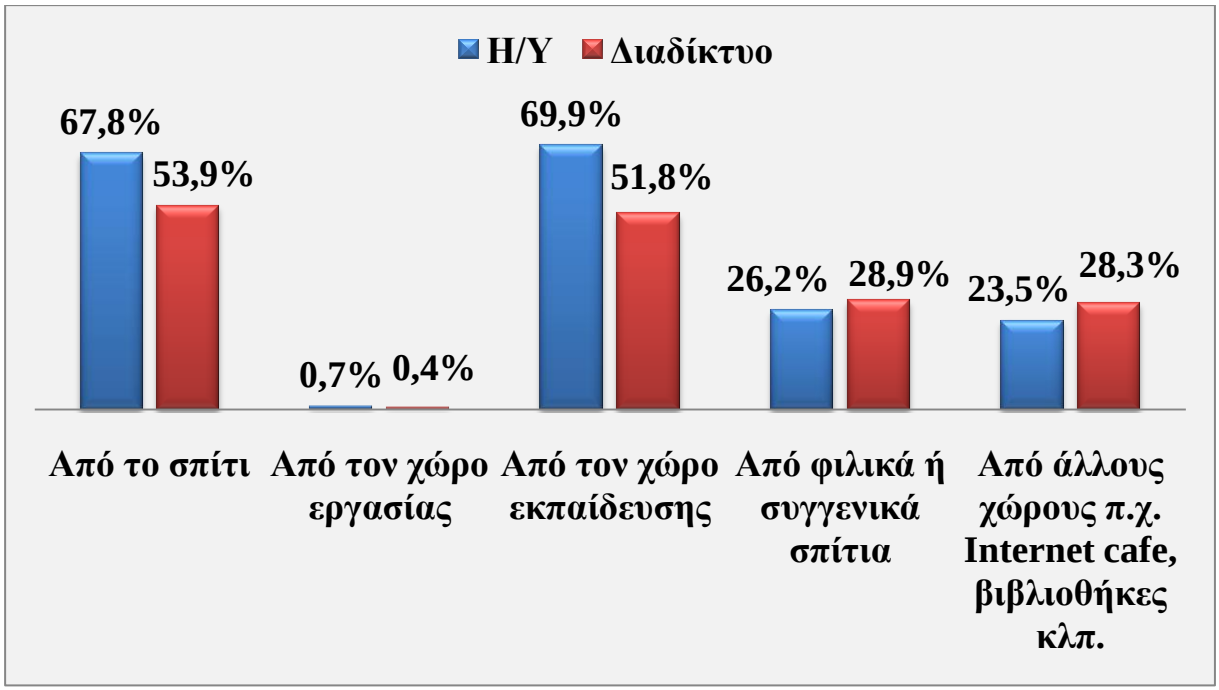
Τα αποτελέσματα σχετικά με την χρήση του Η/Υ και του Διαδικτύου, το πρώτο τρίμηνο του 2008, έδειξαν ότι:

- Το ποσοστό των παιδιών ηλικίας 12 – 15 ετών που είχαν πρόσβαση στο Διαδίκτυο ανέρχεται στο 84,9% και το ποσοστό των παιδιών της ίδιας ηλικίας που έκαναν οποτεδήποτε χρήση του Διαδικτύου στο 88,1%.
- Το ποσοστό των παιδιών που έκαναν τακτική χρήση (κάθε ημέρα ή τουλάχιστον μία φορά την εβδομάδα) του Η/Υ, ανέρχεται στο 88,2% και το αντίστοιχο ποσοστό των παιδιών που χρησιμοποίησαν το Διαδίκτυο, ανέρχεται στο 71,7%.
- Το ποσοστό των παιδιών που χρησιμοποίησαν τον Η/Υ ή το Διαδίκτυο, έκανε χρήση τουλάχιστον μία φορά την εβδομάδα (αλλά όχι κάθε ημέρα), ανέρχεται σε 53,8% και 48,9% αντίστοιχα.



Σχήμα 11 – Συχνότητα χρήσης Η/Υ και Διαδικτύου

Από τα αποτελέσματα της έρευνας, προκύπτει ότι η πλειοψηφία των παιδιών που κατά το πρώτο τρίμηνο του 2008 χρησιμοποίησαν ηλεκτρονικό υπολογιστή ή το Διαδίκτυο, έκανε χρήση από το χώρο εκπαίδευσης και κατοικίας. Αν και πρόκειται για παιδιά μικρής ηλικίας, τα ποσοστά πρόσβασης από άλλους χώρους, δηλαδή Internet café, δημόσιες βιβλιοθήκες, κ.λπ., είναι υψηλά και ανέρχονται στο 23,5% για χρήση Η/Υ και στο 28,3% για πρόσβαση στο Διαδίκτυο. Σημειώνεται ότι τα Internet café αποτελούν το 97,3% των άλλων χώρων. Όσον αφορά στο φύλο των παιδιών που επισκέπτονται τα Internet café, το 68,3% είναι αγόρια και το 31,7% κορίτσια.



Σχήμα 12 – Χώροι πρόσβασης Η/Υ και Διαδικτύου

Σύμφωνα με τα αποτελέσματα της έρευνας, το 29,3% των παιδιών χρησιμοποιεί το Διαδίκτυο για επικοινωνία με την αποστολή γραπτών μηνυμάτων σε πραγματικό χρόνο (instant messaging). Τα ποσοστά χρήσης της συγκεκριμένης εφαρμογής, κατά ηλικιακή ομάδα, είναι:

- 12 ετών 14,5%
- 13 ετών 21,7%
- 14 ετών 38,0%
- 15 ετών 39,7%

Αξιοσημείωτο είναι ότι το 58,8% των παιδιών που κάνουν χρήση του Διαδικτύου, δε χρησιμοποιεί καμία από τις προηγμένες υπηρεσίες που σχετίζονται με επικοινωνία. Στην πλειοψηφία τους (48,7%) τα παιδιά χρησιμοποιούν για ψυχαγωγία το «κατέβασμα» ή την ακρόαση μουσικής. Τα ποσοστά χρήσης της συγκεκριμένης εφαρμογής, κατά ηλικιακή ομάδα, είναι:

- 12 ετών 40,0%
- 13 ετών 48,3%
- 14 ετών 55,1%
- 15 ετών 50,0%

Το 36,5% των παιδιών που κάνουν χρήση του Διαδικτύου δε χρησιμοποιεί καμία από τις προηγμένες υπηρεσίες που σχετίζονται με ψυχαγωγία.

3.1.2 Θέματα ηθικής[31]

Την απουσία «ηθικών φραγμών» στους νέους την ώρα που πλοηγούνται στο Διαδίκτυο κατέδειξε έρευνα του πανεπιστημίου Χάρβαρντ που μελέτησε τις ηθικές ευαισθησίες της «ψηφιακής γενιάς». Οι νέοι, την ώρα που βρίσκονται στο Διαδίκτυο, υποδύονται έναν διαφορετικό ρόλο από αυτόν που έχουν όταν δρουν στον πραγματικό κόσμο. Ο «ψηφιακός εαυτός» τους είναι πιο ανάλγητος, πιο σκληρός και πιο «ανήθικος».

Η έρευνα GoodPlay Project παρουσιάστηκε στο συνέδριο Social Good Summit της ιστοσελίδας Mashable. Παρουσιάζοντας τα βασικότερα ευρήματα, η Κάρι Τζέιμς, διευθύντρια Έρευνας του Χάρβαρντ, αναφέρθηκε στην ανάγκη καθοδήγησης των νέων για την ορθή χρήση των κοινωνικών δικτύων. Η μελέτη ερεύνησε την «ταυτότητα» της «δικτυωμένης» νεολαίας και την συμπεριφορά που αυτή επιδεικνύει απέναντι σε θέματα όπως η ιδιωτική ζωή, η ιδιοκτησία, η εξουσία, η αξιοπιστία και η συμμετοχή.

Η ερευνητική ομάδα του Χάρβαρντ διαπίστωσε ότι οι περισσότεροι νέοι στερούνται ηθικής σκέψης και σεβασμού για τον υπόλοιπο κόσμο όταν

[31] http://www.madata.gr/diafora/science/76851.html

χρησιμοποιούν το Διαδίκτυο, ενώ οι ηθικές τους αναστολές αμβλύνονται ή εξαφανίζονται.

«Κάνω online οτιδήποτε θέλω να κάνω. Δε νομίζω ότι είναι δουλειά κανενός να μου λέει τι δεν πρέπει να κάνω. Δε νιώθω υπεύθυνος απέναντι σε άλλους ανθρώπους όταν είμαι online. Περισσότερο νοιάζομαι για μένα, παρά για οποιονδήποτε άλλο».

Στην απάντηση αυτή, που έδωσαν αρκετοί ερωτώμενοι, συνοψίζεται ο τρόπος με τον οποίο σκέφτονται οι νέοι όταν πλοηγούνται στο Διαδίκτυο και το μέγεθος της ευθύνης που αντιλαμβάνονται ότι τους αναλογεί. Οι νέοι που συμμετείχαν στην έρευνα, δεν θεωρούν ανήθικο το «κατέβασμα» μουσικής από το Διαδίκτυο, ενώ φαίνεται ότι δεν τους απασχολεί ιδιαίτερα το θέμα των πνευματικών δικαιωμάτων και της αμοιβής των δημιουργών.

Ακόμα, η αντίδραση των περισσότερων όταν βλέπουν στο Διαδίκτυο κάτι περίεργο είναι να βάζουν τα γέλια. Ακόμη κι αν είναι κάτι που στον έξω κόσμο θα τους ενοχλούσε, στο Διαδίκτυο το προσπερνούν, θεωρώντας ότι δεν μπορούν να το αλλάξουν.

Η έρευνα προσδίδει ιδιαίτερη σημασία στο ρόλο των κοινωνικών δικτύων στη σημερινή εποχή και για το λόγο αυτό, συμπεραίνει ότι είναι σημαντικό να βελτιωθεί η διαδικτυακή συμπεριφορά των νέων.

3.2 Εθισμός[32]

Το να διατηρηθεί μια υγιή ισορροπία ανάμεσα στα μέσα ψυχαγωγίας και στις άλλες δραστηριότητες στη ζωή των παιδιών, αποτελούσε πάντα μια πρόκληση. Το Διαδίκτυο έκανε αυτή την πρόκληση ακόμα πιο έντονη. Η δεσμευτική φύση των διαδικτυακών επικοινωνιών και των διαδραστικών παιχνιδιών οδηγεί πολλά

[32] Καλμαντή Μ., Μαρκάκη Ε.Α. (2010), «Ο εθισμός στο Διαδίκτυο», περιοδικό «Γιατρεύω», τεύχος 15, σελ. 14-21
Παναγιώτης Αθανάσαινας (21/01/2008), *Εθισμός στο Διαδίκτυο, μια νέα μορφή εξάρτησης*
http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_21_21/01/2008_219134
http://www.saferinternet.gr/index.php?objId=Category35&parentobjId=Page2
http://el.wikipedia.org/wiki/Εθισμός_των_νέων_στο_διαδίκτυο

παιδιά και εφήβους στο σημείο να μην αντιλαμβάνονται την ώρα που περνάνε στο Διαδίκτυο.

Ο εθισμός στο Διαδίκτυο είναι μια σχετικά νέα μορφή εξάρτησης, η οποία βρίσκεται υπό εξέταση από την επιστημονική κοινότητα προκειμένου να οριοθετηθεί, αφού η εξάρτηση από το Διαδίκτυο δεν είναι ακόμη μια κλινική οντότητα που συναντάμε σε ψυχιατρικά εγχειρίδια. Αυτή η μορφή εθισμού ορίζεται ως η «ενασχόληση με το Διαδίκτυο για άντληση αισθήματος ικανοποίησης που συνοδεύεται με αύξηση του χρόνου που καταναλώνεται για την άντληση αυτού του αισθήματος».

Το ψηφιακό χάσμα χωρίζει τους αναλφάβητους τεχνολογικά γονείς και καθηγητές, από τα ημιμαθή στις περισσότερες περιπτώσεις παιδιά, τα οποία βρίσκονται εκτεθειμένα στο νέο τεχνολογικό περιβάλλον. Δυστυχώς κάποιες φορές, γονείς και καθηγητές δεν καταλαβαίνουν το πρόβλημα πριν αυτό γίνει σοβαρό. Αυτό συμβαίνει, γιατί ότι γίνεται στο Διαδίκτυο, είναι εύκολο να κρυφτεί και γιατί ο εθισμός στο Διαδίκτυο δεν είναι ευρέως αναγνωρισμένος από την ιατρική κοινότητα. Οι ψυχίατροι συνεχίζουν να διαφωνούν για το αν αυτή η συμπεριφορά μπορεί να χαρακτηριστεί «εθισμός», με μερικούς να προτιμούν να την αποκαλούν «καταναγκαστική συμπεριφορά».

Οι ψυχίατροι παρατηρούν ότι ο εθισμένος χρήστης εμφανίζει συμπτώματα απόσυρσης από την υπόλοιπη ζωή του και «συρρίκνωση της πραγματικότητας του» στο τετράγωνο της οθόνης, καταναγκαστική συμπεριφορά και απώλεια ελέγχου των αρνητικών επιπτώσεων. Περιγράφουν την νέα αυτή διαταραχή ως βιο-ψυχο-κοινωνική και την παρομοιάζουν με διαταραχές όπως η βουλιμία, ο αλκοολισμός και ο τζόγος.

Το φαινόμενο μπορεί να εμφανιστεί σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι πιο συχνό κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και κατά την όψιμη εφηβεία (> 17 ετών). Όσο ο έφηβος μεγαλώνει και πλησιάζει την μέση εφηβεία, ο πειραματισμός και η περιέργεια, η

μη συνειδητοποίηση του κινδύνου και η φυσιολογική αντίδραση σε κάθε καταπίεση, γίνονται βασικά χαρακτηριστικά του και τον καθιστούν ευάλωτο και ευαίσθητο σε εξαρτήσεις. Τα παραπάνω δεν είναι απόλυτα, αφού η χρονολογική ηλικία μπορεί να μην συμβαδίζει πάντα με το αναπτυξιακό ψυχοκοινωνικό και γνωστικό στάδιο.

Στην Νότια Κορέα η οποία αποτελεί αντικείμενο μελέτης ως προς το πρόβλημα της εξάρτησης, υπολογίζεται ότι το 30% των εφήβων αντιμετωπίζει προβλήματα εθισμού, το οποίο θεωρείται ένα από τα πιο σοβαρά ζητήματα της δημόσιας υγείας τους.

3.2.1 Συμπτώματα και αιτίες[33]

Πριν ο έφηβος φθάσει στον εθισμό υπάρχουν πρόδρομα συμπτώματα της εξάρτησης από το Διαδίκτυο και συμπεριφορές, τα οποία θα πρέπει οι γονείς να προσέξουν και να μην υποτιμήσουν.

- Υπερβολικός χρόνος ενασχόλησης με τον ηλεκτρονικό υπολογιστή
- Αίσθηση κενού και κατάθλιψης μακριά από τον υπολογιστή
- Αίσθηση ευεξίας ή εφορίας μπροστά στον υπολογιστή
- Αδυναμία διακοπής της δραστηριότητας
- Παραμέληση των υποχρεώσεων και άλλων ασχολιών
- Απότομη πτώση της σχολικής επίδοσης
- Μείωση του χρόνου δραστηριοτήτων και του χρόνου που περνά με οικογένεια και φίλους,
- Μεταβολή της συμπεριφοράς (ευερεθιστότητα και επιθετικότητα)
- Αδιαφορία για πράγματα που τον/την ευχαριστούσαν.

[33] Καλμαντή Μ., Μαρκάκη Ε.Α. (2010), «Ο εθισμός στο Διαδίκτυο», περιοδικό «Γιατρεύω», τεύχος 15, σελ. 14-21
Παναγιώτης Αθανάσαινας (21/01/2008), *Εθισμός στο Διαδίκτυο, μια νέα μορφή εξάρτησης*
http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_21_21/01/2008_219134

Επιπλέον υπάρχουν και σωματικά συμπτώματα όπως:

- ημικρανίες
- πονοκέφαλοι
- ξηρότητα οφθαλμών
- εξασθένηση και θόλωση όρασης
- δυσκολία εστίασης σε μακρινές αποστάσεις
- φωτοεπιληψία
- πόνοι στην πλάτη
- ακατάστατη διατροφή και παράλειψη γευμάτων
- διαταραχές του ύπνου και αλλαγή των συνηθειών του ύπνου
- μυοσκελετικές παθήσεις
- μειωμένη αθλητική δραστηριότητα
- παραμέληση προσωπικής υγιεινής

Το Διαδίκτυο έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του, είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητας του χωρίς να έχει περιορισμούς και συνέπειες. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων. Ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει, πολλές φορές, οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου.

Ο εθισμός στο Διαδίκτυο μπορεί να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, τα οποία πιθανώς συμβάλουν στην ανάπτυξη του προβλήματος, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας και κοινωνική φοβία. Παράλληλα, οικογενειακοί παράγοντες όπως, η έλλειψη

επικοινωνίας μεταξύ των μελών της οικογένειας, η απουσία επίβλεψης από τους γονείς λόγω εργασίας εκτός σπιτιού για πολλές ώρες, οι επιπτώσεις ενός διαζυγίου και γενικώς μια δυσλειτουργική οικογένεια, καθώς επίσης και η έλλειψη ενδιαφερόντων, φαίνεται να παίζουν ρόλο στην ανάπτυξη του φαινομένου, το οποίο έχει παρατηρηθεί ότι παρουσιάζεται συχνότερα στα αγόρια.

Υπολογίζεται ότι διεθνώς ένα ποσοστό της τάξης του 5 έως 10% εμφανίζει συμπτώματα εξάρτησης, σε βαθμό που να μην μπορεί να ανταπεξέλθει στις καθημερινές του υποχρεώσεις.

3.2.1.1 Πειραματικά δεδομένα για τον εθισμό στο Διαδίκτυο[34]

Ένα ιδιότυπο πείραμα διεξήχθη στις ΗΠΑ που επιβεβαιώνει τους φόβους για τις τάσεις εθισμού των εφήβων για τα ηλεκτρονικά μέσα και το Διαδίκτυο. Το πείραμα ήταν απλό. Οι μαθητές της πρώτης Λυκείου στο Shannon Meyers στην πολιτεία της California έπρεπε για μια βδομάδα να απαρνηθούν την ενασχόλησή τους με τα ηλεκτρονικά μέσα και το Διαδίκτυο. Μόνη υποχρέωση τους να κρατούν ένα ημερολόγιο με τα συναισθήματά τους σε καθημερινή βάση.

Τα αποτελέσματα ήταν αναμενόμενα όσο και απογοητευτικά. 9 στα 22 παιδιά σήκωσαν το χέρι τους σε ερώτηση του καθηγητή τους μετά τη λήξη του πειράματος για το αν έστω και μια φορά παρέβησαν τη συμφωνία.

Ακόμη πιο ανησυχητικά είναι τα σχόλια των μαθητών που συγκεντρώθηκαν από την ημερήσια καταγραφή των συναισθημάτων τους. Τα περισσότερα παιδιά εμφάνισαν συμπτώματα στερητικού συνδρόμου όμοιου εκείνων που θα «απείχαν» από το ποτό, το τσιγάρο, ή ακόμη και τα ναρκωτικά.

Χαρακτηριστικά σχόλια από τα ημερολόγια των παιδιών είναι τα παρακάτω: «Οι πρώτες ημέρες ήταν σκέτη κόλαση, ξυπνούσα μέσα στην νύχτα ιδρωμένη και στην έλλειψη του τηλεφώνου μου χτύπαγα το κεφάλι μου στον τοίχο» περιέγραφε μια μαθήτρια, ενώ ένας συμμαθητής της: «Ήμουν σαν χαμένος στην

[34] http://www.internetandkids.com/2009/05/blog-post.html

έρημο χωρίς στάλα νερού, ήταν ότι πιο απαίσιο έχω ζήσει έως τώρα, ένοιωθα σαν να πέθαινα, η ζωή ήταν κόλαση».

Χαρακτηριστική όμως είναι και η ανακάλυψη μεγάλης μερίδας μαθητών: «Ανακάλυψα πως έχω αδέλφια και ξεκίνησα να τους μιλάω» για άλλους τα πράγματα ήταν λιγότερο επώδυνα: «Απλώς έκανα υπομονή να περάσουν οι ημέρες και καθάριζα καθημερινά το δωμάτιο μου» σημείωσαν μερικοί.

3.2.2 Εθισμός σε Έλληνες έφηβους[35]

Το πρόβλημα του εθισμού στο Διαδίκτυο εμφανίζεται και στην Ελλάδα. Βάσει έρευνας που πραγματοποιήθηκε από την Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) του Πανεπιστημίου Αθηνών σε δείγμα 897 εφήβων Αττικής 15-16 ετών (430 αγόρια και 467 κορίτσια) τα αποτελέσματα έδειξαν ότι:

- 53,4% χρησιμοποιούσαν το Διαδίκτυο για χρονικό διάστημα μεγαλύτερο του ενός έτους.
- 26% ανέφεραν ότι έκαναν καθημερινή χρήση του Διαδικτύου.
- 8% έκαναν χρήση περισσότερο από 20 ώρες την εβδομάδα.
- Τα αγόρια χρησιμοποιούσαν το Διαδίκτυο σημαντικά περισσότερο από τα κορίτσια.
- το 1% είχαν εθιστεί από το Διαδίκτυο.
- 12,8% παρουσίαζαν περιοδικά ή συχνά προβλήματα σχετικά με την κατάχρηση Διαδικτύου (κατάσταση πριν το εθισμό).
- Υπήρξε θετική συσχέτιση της χρήσης Διαδικτύου και της διάσπασης προσοχής-υπερκινητικότητας.
- Τέλος παρατηρήθηκε ότι ο πιο συχνός λόγος χρήσης (55,2%), ήταν τα διάφορα παιχνίδια.

Σε ανάλογη μελέτη της ψυχιατρικής κλινικής του πανεπιστημιακού νοσοκομείου Λάρισας, σε δείγμα 2200 εφήβων 12-18 ετών που αφορούσε

[35] http://www.youth-health.gr/gr/index.php?I=5&J=2&K=7
Χρυσοστομίδου Β. (11 Μαΐου 2008), «Παιδιά στο ίντερνετ», περιοδικό «Κ», τεύχος 258, σελ.29-32
Καλμαντή Μ., Μαρκάκη Ε.Α. (2010), «Ο εθισμός στο Διαδίκτυο», περιοδικό «Γιατρεύω», τεύχος 15, σελ. 14-21

συνολικά το 10% των μαθητών της Θεσσαλίας από 85 διαφορετικά σχολεία, το 70,8% των εφήβων είχε πρόσβαση στο Διαδίκτυο, αλλά εντυπωσιακά σε σύγκριση με τους εφήβους της Αττικής, διαπιστώθηκε εθισμός σε ποσοστό 8,2% ενώ και το 26,3% παρουσίαζε «προβληματική χρήση», με συχνότερη χρήση 50,9% τα online βιντεοπαιχνίδια ,με τα αγόρια να είναι τριπλάσια από τα κορίτσια.

Πιθανόν τα παιδιά της επαρχίας να εθίζονται περισσότερο στο Διαδίκτυο καθώς δεν υπάρχουν τόσες επιλογές ενασχόλησης με άλλες δραστηριότητες στον τόπο διαμονής τους. Τα διεθνή δεδομένα του εθισμού στο Διαδίκτυο ποικίλουν ανάλογα με την ταχύτητα που ενσωματώθηκαν οι Η/Υ στην καθημερινότητα κάθε κοινωνίας και εάν αυτή η διαδικασία αφορούσε προσωπικά τον κάθε χρήστη ή γινόταν στα πλαίσια μιας εκπαιδευτικής διαδικασίας στο σχολείο όπως π.χ. συνέβη σταδιακά στην Νορβηγία, η οποία παρουσιάζει από τα μικρότερα ποσοστά ηλεκτρονικού εθισμού διεθνώς (1,98%). Σε αντίθεση με την Ταϊβάν στην οποία η ταχύτατη εισβολή των Η/Υ σε ανώριμους και όχι μορφωμένους χρήστες δικαιολογεί τα καταγραμμένα από τα υψηλότερα ποσοστά εθισμού (7,5%).

Πανελλαδικά αλλά και διεθνώς, τα επικρατέστερα εξαρτησιογόνα είναι τα ηλεκτρονικά παιχνίδια «ρόλων» και τα chat rooms. Παρατηρούνται κυρίως στα αγόρια, σε μονογονεϊκές και δυσλειτουργικές οικογένειες, με απουσία επίβλεψης από τους γονείς.

Στην μονάδα εφηβικής υγείας του νοσοκομείου «Παίδων Αγλαΐα Κυριακού» τα τελευταία χρόνια έχουν απευθυνθεί 47 έφηβοι με σοβαρό εθισμό στο Διαδίκτυο από τους οποίους το 94,3% ήταν αγόρια. «Υπάρχουν και παιδιά, τα οποία, μας αναζήτησαν με δική τους πρωτοβουλία όταν, έχοντας εγκαταλείψει το σχολείο, ήρθαν σε απόγνωση λόγο απουσιών και χρειάστηκαν οπωσδήποτε χαρτί από δημόσιο φορέα που να πιστοποιεί την διαταραχή τους», δηλώνει η επιστημονική υπεύθυνη της Μονάδας Εφηβικής Υγείας, κ. Α. Τσίτσικα.

Σύμφωνα με τον κ. Καφετζή, διευθυντή της Μονάδας Εφηβικής Υγείας Β' παιδιατρικής κλινική του πανεπιστημίου Αθηνών, «τον αρχικό ενθουσιασμό διαδέχεται η απληστία», δηλαδή για να εισπράξει το ίδιο αίσθημα ικανοποίησης, το παιδί χρειάζεται να περάσει όλο και περισσότερο χρόνο στο Διαδίκτυο.

Στη συμβουλευτική τηλεφωνική γραμμή της ΕΨΥΠΕ (Εταιρεία Ψυχοκοινωνικής Υγείας Παιδιού και Εφήβου), οι ψυχολόγοι λένε ότι δέχονται όλο και περισσότερα τηλεφωνήματα από γονείς που τους ρωτάνε για το τι πρέπει να πράξουν. Περίπου το 15% των γονέων κάνει αναφορά σε δυσκολία να χειριστεί το γεγονός ότι το παιδί τους ασχολείται συνεχώς με τον υπολογιστή, παίζει ηλεκτρονικά παιχνίδια, ή πλοηγείται συνεχώς στο Διαδίκτυο.

3.2.3 Αντιμετώπιση του εθισμού[36]

Το σημαντικότερο πράγμα που θα χρειαστεί να πράξουν οι γονείς προκειμένου να μπορέσουν να ελέγξουν αποτελεσματικά τη χρήση του Διαδικτύου από τα παιδιά τους, είναι να γνωρίσουν οι ίδιοι το μέσο. Σε αρκετές περιπτώσεις οι γονείς δε γνωρίζουν το μέσο επαρκώς και επιπλέον δε φαίνονται διατεθειμένοι να έλθουν σε επαφή με το Διαδίκτυο, ενώ ταυτόχρονα δεν ενδιαφέρονται για τις δραστηριότητες των παιδιών τους στο Διαδίκτυο.

3.2.3.1 Συμβουλές προς τους γονείς[37]

- Από μικρή ηλικία θα πρέπει να τίθενται και να τηρούνται όρια μέσα στην οικογένεια. Τα όρια δεν θα πρέπει να είναι υπερβολικά και ιδιαίτερα αυστηρά, ώστε να μην καταπιέζουν τα παιδιά, αλλά να τα κατευθύνουν και να σημαίνουν ενδιαφέρον για την προστασία και την ασφάλεια τους. Όσο ένα παιδί μεγαλώνει, τα όρια που θα ισχύουν είναι καλό να συζητιούνται, ώστε να λαμβάνεται υπόψη η γνώμη του ίδιου

[36] Παναγιώτης Αθανάσαινας (21/01/2008), *Εθισμός στο Διαδίκτυο, μια νέα μορφή εξάρτησης:* http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_21_21/01/2008_219134

[37] Άρτεμις Κ. Τσίτσικα, *Χρήση – Κατάχρηση Διαδικτύου*: http://www.youth-health.gr/gr/index.php?I=6&J=2&K=42

του παιδιού. Ο σεβασμός της προσωπικότητας των παιδιών από μικρή ηλικία, είναι στοιχείο πολύ σημαντικό για την εφαρμογή πειθαρχίας.

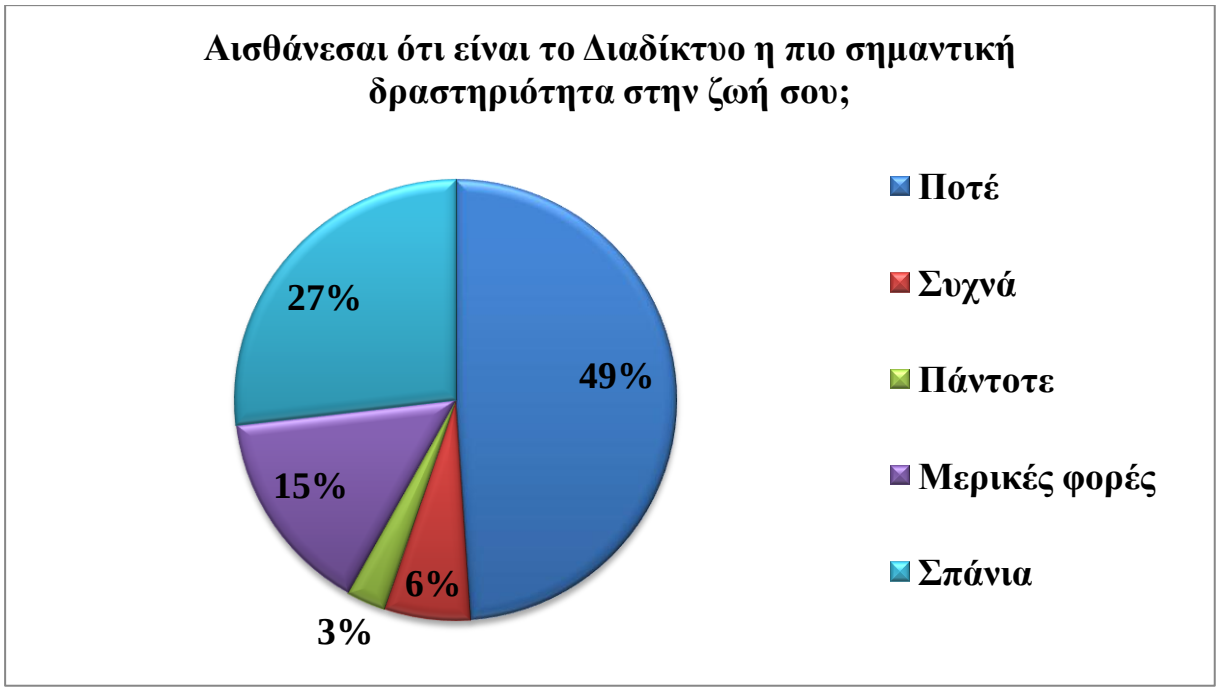
- Οι γονείς χρειάζεται να αφιερώνουν χρόνο και διάθεση ώστε να ασχοληθούν με θέματα Διαδικτύου μαζί με τα παιδιά τους.
- Καλό είναι, ο υπολογιστής να βρίσκεται σε κοινόχρηστο χώρο, ώστε να μη δίνεται η δυνατότητα απομόνωσης του παιδιού και να υπάρχει επίβλεψη από τους γονείς.
- Χρήση φίλτρων για επιβλαβείς ιστοσελίδες και συμμετοχή στις επιλογές του εφήβου (χωρίς υπερβολές και παράλογες απαγορεύσεις) συμβάλλουν σε ένα θετικό αποτέλεσμα.
- Ενημέρωση των παιδιών με απλά λόγια από μικρή ηλικία για τα φαινόμενα του εθισμού.
- Θα πρέπει να αποφεύγεται η χρήση του υπολογιστή για επιβράβευση ή τιμωρία.
- Εάν οι γονείς παρατηρήσουν υπερβολική χρήση και συμπεριφορές εθισμού, θα πρέπει να αναζητήσουν αμέσως βοήθεια.

Η ποιοτική σχέση με τους γονείς, ο χρόνος που οι γονείς αφιερώνουν στα παιδιά και η ενασχόληση τους στο Διαδίκτυο μαζί με τα παιδιά, μπορούν να συμβάλλουν στην αποφυγή του φαινομένου. Η συναισθηματική κάλυψη των παιδιών, η καλή σχέση και η επικοινωνία όλων των μελών, οδηγούν σε σωστή εφαρμογή ορίων μέσα στο σπίτι, τα οποία μπορούν να τηρούνται (οι ενοχικοί γονείς αδυνατούν να βάλουν όρια).

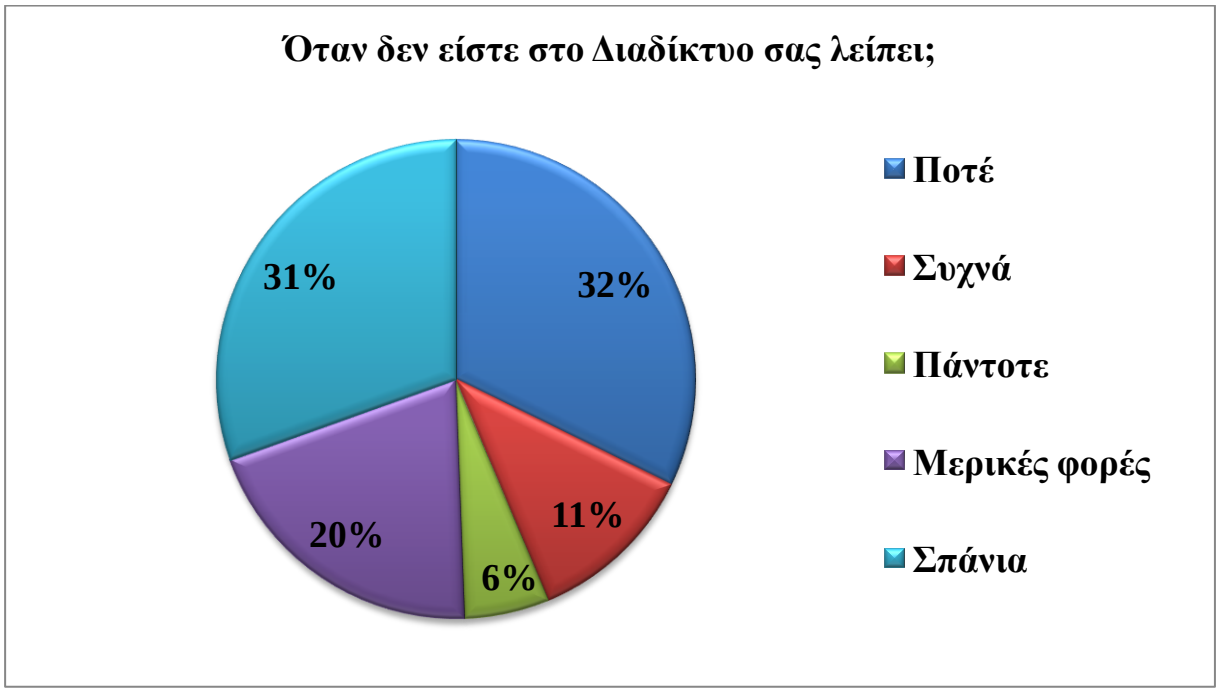
Έχει πάντως ιδιαίτερη βαρύτητα το να μη θεωρήσουν οι γονείς το Διαδίκτυο τον κακό δαίμονα των καιρών και να μην ενστερνιστούν την βολική άποψη ότι προκαλεί εθισμό. Το Διαδίκτυο είναι ένα μέσο επικοινωνίας, γνώσης, αλλά και ψυχαγωγίας. Είναι χρήσιμο, θετικό και διευκολύνει την ζωή των χρηστών σε ένα μεγάλο ποσοστό. Η ατομική ευθύνη ως προς τη συνετή χρήση του από τους γονείς και τα παιδιά είναι τεράστια. Πρέπει ο καθένας να γνωρίζει τι θέλει να

κάνει και να αυτοπεριορίζεται. Η ενημέρωση των εκπαιδευτικών και τα σεμινάρια στους έφηβους από ειδικούς μαζί με τη συνεργασία της οικογένειας, θα βοηθήσουν σημαντικά στη εκπαίδευση των νέων ως προς την ανακάλυψη της υγιούς και συνετής χρήσης του Διαδικτύου.

Στα παρακάτω σχήματα παρουσιάζονται οι απαντήσεις σε δείγμα 1183 μαθητών γυμνασίου και λυκείου, σε έρευνα που πραγματοποιήθηκε την περίοδο 2006-2007 από το Ινστιτούτο Οπτικοακουστικών Μέσων.

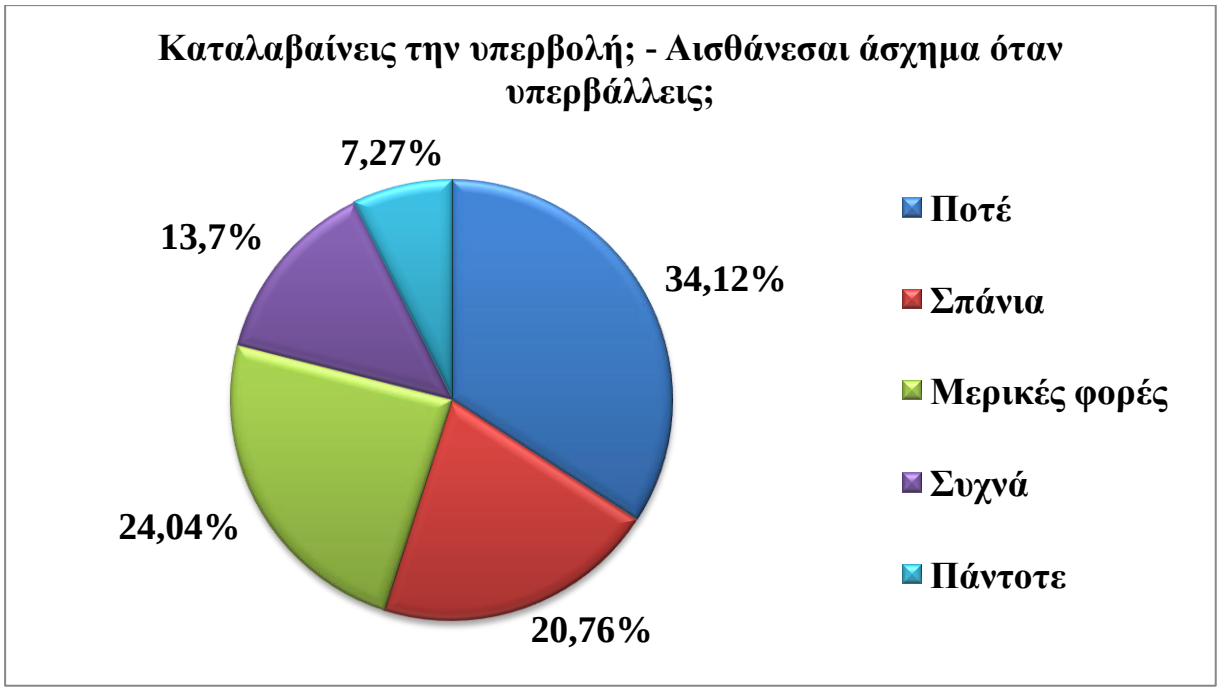


Σχήμα 13 – Σημαντικότητα Διαδικτύου στην ζωή των παιδιών[38]

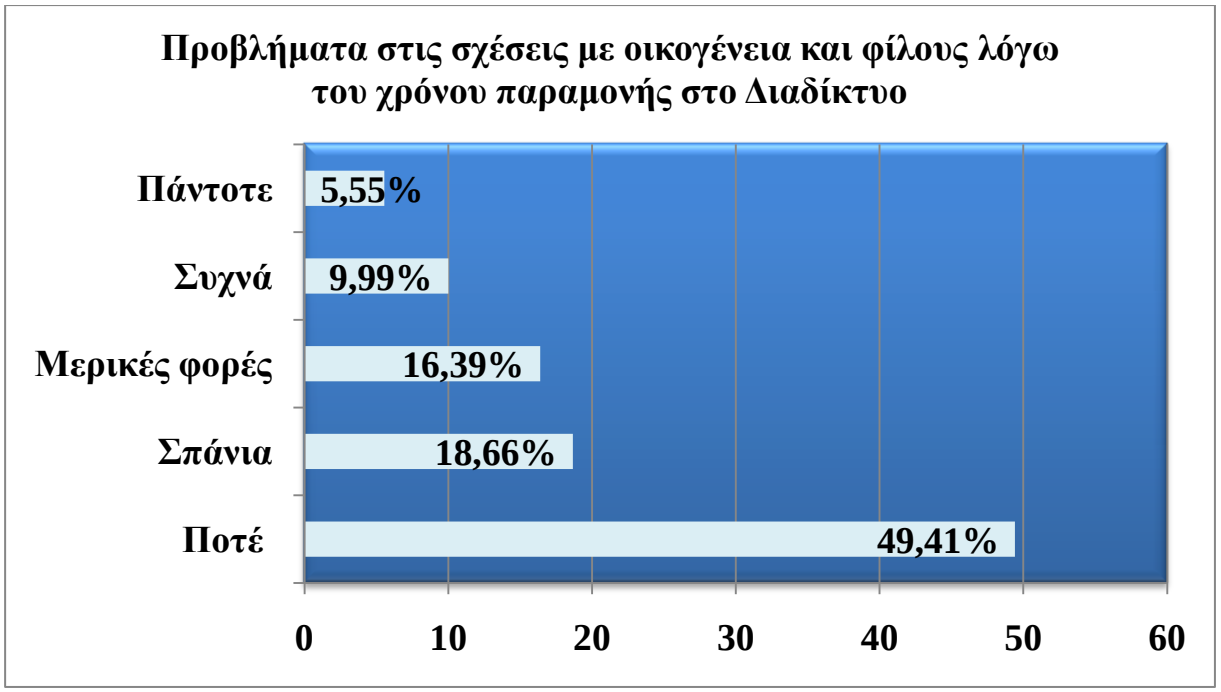


Σχήμα 14 – Αίσθημα Έλλειψης[39]

[38] ,[39] Καθημερινή, 25/05/2008



Σχήμα 15 – Αίσθηση Υπερβολής[40]



Σχήμα 16 – Προβλήματα στις σχέσεις [41]

[40,41] Καθημερινή, 25/05/2008

3.3 Διαδικτυακά παιχνίδια[42]

Μια από τις συνηθέστερες και πιο αγαπημένες ασχολίες των παιδιών στο Διαδίκτυο είναι τα ηλεκτρονικά παιχνίδια, τα οποία είναι άρρηκτα δεμένα με την εξέλιξη του Διαδικτύου, έχοντας ωθήσει την ανάπτυξη και τη διαμόρφωση του καθοριστικά. Τα παιχνίδια μπορούν να γίνουν διασκεδαστικά και επιμορφωτικά αν χρησιμοποιηθούν σωστά, μπορούν όμως να γίνουν επικίνδυνα για κάποιον που δεν ξέρει τι χρειάζεται να προσέξει.

Τα διαδικτυακά παιχνίδια (online games) διαφέρουν από τα κανονικά, διότι χρησιμοποιούν μία ενεργή σύνδεση δικτύου. Οι παίχτες μπορούν να παίζουν και να επικοινωνούν μεταξύ τους μέσα στο παιχνίδι. Αυτό δεν περιλαμβάνει μόνο τα παιχνίδια που παίζονται στο Διαδίκτυο, αλλά επίσης εκείνα που παίζονται σε σύνδεση μέσω κονσόλας, μέσω κινητών τηλεφώνων ή μέσω ομότιμων δικτύων. Παιχνίδια τα οποία δεν απαιτούν ενεργή σύνδεση δικτύου για τη δραστηριότητα παιχνιδιού, αλλά χρησιμοποιούν μόνο το Διαδίκτυο για τη δημοσιοποίηση υψηλών βαθμολογιών, τη λήψη στοιχείων παιχνιδιού ή την ανταλλαγή δεδομένων, δεν θεωρούνται διαδικτυακά παιχνίδια.

Σε μερικά ηλεκτρονικά παιχνίδια μπορούν να παίξουν παραπάνω από ένας παίχτες που μοιράζονται την ίδια περιοχή του παιχνιδιού (multiplayer παιχνίδια). Οι παίχτες μπορούν είτε να δημιουργήσουν ομάδες που παίζουν μεταξύ τους είτε απλά να βλέπουν ποιος μεμονωμένος παίχτης είναι ο καλύτερος. Μπορεί κανείς να παίξει multiplayer παιχνίδια μέσω υπολογιστών συνδεδεμένων σε τοπικό δίκτυο ή μέσω Διαδικτύου.

Αυτό που καθιστά τα διαδικτυακά παιχνίδια τόσο ιδιαίτερα, είναι το υψηλό επίπεδο διαδραστικότητας που δημιουργείται μεταξύ χρηστών που δεν γνωρίζονται απαραίτητα μεταξύ τους. Ενώ σε offline περιβάλλον οι άνθρωποι τις περισσότερες φορές έχουν να αντιμετωπίσουν χαρακτήρες που ελέγχονται

[42] «Παιδί & INTERNET», 09/09/2007
http://www.saferinternet.gr
Χρυσοστομίδου Β. (11 Μαΐου 2008), «Παιδιά στο ίντερνετ», περιοδικό «Κ», τεύχος 258, σελ.29-32
Καθημερινή 25/05/2008

από τον υπολογιστή (με εξαίρεση τα παιχνίδια τοπικού δικτύου), όταν παίζουν online συναγωνίζονται με χαρακτήρες που ελέγχονται από άλλους παίκτες. Από την άποψη της προστασίας διαπιστώνεται μεγάλη διαφορά ανάμεσα στα δύο παραπάνω είδη των παιχνιδιών, καθώς οι γονείς πρέπει να αφήσουν τα παιδιά τους (με ή χωρίς επίβλεψη) σε ένα περιβάλλον όπου μπορούν να διαδράσουν (chat, ζωντανή συζήτηση, μάχη) δημιουργώντας μακροχρόνιες και στενές σχέσεις με άγνωστα άτομα.

Πολλές φορές, άτομα τα οποία είναι κλεισμένα στον εαυτό τους ή υστερούν σωματικής δύναμης και αυτοπεποίθησης, μπαίνοντας στον εικονικό κόσμο αποκτούν τη δυνατότητα μιας δεύτερης πραγματικότητας οπού μπορούν να διαμορφώσουν το προφίλ που θα ήθελαν. Μια τέτοιου είδους «επιβεβαίωση» θα την αναζητήσει ο έφηβος που δεν την βρίσκει μέσα στην οικογένεια του.

3.3.1 Οι Κίνδυνοι των παιχνιδιών

3.3.1.1 Εθισμός

Το μεγαλύτερο και σοβαρότερο πρόβλημα που δημιουργείται από τα διαδικτυακά παιχνίδια είναι το πρόβλημα του εθισμού. Έρευνες έχουν αποδείξει ότι αυτό σπάνια έχει να κάνει με το ίδιο το παιχνίδι, αλλά με το κοινωνικό δίκτυο που υπάρχει στο παιχνίδι. Οι συμπαίκτες και οι αντίπαλοι του χρήστη είναι άλλα φυσικά πρόσωπα, με αποτέλεσμα να αποδεσμεύεται δυσκολότερα. Για παιδιά που δεν είναι ικανά να διαμορφώσουν τακτικούς κοινωνικούς δεσμούς στην δική τους πραγματική κοινότητα, αυτές οι διαδικτυακές κοινότητες μπορούν να δώσουν ώθηση στην αυτοπεποίθησή τους και να τους επιτρέψουν κατ' επέκταση να δημιουργήσουν σχέσεις με τους γύρω τους.

Ο κίνδυνος της υπερβολικής ενασχόλησης των παικτών με ένα παιχνίδι για ώρες καθημερινά, μπορεί να επηρεάσει το υπόλοιπο της ζωής τους σοβαρά. Όταν ένα παιδί παίζει ηλεκτρονικά παιχνίδια τέσσερεις ή πέντε ώρες την ημέρα, αρχίζει να δημιουργείται πρόβλημα. Τα παιδιά πολλές φορές βρίσκουν καταφύγιο σε αυτά και ξεφεύγουν από την πραγματικότητα.

Συχνά έχουν παρατηρηθεί ακραία φαινόμενα εθισμού σε διαδικτυακά παιχνίδια οπού έφηβοι, ή και μικρότερης ηλικίας, έπαιζαν για πάνω από 12 ώρες την ημέρα για διάστημα μηνών (ακόμα και σε Internet cafe), παραμελούσαν την προσωπική τους υγιεινή, δεν έτρωγαν, παραμελούσαν τις σχολικές τους υποχρεώσεις και ζούσαν την καθημερινότητα τους εξαρτημένη από τον εικονικό κόσμου του παιχνιδιού.

«Είναι στερεότυπο ότι τα παιδιά που παίζουν είναι αντικοινωνικά. Δεν είναι σαφές αν οφείλεται στα παιχνίδια ή όχι. Τα παιχνίδια δεν δημιουργούν εθισμό από μόνα τους, βρίσκουν το έδαφος εκεί που υπάρχει ήδη. Σε πολλές περιπτώσεις ικανοποιούν και άλλες ανάγκες όπως κοινωνικότητα και μάθηση. Υπάρχει μάλιστα ρεύμα στην εκπαιδευτική τεχνολογία που προσπαθήσει να χτίσει πάνω σε αυτά. Όπως η τηλεόραση ανταγωνίστηκε τη γειτονιά και τα παιδιά αντί να βγουν να παίξουν έκατσαν να δουν τηλεοπτικές σειρές, έτσι και τα παιχνίδια ή το Διαδίκτυο σήμερα διεκδικεί ένα κομμάτι του χρόνου μας. Είναι ζήτημα προσωπικής επιλογής.» αναφέρει ο κ. Δ. Γκούσκος, λέκτορας στο Τμήμα Επικοινωνίας και ΜΜΕ του Πανεπιστημίου Αθηνών.

3.3.1.2 Βίαιη συμπεριφορά

Πολλές έρευνες έχουν πραγματοποιηθεί για να βρεθούν τυχόν δεσμοί μεταξύ των ηλεκτρονικών παιχνιδιών και της βίαιης συμπεριφοράς. Δεν έχει εδραιωθεί ακόμα επιστημονικά η ύπαρξη μιας τέτοιας σχέσης, ούτε αναμένεται ότι κάτι τέτοιο θα γίνει ποτέ, παρά τις αναφορές και τα περιστατικά που κάνουν λόγο για το αντίθετο. Μια βραχυχρόνια αλλαγή συμπεριφοράς, που δεν ξεπερνά την μία ώρα, μπορεί να είναι απόρροια της έκκρισης αδρεναλίνης κατά την διάρκεια του παιχνιδιού και τίποτε περισσότερο. Είναι όμως σημαντικό ένα παιδί να δίνει λίγο χρόνο στον εαυτό του για να ηρεμήσει μετά από ένα παιχνίδι πριν πάει για ύπνο, αλλιώς μπορεί να διαταραχθεί ο ύπνος του και αυτό να οδηγήσει σε περαιτέρω προβλήματα. Η συστηματική ενασχόληση με τα παιχνίδια είναι μια κυρίως στατική δραστηριότητα. Πρέπει λοιπόν να γίνονται συχνά διαλείμματα,

να υπάρχει φυσική κίνηση και να παρέχονται αρκετά υγρά και τροφή στον οργανισμό.

3.3.1.3 Παρενόχληση

Το πρόβλημα της παρενόχλησης εμφανίζεται και στα διαδικτυακά παιχνίδια. Πολλοί είναι αυτοί που παρενοχλούν τους άλλους παίχτες, ιδίως τους αρχάριους, χρησιμοποιούν ακατάλληλη γλώσσα, κλέβουν και γενικά χρησιμοποιούν το παιχνίδι μόνο και μόνο για να ενοχλήσουν εύκολους στόχους ή να παρενοχλήσουν κάποιον συγκεκριμένο παίκτη που αντέδρασε στην κακή τους πρόθεση. Αν και είναι μόνο ένα μικρό ποσοστό της κοινότητας των παικτών βιντεοπαιχνιδιών, πολλές εταιρείες φοβούνται πως λόγω των παρενοχλητών, μπορεί να χάσουν συνδρομητές. Ως αποτέλεσμα, πολλές τοποθεσίες και πάροχοι παιχνιδιών, αρχίζουν να γίνονται λιγότερο ανεκτικοί με τους παρενοχλητές και χρησιμοποιούν νέες μεθόδους παρακολούθησης ή περιορισμού της δράσης τους.

Η αγνόηση των παρενοχλητών βοηθά σε αυτές τις περιπτώσεις διότι οι περισσότεροι από αυτούς θα βαρεθούν και θα σταματήσουν. Οι αλλαγές των ρυθμίσεων του παιχνιδιού, οι τοποθεσίες με αυστηρούς κανόνες, τα παιχνίδια που περιορίζουν τους παρενοχλητές και η δημιουργία ενός κλειστού παιχνιδιού, που επιτρέπεται δηλαδή η συμμετοχή μόνο σε φίλους, είναι χρήσιμες και αποτελεσματικές λύσεις.

Επίσης καλό είναι να αποφεύγεται η χρήση προκλητικών ονομάτων και ψευδώνυμων που μπορούν να προκαλέσουν τους παρενοχλητές. Τα προσωπικά δεδομένα όπως ονοματεπώνυμο, αριθμοί τηλεφώνου ή διευθύνσεις ηλεκτρονικού ταχυδρομείου δεν πρέπει ποτέ να αποκαλύπτονται μέσα σε κάποιο παιχνίδι.

Εάν κάποιος παρενοχλεί συνεχώς το παιδί, καλό είναι αυτό να δοκιμάσει κάποιο άλλο παιχνίδι ή να διακόψει την δραστηριότητα του και να συνεχίσει αργότερα. Παρόλα αυτά, ο καλύτερος τρόπος είναι να ενημερωθούν οι γονείς και να

προετοιμάσουν τα παιδιά για το πώς να αντιμετωπίσουν τους παρενοχλητές. Η ανοικτή συζήτηση με τα παιδιά είναι σημαντική, όσον αφορά οποιαδήποτε διαδικτυακή δραστηριότητα στην οποία εμπλέκονται.

3.3.1.4 Έκθεση σε διαφημιστικό υλικό

Οι διαφημίσεις με τη μορφή παιχνιδιού και οι διαφημίσεις ενσωματωμένες σε παιχνίδια γίνονται όλο και πιο συχνές. Ήδη τα μικρά παιδιά δυσκολεύονται να διαχωρίσουν τη διαφήμιση από το κύριο πρόγραμμα στην τηλεόραση, παρ' όλο που τα όρια εκεί παραμένουν ευδιάκριτα. Στα διαδικτυακά παιχνίδια ωστόσο, τα όρια μεταξύ μιας εμπορικής και μιας ιστοσελίδας ψυχαγωγίας είναι πολύ δυσδιάκριτα, σχεδόν ανύπαρκτα, με αποτέλεσμα τα παιδιά συχνά να μην αντιλαμβάνονται ότι πρόκειται για διαφήμιση. Άλλωστε, αυτός ακριβώς είναι και ο στόχος.

Τα παιδιά παίζουν σε μια κοινωνία «brand names» όπου δεν ξεχωρίζουν την ψυχαγωγία από τη διαφήμιση. Ελάχιστα παιδιά στην ηλικία 9 έως 11 ετών αντιλαμβάνονται ότι η αγαπημένη τους ιστοσελίδα έχει εμπορικούς σκοπούς. Τα περισσότερα θεωρούν ότι οι ιστοσελίδες έχουν φτιαχτεί αποκλειστικά για διασκέδαση. Μέσα στα παιχνίδια τα εμπορικά μηνύματα εμφανίζονται ως λογότυπα, φιγούρες και χαρακτήρες μασκότ που τα παιδιά ταυτίζουν με το ίδιο το προϊόν που αντιπροσωπεύουν. Επιπλέον, μετά την εγγραφή τους σε μια υπηρεσία ή σε ένα παιχνίδι, τα παιδιά αρχίζουν να λαμβάνουν πληροφορίες και διαφημίσεις και για άλλα προϊόντα. Υπάρχουν ακόμα και κωδικοί κρυμμένοι σε προϊόντα οπού τα παιδιά πρέπει να αγοράσουν ώστε να εντοπίσουν τον κρυμμένο κωδικό με τον οποίο θα «περάσουν πίστα» σε κάποιο διαδικτυακό παιχνίδι.

3.3.1.5 Ακατάλληλο περιεχόμενο

Τα ηλεκτρονικά παιχνίδια απευθύνονται σε ένα καταναλωτικό κοινό ευρέως ηλικιακού φάσματος. Επομένως υπάρχουν και παιχνίδια που περιέχουν ακατάλληλο περιεχόμενο για ανήλικους ή για πολύ μικρά παιδιά. Για παράδειγμα, πολύ συχνή είναι η παρουσία βίαιων σκηνών στα ηλεκτρονικά παιχνίδια, ενώ διαδεδομένη είναι η χρήση χυδαίας γλώσσας και σεξουαλικών αναφορών.

3.3.2 Σύστημα αξιολόγησης P.E.G.I.[43]

Το σύστημα ηλικιακών διαβαθμίσεων με την ονομασία Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (Pan-European Game Information – P.E.G.I.) έχει σχεδιαστεί προκειμένου να βοηθήσει τους Ευρωπαίους γονείς να λαμβάνουν υπεύθυνες αποφάσεις σχετικά με την αγορά παιχνιδιών.

Τέθηκε σε εφαρμογή την άνοιξη του 2003 και αντικατέστησε μια σειρά από εθνικά συστήματα ηλικιακών διαβαθμίσεων, με ένα ενιαίο σύστημα το οποίο χρησιμοποιείται πλέον στο μεγαλύτερο μέρος της Ευρώπης, σε 30 χώρες (Αυστρία, Δανία, Ουγγαρία, Λετονία, Νορβηγία, Σλοβενία, Βέλγιο, Εσθονία, Ισλανδία, Λιθουανία, Πολωνία, Ισπανία, Βουλγαρία, Φινλανδία, Ιρλανδία, Λουξεμβούργο, Πορτογαλία, Σουηδία, Κύπρος, Γαλλία, Ισραήλ, Μάλτα, Ρουμανία, Ελβετία, Τσεχική Δημοκρατία, Ελλάδα, Ιταλία, Κάτω χώρες, Σλοβακία και Ηνωμένο Βασίλειο).

Το σύστημα υποστηρίζεται από τους κυριότερους κατασκευαστές κονσολών, συμπεριλαμβανομένων της Sony, της Microsoft και της Nintendo, καθώς και από τους εκδότες και τους προγραμματιστές αλληλεπιδραστικών παιχνιδιών σε όλη την Ευρώπη. Το σύστημα ηλικιακών διαβαθμίσεων αναπτύχθηκε από την Ευρωπαϊκή Ομοσπονδία Αλληλεπιδραστικού Λογισμικού (Interactive Software Federation of Europe - ISFE).

[43] http://www.saferinternet.gr/
http://www.pegi.info/gr/index/id/212

Το σύστημα P.E.G.I. αποτελείται από δύο μέρη. Στο πρώτο μέρος αναγράφεται η κατάταξη του παιχνιδιού σε ηλικιακές ομάδες (3+, 7+, 12+, 16+, 18+,) και στον δεύτερο μέρος ο χαρακτηρισμός του περιεχομένου (βία, τζόγος, φόβος, σεξ, ναρκωτικά, ρατσισμός, χυδαία γλώσσα).

Σχήμα 17 – Σύστημα P.E.G.I. με βάση την ηλικία

ΒΙΑ

Το παιχνίδι εμπεριέχει απεικονίσεις βίας.

ΝΑΡΚΩΤΙΚΑ

Το παιχνίδι απεικονίζει τη χρήση ναρκωτικών ή εμπεριέχει αναφορές σε αυτήν.

ΧΥΔΑΙΑ ΓΛΩΣΣΑ

Το παιχνίδι εμπεριέχει χυδαία γλώσσα.

ΦΟΒΟΣ

Το παιχνίδι μπορεί να είναι τρομακτικό για τα μικρά παιδιά.

ΣΕΞ

Το παιχνίδι απεικονίζει γυμνό και/ή σεξουαλική συμπεριφορά ή σεξουαλικές αναφορές.

ΔΙΑΚΡΙΣΕΙΣ

Το παιχνίδι απεικονίζει διακρίσεις ή εμπεριέχει υλικό που μπορεί να τις ενθαρρύνει.

ΤΖΟΓΟΣ

Παιχνίδια που παροτρύνουν σε τζόγο ή τον διδάσκουν.

Σχήμα 18 – Σύστημα P.E.G.I., Χαρακτηρισμός Περιεχομένου

Ενδιαφέρον παρουσιάζουν τα στοιχεία που διατέθηκαν στον Ελληνικό κόμβο στις 14 Απριλίου 2008 από τον οργανισμό I.S.F.E. (Interactive Software Federation of Europe). Σε σύνολο 8.873 παιχνιδιών που έχουν χαρακτηριστεί από το σύστημα χαρακτηρισμού παιχνιδιών P.E.G.I. το διάστημα από 1/3/2003 έως και 14/4/2008, το 81,5% των παιχνιδιών που θεωρούνται κατάλληλα για ηλικίες 7+ περιέχουν αναπαραστάσεις βίας. Το ποσοστό αυξάνεται στις μεγαλύτερες ηλικιακές κατηγορίες: 87,3% για ηλικίες 12+, 97,6% για ηλικίες 16+ και 92,6% για ηλικίες 18+.

Πίνακας 1: Ποσοστό παιχνιδιών με χαρακτηρισμό «Βία» ανά ηλικιακές ομάδες σε σύνολο 8.873 παιχνιδιών.

Βία	3+	7+	12+	16+	18+	Σύνολο
Όχι	4377	167	269	26	29	4868
Ναι		734	1848	1060	363	4005
Σύνολο	**4377**	**901**	**2117**	**1086**	**392**	**8873**

Βία (%)	3+	7+	12+	16+	18+
Όχι	100%	18,5%	12,7%	2,4%	7,4%
Ναι	0%	81,5%	87,3%	97,6%	92,6%
Σύνολο	100%	100%	100%	100%	100%

Η ανάλυση όλων των χαρακτηρισμών περιεχομένου σε σχέση με την ηλικιακή κατηγορία, καταδεικνύει ότι 45,15% επί του συνόλου των παιχνιδιών έχουν κάποιο χαρακτηρισμό περιεχομένου. Μερικά αξιοσημείωτα στοιχεία είναι τα εξής:

- Όλα τα παιχνίδια που ενημερώνουν ότι το περιεχόμενο μπορεί να είναι τρομακτικό για τα μικρά παιδιά (χαρακτηρισμός «φόβος»), ανήκουν στην ηλικιακή κατηγορία 7+ (241 συνολικά).

- 387 παιχνίδια από τα 8.873 παιχνίδια που αξιολογήθηκαν είναι διαδικτυακά παιχνίδια (online games). 139 από αυτά απευθύνονται σε παιδιά ηλικίας 3+. Στην κατηγορία των online παιχνιδιών υπάγονται και τα παιχνίδια που παίζονται σε σύνδεση μέσω κονσόλας, μέσω κινητών τηλεφώνων ή μέσω ομότιμων δικτύων (δίκτυα που στηρίζονται στο εύρος ζώνης και σε προσωπικούς υπολογιστές αντί για εξυπηρετητές, για να δώσουν τη δυνατότητα παιχνιδιού πολλαπλών παικτών).
- Ιδιαίτερο ενδιαφέρον παρουσιάζει η ηλικιακή κατηγορία 12+. Ειδικότερα:
  α) 65,4% των παιχνιδιών που εμπεριέχουν χυδαία γλώσσα έχουν ηλικιακό χαρακτηρισμό 12+ (556 σε σύνολο 850).
  β) 76,8% των παιχνιδιών που έχουν τον χαρακτηρισμό «σεξ» (δηλαδή, είτε απεικονίζουν γυμνότητα και/ή σεξουαλική συμπεριφορά ή έχουν σεξουαλικές αναφορές) ανήκουν στην ηλικιακή κατηγορία 12+ (139 σε σύνολο 181).
  γ) 46,1% των παιχνιδιών που έχουν τον χαρακτηρισμό «βία» ανήκουν στην ηλικιακή κατηγορία 12+ (1848 σε σύνολο 4006).

Θα πρέπει να τονιστεί, ότι ο χαρακτηρισμός της βίας διαφέρει ανά ηλικιακή ομάδα. Έτσι, ο χαρακτηρισμός της βίας στα παιχνίδια που απευθύνονται σε επτάχρονα παιδιά μπορεί κάλλιστα να αναφέρεται σε διασκεδαστική (αλλά επιθετική) συμπεριφορά χαρακτήρων καρτούν, ενώ αντίστοιχα στα παιχνίδια για τους δεκαεξάχρονους να υποδεικνύει πιστή αναπαράσταση σκοτωμών και άλλων βίαιων πράξεων.

Πίνακας 2: Ανάλυση παιχνιδιών με χαρακτηρισμό περιεχομένου ανά ηλικιακή κατηγορία.

	3+	7+	12+	16+	18+	Σύνολο	%*
Ναρκωτικά 	-	-	-	29	30	**59**	**0,7%**
Χυδαία Γλώσσα 	-	-	556	147	147	**850**	**9,6%**
Διακρίσεις 	-	-	5	-	8	**13**	**0,15%**
Φόβος 	-	241	-	-	-	**241**	**2,7%**
Τζόγος 	-	-	65	6	6	**77**	**0,9%**
Online 	139	34	80	88	46	**387**	**4,4%**
Σεξ 	-	-	139	33	9	**181**	**2%**
Βία 	-	734	1848	1060	364	**4006**	**45,15%**

* επί του συνόλου των παιχνιδιών που έχουν αξιολογηθεί (N=8.873)

Για να γίνει πιο κατανοητό το θέμα της ασφάλειας των παιδιών στα διαδικτυακά παιχνίδια, ας σκεφτούν οι γονείς ένα παράδειγμα από την καθημερινή ζωή: Θα άφηναν ποτέ τα παιδιά τους να παίζουν σε ένα πάρκο χωρίς επιτήρηση, να συζητούν και να δημιουργούν σχέσεις με αγνώστους; Η απάντηση στο ερώτημα εξαρτάται σε μεγάλο βαθμό από την ηλικία του παιδιού αλλά και από την ασφάλεια του πάρκου. Το ίδιο ισχύει και για τα διαδικτυακά παιχνίδια, οι γονείς θα πρέπει να έχουν πρόσβαση σε μια αντικειμενική πηγή πληροφόρησης για το περιβάλλον στο οποίο τα παιδιά τους αφιερώνουν σημαντικό χρόνο παίζοντας με άλλους ανθρώπους. Το να έχουν μια καλή γνώση των κατηγοριών των παιχνιδιών που είναι διαθέσιμα μέσω Διαδικτύου, είναι απαραίτητη προϋπόθεση για την αξιολόγηση και την αποφυγή των πιθανών κινδύνων.

3.4 Ηλεκτρονική παρενόχληση[44]

Ως ηλεκτρονική παρενόχληση (cyber bullying), ορίζεται οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς, που θεσπίζεται και πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών επικοινωνίας, συγκεκριμένα του Διαδικτύου και των κινητών τηλεφώνων και η οποία επαναλαμβάνεται ανά τακτά ή άτακτα χρονικά διαστήματα. Ο όρος cyber bulling έχει τις ρίζες του στην παραδοσιακή φυσική ή ψυχολογική φοβέρα όπου ο στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του.

Τέτοιου είδους συμπεριφορές μπορεί να κάνουν τα νέα άτομα να νιώθουν μοναχικά, δυστυχή, φοβισμένα και να αισθάνονται ανασφαλή. Χάνουν την εμπιστοσύνη στον εαυτό τους, αρνιούνται να πάνε στο σχολείο και απομονώνονται από τις παρέες τους. Σε ακραίες περιπτώσεις, η συνεχής, επίμονη και έντονη παρενόχληση, έχει οδηγήσει σε τρομερές συνέπειες όπως η πρόθεση για αυτοκτονία.

[44] http://www.saferinternet.gr
«Παιδί & INTERNET», 09/09/2009
http://www.ethnos.gr/article.asp?catid=11424&subid=2&pubid=2394807

Περιστατικά παρενόχλησης μεταξύ παιδιών και εφήβων μπορούν να συμβούν με πολύ διαφορετικές μορφές. Δεν εκδηλώνονται μόνο μέσω καυγάδων και επιθετικότητας, αλλά και μέσω διαφορετικών τύπων εκφοβισμού που αφήνουν το θύμα εκτεθειμένο.

Είδη παρενόχλησης

- Μηνύματα (SMS, MMS, e-mail) με απειλητικό ή προσβλητικό περιεχόμενο.
- Ανάρτηση προσβλητικών/εξευτελιστικών φωτογραφιών, βίντεο και άλλου υλικού σε ιστοσελίδες όπου και άλλα άτομα έχουν πρόσβαση, όπως για παράδειγμα blogs, ιστοσελίδες κοινωνικής δικτύωσης, κ.α.
- Η διάδοση φημών στο περιβάλλον του θύματος μέσω της χρήσης κινητού, ηλεκτρονικού ταχυδρομείων και μέσω άλλων υπηρεσιών ηλεκτρονικής επικοινωνίας.
- Κλοπή «ταυτότητας».

Μερικές φορές προσβλητικά γραπτά μηνύματα προς κινητά τηλέφωνα στέλνονται μέσω ιστοσελίδων χρησιμοποιώντας ονόματα και τηλέφωνα ανθρώπων που δεν έχουν καμία σχέση με το μήνυμα αυτό, αλλά καταλήγουν να κατηγορούνται ότι το έστειλαν οι ίδιοι. Μια άλλη τεχνική που χρησιμοποιείται από τους παρενοχλητές είναι η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

Ήδη στην Ελλάδα υπάρχουν θύματα ηλεκτρονικού εκφοβισμού που έχουν απασχολήσει τη Δίωξη Ηλεκτρονικού Εγκλήματος, ενώ αποκαλυπτικά είναι τα ευρήματα έρευνας που πραγματοποιήθηκε στην Ελλάδα, για λογαριασμό της Ευρωπαϊκής δράσης «Safe Net Home», σε 450 μαθητές.

Τα αποτελέσματα έδειξαν ότι σχεδόν το 54% των μαθητών έχουν υπάρξει θύματα εκφοβισμού και πάνω από το 1/4 αυτών έχουν δεχτεί ουσιαστική ενόχληση-εκβιασμό ή εκφοβισμό. Περισσότεροι από τους μισούς γνώριζαν

κάποιο συμμαθητή ή συμμαθήτρια που είχε αντιμετωπίσει παρόμοιο πρόβλημα και πάνω από το 40% των θυμάτων δεν γνώριζαν ή δεν είχαν καμία ιδέα για το ποιος ευθυνόταν γι αυτή την πράξη.

«Για το προφίλ των παιδιών που προβαίνουν στην καταχρηστική συμπεριφορά του cyber bullying οι λίγες έρευνες που έχουν διεξαχθεί δείχνουν ότι τα κίνητρά τους είναι συχνά η ζήλια, η εκδίκηση, το αίσθημα υπεροχής και η επίδειξη δύναμης απέναντι στους συνομηλίκους», όπως αναφέρει η κ. Βάσω Αρτινοπούλου, αν. καθηγήτρια Εγκληματολογίας, Τμήμα Ψυχολογίας Παντείου Πανεπιστημίου.

3.4.1 Ρατσιστική παρενόχληση

Η ρατσιστική παρενόχληση προκύπτει όταν ορισμένα άτομα παρενοχλούνται εξαιτίας της φυλής τους, της κουλτούρας τους, ή της θρησκευτικής τους πίστης. Τα θύματα αυτού του τύπου παρενόχλησης είναι πολιτισμικές, φυλετικές ή θρησκευτικές μειονότητες. Σε αυτές τις περιπτώσεις οι ρατσιστικές βρισιές και η χρήση στερεοτυπικών εκφράσεων είναι πολύ διαδεδομένη.

Η χρήση του Διαδικτύου με σκοπό τη διάδοση ρατσιστικής, αντισημιτικής και άλλου είδους προπαγάνδας αυξάνεται σε όλο τον κόσμο. Οι στόχοι του μίσους μπορεί να ποικίλουν από τόπο σε τόπο, αλλά καμία χώρα δεν έχει ανοσία στο πρόβλημα. Συχνά τα πράγματα είναι πιο περίπλοκα αφού η διαχείριση ορισμένων ιστοσελίδων γίνεται από περισσότερες από μία χώρες.

Υπάρχει η συνεχώς αυξανόμενη ανησυχία ότι το διαδικτυακό μίσος μπορεί να προκαλέσει βία και να οδηγήσει σε κανονικά εγκλήματα μίσους. Ακόμα και αν είναι δύσκολο να εδραιωθεί ένας αιτιολογικός δεσμός, δεν υπάρχει αμφιβολία ότι το Διαδίκτυο μπορεί να χρησιμοποιηθεί ώστε να ενισχύσει το εχθρικό κλίμα εναντίον συγκεκριμένων ομάδων, όπως άλλωστε και για τη συγκέντρωση χρημάτων και την προσέλκυση συμπαθούντων.

Το Διαδίκτυο φιλοξενεί με ποικίλους τρόπους περιεχόμενο που μπορεί να χαρακτηριστεί ρατσιστικό. Οι πιο διαδεδομένοι είναι:

- **Ιστοσελίδες:** Ρατσιστικές ομάδες δημιουργούν ιστοχώρους, το περιεχόμενο των οποίων ενδέχεται να προσβάλλει ή να υποβιβάζει κάποιες ομάδες ανθρώπων. Επιπλέον μέσω τέτοιων ιστοσελίδων μπορεί να ενθαρρυνθεί η συμμετοχή σε ρατσιστικές ομάδες.
- **Παιχνίδια:** Παιχνίδια με ρατσιστικό περιεχόμενο εμφανίζονται πολύ συχνά στο Διαδίκτυο. Έχουν συνήθως προκλητικούς τίτλους και στο στόχαστρό τους βρίσκονται εθνικές και θρησκευτικές μειονότητες.
- **Περιεχόμενο ελεγχόμενο από τους επισκέπτες:** Υπάρχουν ιστοσελίδες στο Διαδίκτυο όπου ο καθένας μπορεί να δημοσιεύσει οτιδήποτε επιθυμεί, χωρίς να υποστεί έλεγχο. Έτσι είναι εξαιρετικά εύκολο να γραφτούν ρατσιστικά σχόλια.
- **E-mail, chat rooms, ομάδες συζητήσεων:** Οι ρατσιστικές ομάδες στέλνουν προσωπικά μηνύματα με πληροφορίες και ρατσιστικό υλικό, ενώ μέλη τους μπαίνουν σε forum και chat rooms, όπου χάρη στην ανωνυμία που τους προσφέρεται, επιδίδονται σε ρατσιστικές δημοσιεύσεις.

3.4.2 Αντιμετώπιση της ηλεκτρονικής παρενόχλησης

«Τα ζητήματα της προστασίας των ανηλίκων αποτελούν θέματα μείζονος προτεραιότητας, ιδιαίτερα τα τελευταία χρόνια, στην ατζέντα των συζητήσεων σε εθνικό, ευρωπαϊκό και παγκόσμιο επίπεδο. Είναι γεγονός ότι οι νέες μορφές θυματοποίησης απαιτούν νέες παρεμ-βάσεις πρόληψης, πέραν των παραδοσιακών μέτρων», επισημαίνει η Βάσω Αρτινοπούλου, αν. καθηγήτρια εγκληματολογίας στο τμήμα ψυχολογίας Παντείου πανεπιστημίου και προσθέτει: «Στο επίπεδο της πρόληψης θεωρείται σημαντική η ενημέρωση τόσο των παιδιών όσο και των γονέων και δασκάλων για τους κινδύνους που διατρέχουν με την κακή χρήση των νέων τεχνολογιών».

Για την πρόληψη και την αποφυγή της ηλεκτρονικής παρενόχλησης είναι απαραίτητο:

- Οι γονείς να συζητούν με τα παιδιά για την ηλεκτρονική παρενόχληση, να ενημερώνονται για το τι κάνουν τα παιδιά στο Διαδίκτυο, να βλέπουν τις σελίδες που επισκέπτονται, να τα συμβουλεύουν να μη δίνουν προσωπικές πληροφορίες, να τα ενημερώνουν ότι η ηλεκτρονική παρενόχληση δεν είναι ανώνυμη και ότι αφήνει ίχνη και τέλος, να εμπνεύσουν εμπιστοσύνη προς αυτά, ώστε να απευθυνθούν στους γονείς τους σε περίπτωση που πέσουν θύμα της ηλεκτρονικής παρενόχλησης. Οι γονείς δεν θα πρέπει απαγορεύουν τη χρήση του Διαδικτύου ως αντίδραση σε περιστατικό παρενόχλησης, γιατί αυτό θα αποθαρρύνει το παιδί από το να τους εμπιστευτεί.
- Τα παιδιά να μη δίνουν προσωπικές πληροφορίες σε chat rooms (δωμάτια συνομιλίας), σε ιστοσελίδες, σε blogs ή όπου αλλού στο Διαδίκτυο. Να μη αποκαλύπτουν σε κανέναν κωδικούς πρόσβασης. Αν λάβουν κάποιο απειλητικό μήνυμα, να μην απαντήσουν, αλλά να ενημερώσουν έναν ενήλικο.
- Τα παιδιά να μην ανοίγουν ποτέ e-mail από κάποιον που δεν ξέρουν, ή που γνωρίζουν εκ των προτέρων ότι αυτός μπορεί να τους απειλήσει.
- Αν τα παιδιά έχουν ήδη απειληθεί, οι γονείς θα πρέπει να τα εκπαιδεύουν να μην απαντούν σε αυτούς που τα ενοχλούν, να διαγράφουν τα απειλητικά μηνύματα χωρίς να τα ανοίγουν και να μη ζητούν εκδίκηση. Θα πρέπει να υπάρχει η διαβεβαίωση από τους γονείς ότι τα παιδιά δεν θα σταματήσουν τη χρήση του Διαδικτύου (ο φόβος των παιδιών είναι ότι αν αποκαλύψουν στους γονείς ότι είναι θύματα, οι γονείς θα τους απαγορεύσουν τη χρήση του Διαδικτύου). Ακόμα, οι γονείς θα πρέπει να βοηθούν τα παιδιά να καταγράφουν τις εμπειρίες τους (αυτό θα βοηθήσει αν χρειαστεί να επέμβει η αστυνομία).

- Να μην υποβαθμίζεται το συμβάν. Η παρενόχληση μπορεί να μη μείνει μόνο στο ηλεκτρονικό επίπεδο και να εξελιχθεί σε κάτι σοβαρότερο αν δεν δοθεί η πρέπουσα σημασία.

3.5 Παιδική πορνογραφία[45]

Η παιδική πορνογραφία είναι ίσως το πιο σοβαρό, επικίνδυνο και ευαίσθητο θέμα, που αφορά τους κινδύνους που ελλοχεύουν κατά την πλοήγηση των παιδιών στο Διαδίκτυο. Ο ορισμός της διαφέρει από την νομοθεσία της κάθε χώρας. Ο κοινός παράγοντας είναι οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Κάποιες φορές περιλαμβάνει φωτογραφίες που έχουν υποστεί ηλεκτρονική επεξεργασία η ακόμα και εικόνες με χαρακτήρες καρτούν.

Σήμερα, οι νέες τεχνολογίες και ειδικότερα το Διαδίκτυο έχουν γίνει μια από τις επικρατέστερες τεχνικές που χρησιμοποιούνται από τους παιδόφιλους, για να μοιραστούν παράνομο ψηφιακό φωτογραφικό υλικό ανηλίκων και για να δελεάσουν τα παιδιά σε παράνομες σεξουαλικές πράξεις. Το Διαδίκτυο κάνει πιο εύκολη την προσέγγιση από τους «παραβάτες» των υποψηφίων θυμάτων τους, ενώ παράλληλα δίνει σε αυτούς απεριόριστη πρόσβαση σε μια κοινότητα ανθρώπων με τις ίδιες σεξουαλικές προτιμήσεις.

Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Επιπλέον υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα. Σε ορισμένες χώρες, όπως στην Ελλάδα και την Ισπανία, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας, είναι έγκλημα.

[45] http://www.saferinternet.gr
«Παιδί & INTERNET», 09/09/2009
http://www.annaefthymiou.gr
http://www.skai.gr

Σύμφωνα με τη σύμβαση για τα διαδικτυακά εγκλήματα του συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές:

- Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
- Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Μερικά στατιστικά στοιχεία που έδωσε στη δημοσιότητα η UNESCO (United Nations Educational, Scientific and Cultural Organization) σχετικά με την παιδική πορνογραφία στο Διαδίκτυο βοηθούν στην αντίληψη του προβλήματος και τις διαστάσεις που καταλαμβάνει:

- Ο τζίρος της βιομηχανίας παιδικής πορνογραφίας στο Διαδίκτυο ξεπερνά τα 3 δις ευρώ κάθε χρόνο.
- Ο αριθμός των ιστοσελίδων που φιλοξενούν πορνογραφικό περιεχόμενο με πρωταγωνιστές ανήλικα παιδιά, ακόμη και βρέφη, υπολογίζεται ότι σημείωσε την τελευταία πενταετία αύξηση της τάξης του 345%.
- Ορισμένες ιστοσελίδες παιδικής πορνογραφίας, έχουν ημερήσια επισκεψιμότητα περίπου 150.000, παρά το υψηλό κόστος.

Κάποια άλλα πολύ σοβαρά στοιχεία γύρω από το θέμα:

- Μηνιαία εμφανίζονται 67 με 82 νέες ιστοσελίδες και περίπου 8 με 21 σε καθημερινή βάση.
- Είκοσι παιδιά (2-12 ετών) εμφανίζονται κάθε μήνα σε τέτοιες ιστοσελίδες, ενώ σύμφωνα με τις πληροφορίες που δίνουν κατά καιρούς στη δημοσιότητα οι διάφορες υπηρεσίες και οργανισμοί καταπολέμησης της παιδοφιλίας στην Ευρώπη, κάθε εβδομάδα γύρω στις 20.000 φωτογραφίες με άσεμνες στάσεις παιδιών, από οκτώ μηνών μέχρι 17

ετών, προωθούνται στις 100 και πλέον χιλιάδες πορνογραφικές ιστοσελίδες του κυβερνοχώρου.

- Σύμφωνα με κεντρική έρευνα της Αμερικής, 200 νέες εικόνες παιδικής πορνογραφίας ταχυδρομούνται καθημερινά, και 1 στα 7 παιδιά έχει λάβει μια σεξουαλική διαδικτυακή παρενόχληση κατά την πλοήγησή του. Αυτό όμως που συγκλονίζει είναι ότι ένα 35% των παραβατών είναι γονείς κακοποιημένων παιδιών ενώ ένα 10% αποτελείται από άλλα συγγενικά πρόσωπα.
- Τα δύο σημαντικότερα κέντρα διακίνησης πορνογραφικού υλικού είναι οι ΗΠΑ και η Ρωσία. Το φαινόμενο όμως παρουσιάζει έξαρση και στην Ανατολική Ευρώπη, τη Βρετανία και τη Λατινική Αμερική.

Το πρόβλημα της παιδικής πορνογραφίας εμφανίζεται και στην Ελλάδα:

- Το 1997 απασχολούσαν τις αρμόδιες αρχές μία ή δύο υποθέσεις παιδικής πορνογραφίας το τρίμηνο, ενώ σήμερα εντοπίζονται καθημερινά 5-7 σχετικά ηλεκτρονικά ίχνη.
- Μέσα σε διάστημα 15 μηνών και παρόλα τα εμπόδια, νομικά και άλλα, το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής έφερε στο φως 30 τέτοιες υποθέσεις, ενώ από τους 85 συνολικά κατηγορούμενους οι 40 έχουν συλληφθεί.
- Περίπου 107.572 εικόνες σεξουαλικά κακοποιημένων παιδιών ταχυδρομήθηκαν στους Ελληνικούς ιστοχώρους κατά τη διάρκεια των προηγούμενων τριών ετών, αλλά οι Ελληνικές αρχές έχουν κάνει μόνο 119 σχετικές συλλήψεις.
- Σύμφωνα με τα στοιχεία Ελληνικών υπηρεσιών, χιλιάδες άτομα στην Ελλάδα πληρώνουν ετησίως για να έχουν πρόσβαση σε υλικό παιδιών που έχουν πέσει θύματα της «σεξουαλικής βιομηχανίας».

3.5.1 Διαφορές παιδικής πορνογραφίας και πορνογραφίας ενηλίκων

Η παιδική πορνογραφία διαφέρει σε πολύ μεγάλο βαθμό από την πορνογραφία ενηλίκων. Οι δύο αυτοί όροι θα πρέπει να διαχωρίζονται, καθώς παρουσιάζουν σημαντικές διαφορές και νομοθετικές ρυθμίσεις.

Η πορνογραφία ενηλίκων ορίζεται ως μια αναπαράσταση (βίντεο, dvd, ήχος, κείμενο) ενός ενήλικου ατόμου που συμμετέχει ή απεικονίζεται ως συμμετέχων σε σαφή σεξουαλική δραστηριότητα. Οι νομικοί καθορισμοί και τα διαφορετικά επίπεδα αποδοχής διαφέρουν από χώρα σε χώρα. Παρόλα αυτά, υπάρχει αρκετά μεγάλος ο βαθμός συναίνεσης σε ευρωπαϊκό επίπεδο, ότι η πρόσβαση στο συγκεκριμένο υλικό μπορεί να επηρεάσει τη σωματική και την πνευματική ανάπτυξη των ανηλίκων και ότι θα πρέπει να επιτρέπεται μόνο σε ενηλίκους.

Πολλοί άνθρωποι το βρίσκουν δύσκολο να φανταστούν πορνογραφικές εικόνες παιδιών και επομένως δεν αντιλαμβάνονται τον όρο «παιδική πορνογραφία». Αυτό που είναι σημαντικό είναι ότι η παιδική πορνογραφία είναι η απεικόνιση ενός εγκλήματος, όπου θύμα είναι ένας ανήλικος. Είναι φωτογραφίες της σεξουαλικής κακοποίησης ενός παιδιού και τίποτα λιγότερο από μια επίθεση σε ένα παιδί. Πρόκειται για εικόνες ενηλίκων σε σεξουαλικές δραστηριότητες με ανηλίκους και όταν αυτές οι φωτογραφίες διαδοθούν μέσω Διαδικτύου, οι ανήλικοι αυτοί γίνονται θύματα της ίδιας πράξης, ξανά και ξανά.

3.5.2 Ποιοι κινδυνεύουν

Οι έφηβοι εμφανίζονται ως η πιο ευάλωτη ηλικιακή ομάδα σε ότι αφορά την παιδική πορνογραφία και το πορνογραφικό περιεχόμενο που δημοσιεύεται γενικότερα στο Διαδίκτυο . Σύμφωνα με έρευνα που δημοσίευσε το 2004 το περιοδικό «Journal of Adolescent Health», το 76% των ατόμων που υπέστησαν σεξουαλική παρενόχληση η οποία ξεκίνησε μέσω διαδικτυακής επικοινωνίας ανήκουν στην ηλικιακή ομάδα των 13 έως 15 ετών. Η συντριπτική πλειοψηφία αυτών είναι κορίτσια. Και στον Ελληνικό χώρο τα στοιχεία συμπίπτουν. Σύμφωνα με έρευνα που δημοσιεύθηκε τον Ιούνιο του 2006, το 71% των

παιδιών ηλικίας μέχρι 12 ετών έχει ήδη συναντήσει πορνογραφικό υλικό μέσω Διαδικτύου είτε σκόπιμα είτε τυχαία (πηγή: Εταιρία Μελέτης Ανθρώπινης Σεξουαλικότητας).

Κατά την περίοδο της εφηβείας τα νεαρά άτομα εξερευνούν τη σεξουαλικότητά τους και προσπαθούν να ανεξαρτητοποιηθούν, κάνοντας την «προσωπική τους επανάσταση». Αυτή η στάση ανεξαρτησίας και η αναζήτηση νέων γνωριμιών μέσω Διαδικτύου, ως αγαπητού μέσου επικοινωνίας και κοινωνικής δικτύωσης, καθιστούν τους εφήβους την πιο ευαίσθητη ομάδα στο ζήτημα της πορνογραφίας αλλά και της σεξουαλικής παρενόχλησης.

3.5.3 Πρόσβαση σε υλικό

Αξιοσημείωτα είναι τα ευρήματα της έρευνας που διεξήγαγε το London School of Economics (2002), σύμφωνα με τα οποία το 90% των παιδιών που ρωτήθηκαν, ηλικίας από 8 έως 16 ετών, είχαν πρόσβαση σε πορνογραφικό υλικό, και μάλιστα τυχαία, κατά τη διάρκεια αναζήτησης πληροφοριών για τις σχολικές τους εργασίες. Μια τέτοιου είδους ελεύθερη και ανεμπόδιστη επαφή με υλικό ακατάλληλο για τις μικρότερες ηλικίες, ιδιαίτερα όταν είναι συνεχής και καθίσταται συνήθεια, μπορεί να έχουν βλαβερές συνέπειες στην ανάπτυξη των παιδιών και των εφήβων και να επηρεάσουν τη μετέπειτα κοινωνική και σεξουαλική τους συμπεριφορά.

Είναι πολύ εύκολο να «ανεβάσει» κάποιος φωτογραφικό υλικό στο Διαδίκτυο. Μπορεί είτε να την στείλει μέσω του ηλεκτρονικού ταχυδρομείου, είτε να τη δημοσιεύσει σε κάποια ιστοσελίδα, είτε να την προωθήσει μέσω κινητής τηλεφωνίας. Είναι επομένως εξαιρετικά πιθανό να συναντήσει κανείς παιδική πορνογραφία ενώ πλοηγείται στο Διαδίκτυο, ή προσπαθώντας να επικοινωνήσει με e-mail ή κινητό τηλέφωνο.

Οι αριθμοί άλλωστε μιλούν από μόνοι τους:

- Στις 25/04/2007, πληκτρολογώντας τη λέξη «sex» σε μια μηχανή αναζήτησης, εμφανίστηκαν ως αποτελέσματα 396.000.000 ιστοσελίδες (ωστόσο τα αποτελέσματα περιλαμβάνουν και ιστοσελίδες με ιατρικό ή άλλου είδους μη πορνογραφικό περιεχόμενο).
- Σύμφωνα με το Internet Watch Foundation, τη Βρετανική ανοιχτή γραμμή καταγγελίας ύποπτων ιστοσελίδων του δικτύου INHOPE, ο αριθμός των ιστοσελίδων που εμφανίζουν τις πιο άσχημες στιγμές σεξουαλικής κακοποίησης αυξήθηκε από 7% που ήταν το 2003 σε 29% το 2006.
- Έρευνα της Εταιρίας Μελέτης Ανθρώπινης Σεξουαλικότητας δείχνει ότι 65% των Ελλήνων θεωρεί ότι η πρόσβαση σε πορνογραφικό υλικό στο Διαδίκτυο είναι εύκολη, πολλοί πιστεύουν ότι ο εντοπισμός ιστοσελίδων που έχουν μόνο ελαφρύ περιεχόμενο πορνογραφίας είναι πολύ εύκολος, ενώ μόλις το 2% πιστεύει ότι ο εντοπισμός πορνογραφικών σελίδων είναι δύσκολος.

Υπάρχει λοιπόν τόσο μεγάλη προσφορά τέτοιου είδους υλικού που τα παιδιά ακόμα και μέσω μιας απλής μηχανής αναζήτησης μπορούν να το εντοπίσουν. Βέβαια ακόμη και αν δεν το αποζητήσουν τα ίδια, υπάρχουν πολλά άτομα που τα προσεγγίζουν στο Διαδίκτυο, δίνοντάς τους πορνογραφικό υλικό. Με πολύ γρήγορο τρόπο, κάποιος μπορεί να διαβιβάσει μέσω του Διαδικτύου φωτογραφίες σεξουαλικού περιεχομένου με παιδιά σε παραλήπτες από όλο τον κόσμο. Είναι προφανές, ότι εκτός από την ζημιά που γίνεται στα παιδιά που χρησιμοποιούνται για τη δημιουργία αυτών των φωτογραφιών, το υλικό αυτό κρύβει κινδύνους και για τα παιδιά που αποκτούν πρόσβαση σε αυτό. Το ίδιο ισχύει και για ιστοσελίδες με περιεχόμενο που προωθεί τη βία, τον ρατσισμό και το μίσος.

3.5.4 Grooming

Το grooming είναι η διαδικασία κατά την οποία, παιδόφιλοι, προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν δωμάτια ανοικτής επικοινωνίας (chat rooms) για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν μία σχέση φιλίας και εμπιστοσύνης με τα παιδιά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, το γονικό περιβάλλον τα ενδιαφέροντα, τα χόμπι, τον κοινωνικό τους περίγυρο, τις σεξουαλικές τους γνώσεις και εμπειρίες.

Τα παιδιά από τη μεριά τους νιώθουν ότι βρίσκουν σ' αυτό το πρόσωπο τον «κολλητό» τους ή έναν ξεχωριστό φίλο, κάποιον που τα καταλαβαίνει, στον οποίο μπορούν να εκμυστηρευτούν τις απορίες, ανησυχίες και προβληματισμούς τους που δεν έχουν την δυνατότητα να πουν στους γονείς τους.

Μέσα από την σχέση αυτή προκαλούν με τον καιρό συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή. Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

Για την αποφυγή και την αντιμετώπιση του grooming, υπάρχουν τρόποι και λύσεις που μπορούν να λάβουν τα παιδιά και οι γονείς:

- Το παιδί πρέπει να κατανοήσει ότι σε χώρους όπως τα chat room δεν μπορεί ποτέ να είναι σίγουρο για την ταυτότητα του άλλου. Επομένως πρέπει να αντιμετωπίζει τις διαδικτυακές γνωριμίες με αρκετή επιφυλακτικότητα, καθώς ακόμη και άτομα που έχουν κερδίσει την εμπιστοσύνη του μπορεί να έχουν σκοπό να το βλάψουν.
- Υπάρχει η δυνατότητα αποθήκευσης των συνομιλιών που πραγματοποιείται στα chat room. Κάτι τέτοιο είναι ιδιαίτερα χρήσιμο σε περίπτωση που θελήσουν να κάνουν μια καταγγελία στις αρχές.
- Δεν είναι ασφαλές να δίνει κάποιος τα προσωπικά του στοιχεία επικοινωνίας σε ένα chat room. Άλλωστε αν κάποιος επιτήδειος γνωρίζει το κινητό τηλέφωνο, τη διεύθυνση κατοικίας και το σχολείο του παιδιού (ακόμη και αν το παιδί αποφασίσει να αποφύγει τη διαδικτυακή επικοινωνία), μπορεί εύκολα να το εντοπίσει στον φυσικό κόσμο.
- Οι γονείς οφείλουν να είναι ενημερωμένοι για τις διαδικτυακές γνωριμίες των παιδιών τους, ώστε όταν παρατηρήσουν κάτι ύποπτο να μπορέσουν να τα συμβουλέψουν αποτελεσματικά.

3.5.5 Κυκλώματα παιδοφιλίας

Ένα κύκλωμα παιδοφιλίας είναι μια ομάδα ανθρώπων που εργάζονται μαζί μέσω Διαδικτύου σε διαφορετικές χώρες και υπό διαφορετικά νομοθετικά πλαίσια, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Μπορεί επίσης να γίνεται και ανταλλαγή εμπειριών και γνώσεων ως προς την αποφυγή ανίχνευσης και το σχεδιασμό εγκληματικών ενεργειών εις βάρος παιδιών.

Υπάρχει μια ισχυρή εντύπωση ότι το Διαδίκτυο έχει γίνει ένας ισχυρός παράγων στην εξέλιξη των παιδοφιλικών κυκλωμάτων παγκοσμίως. Πολλές πρόσφατες καταδίκες στις ΗΠΑ και στο Ηνωμένο Βασίλειο απέδειξαν ότι το Διαδίκτυο

χρησιμοποιείται ευρέως από τα μέλη τέτοιων κυκλωμάτων, τόσο για να την ανταλλαγή εμπειριών όσο και για την διακίνηση φωτογραφιών παιδικής πορνογραφίας. Η διάδοση της παιδικής πορνογραφίας προκαλεί μεγάλη ανησυχία στους διεθνείς φορείς που ασχολούνται με την προστασία των ανηλίκων. Ανεξάρτητα από τους τρόπους που χρησιμοποιούνται για την διακίνηση φωτογραφιών παιδικής πορνογραφίας στο Διαδίκτυο, το πρόβλημα εξακολουθεί να είναι σοβαρό στη δυτική Ευρώπη, όπου αποκαλύφθηκαν σημαντικά κυκλώματα παιδικής πορνογραφίας στη Δανία, την Ισπανία, τη Γερμανία, την Ιταλία, την Ολλανδία, τη Σουηδία και το Ηνωμένο Βασίλειο. Καθώς αυτά τα δίκτυα όλο και συχνότερα χρησιμοποιούν ανεπτυγμένες τεχνολογίες τηλεπικοινωνιών, κάνοντας χρήση κρυπτογράφησης και κωδικών ονομασιών, γίνεται συνεχώς δυσκολότερη η ανακάλυψή τους από τις αρχές.

3.5.6 Ελληνική νομοθεσία[46]

Από τις 24/01/2008 ισχύει ο νέος νόμος για την καταπολέμηση της σεξουαλικής εκμετάλλευσης και της παιδικής πορνογραφίας. Οι ρυθμίσεις του νομοσχεδίου αποβλέπουν, κατά κύριο λόγο, στην προστασία των δικαιωμάτων των ανήλικων θυμάτων του εμπορίου παιδιών, της παιδικής πορνείας και παιδικής πορνογραφίας, επεκτείνονται δε και στην προστασία των δικαιωμάτων των ανήλικων θυμάτων εγκλημάτων κατά της γενετήσιας ζωής και οικονομικής εκμετάλλευσης της γενετήσιας ζωής, λόγω της συγγένειάς τους με αυτά.

Βασικά σημεία του νομοσχεδίου:

- Η παιδική πορνογραφία τιμωρείται και όταν σκοπός του δράστη δεν είναι η αποκόμιση κέρδους, ο οποίος σκοπός, εφόσον βέβαια υφίσταται, ορίσθηκε ως επιβαρυντική περίπτωση.
- Προσδιορίζεται ως τιμωρητέο υλικό παιδικής πορνογραφίας η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή

[46] http://www.ministryofjustice.gr/

άλλο φορέα: α) του σώματος ή μέρους του σώματος ανηλίκου, με τρόπο που καταφανώς προκαλεί γενετήσια διέγερση.

- Για ελαφρότερες προσβολές της γενετήσιας ελευθερίας του θύματος με προτάσεις ή χειρονομίες που αφορούν σε ασελγείς πράξεις από μέρος του δράστη, προβλέπεται ποινή φυλάκισης τουλάχιστον 6 μηνών.
- Θεωρείται αξιόποινη πράξη η παραγωγή, διανομή, δημοσίευση, επίδειξη, εισαγωγή στην Επικράτεια ή εξαγωγή από αυτήν ή η μεταφορά, η προσφορά, η πώληση ή με οποιονδήποτε τρόπο διάθεση, η αγορά, προμήθεια, απόκτηση και κατοχή υλικού παιδικής πορνογραφίας καθώς και η διανομή και μετάδοση πληροφοριών για τις παραπάνω πράξεις.
- Προβλέπεται βαρύτερη τιμωρία για τις πράξεις της παραγωγής, προσφοράς, πώλησης ή με οποιονδήποτε τρόπο διάθεσης, διανομής, διαβίβασης, αγοράς, προμήθειας και κατοχής υλικού παιδικής πορνογραφίας, καθώς και της διανομής πληροφοριών για τις πράξεις αυτές μέσω ηλεκτρονικού υπολογιστή ή του Διαδικτύου.

3.6 Δωμάτια ανοιχτής επικοινωνίας[47]

Τα δωμάτια ανοιχτής επικοινωνίας (chat room) είναι μία από τις πιο συνηθισμένες, αγαπημένες και ελκυστικές δραστηριότητες των παιδιών στο Διαδίκτυο διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους από όλο τον κόσμο. Όμως οι κίνδυνοι που μπορούν να κρύβονται είναι μεγάλοι και δεν είναι εύκολο να αναγνωριστούν και να αποφευχθούν άμεσα.

Τι είναι τα δωμάτια ανοιχτής επικοινωνίας:

Ένα δωμάτιο ανοιχτής επικοινωνίας (chat room) είναι ένας τρόπος άμεσης (συγχρονισμένης) επικοινωνίας σε πραγματικό χρόνο ενός συνόλου ανθρώπων,

[47] http://www.saferinternet.gr/

οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό εικονικό χώρο (chat room) και επικοινωνούν πληκτρολογώντας ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία.

Όπως αποκαλύπτει και η λέξη «συγχρονισμένη», για να κάνει κανείς chat με άλλα άτομα, πρέπει να τα «συναντήσει» την ίδια ώρα σε ένα chat room. Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό, όπως στην περίπτωση του δημοφιλούς IRC, ή των διαφόρων «instant messenger programs» (προγράμματα άμεσων μηνυμάτων) μέσω των οποίων μπορεί κανείς να πληροφορηθεί πότε οι φίλοι του είναι συνδεδεμένοι στο Διαδίκτυο. Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποια από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο χώρο και να επικοινωνούν μόνο μεταξύ τους.

3.6.1 Κίνδυνοι

Η χρήση των ψευδωνύμων στα chat room επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους και να κρύβονται πίσω από αυτή. Η δυνατότητα αυτή, μαζί με την ψευδαίσθηση του παιδιού ότι είναι ασφαλές επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός Internet cafe, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς όσο και από τους εκπαιδευτικούς, είναι ένα από τα σημαντικότερα προβλήματα που επηρεάζουν έμμεσα και τα παιδιά.

3.6.1.1 Παρενόχληση και παιδεραστία στα δωμάτια ανοιχτής επικοινωνίας

Πολλοί επιτήδειοι, εκμεταλλευόμενοι το στοιχείο της ανωνυμίας του Διαδικτύου για να προσεγγίσουν ανήλικα παιδιά, δίνουν ψευδή στοιχεία για την ταυτότητά τους και κυρίως για την ηλικία τους. Ακόμα, μέσα σε ένα chat room ή κατά την ανταλλαγή άμεσων μηνυμάτων μπορεί κάποιος να επιχειρήσει να ενοχλήσει, κοροϊδέψει, προσβάλει, γελοιοποιήσει, ακόμα και να απειλήσει ένα παιδί.

Υπάρχουν συχνά καταγγελίες παιδιών ότι κατά τη διάρκεια τέτοιου είδους συνομιλιών έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Δεκάδες περιπτώσεις σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα, με παιδιά που εξαφανίσθηκαν, τα οποία έπεσαν θύματα παιδόφιλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους με τους οποίους συνομιλούσαν σε δωμάτια επικοινωνίας.

Είναι γεγονός ότι οι παιδεραστές χρησιμοποιούν τις δυνατότητες των chat room και των προγραμμάτων άμεσων μηνυμάτων για να πλησιάσουν τα παιδιά, επιδιώκοντας να τα παρενοχλήσουν ή ακόμη και να παρασύρουν για να τα κακοποιήσουν σε μια προσωπική συνάντηση. Τις περισσότερες φορές οι παιδεραστές χρησιμοποιούν ψεύτικα στοιχεία για να προσεγγίσουν τα υποψήφια θύματά τους (όνομα, ηλικία, ενδιαφέροντα) και ξεγελάνε τα παιδιά ώστε να τα πείσουν να τους δώσουν τη διεύθυνση του σπιτιού τους, το όνομα του σχολείου τους και το τηλέφωνό τους. Στη συνέχεια η συζήτηση κατευθύνεται σε θέματα σεξουαλικού περιεχόμενου και πολλές φορές ο παιδόφιλος στέλνει φωτογραφίες παιδικής πορνογραφίας για να δημιουργήσει στο παιδί την αίσθηση ότι δεν είναι κάτι κακό, αλλά και να το φέρει σε δύσκολη θέση, έτσι ώστε να μην το αναφέρει στους γονείς του. Τέτοιες ενέργειες αποσκοπούν στο να αποδυναμώσουν τα παιδιά και να τα πείσουν να συμμετάσχουν αργότερα σε σεξουαλικές πράξεις.

Αν το παιδί γνωρίσει κάποιο καινούριο πρόσωπο μέσω Διαδικτύου, ενδεχομένως να θελήσει να συναντηθεί και από κοντά με το νέο του φίλο. Ακόμα κι αν αυτή η διαδικτυακή φιλία έχει διατηρηθεί για αρκετό καιρό, είναι σημαντικό να οι γονείς να αντιμετωπίσουν μια ενδεχόμενη συνάντηση με επιφυλακτικότητα. Αν προγραμματιστεί κάποια συνάντηση, είναι απαραίτητο το παιδί να συνοδεύεται από γονέα ή κάποιον έμπιστο ενήλικα και η συνάντηση να γίνει σε δημόσιο χώρο. Καλό είναι οι γονείς και το παιδί να συμφωνήσουν εκ των προτέρων πώς θα αντιμετωπίζουν τις περιπτώσεις συναντήσεων με διαδικτυακές γνωριμίες.

3.6.2 Ασφαλής συνομιλία

Γεννιέται λοιπόν το ερώτημα, αν υπάρχουν τρόποι ασφαλούς συνομιλίας των παιδιών στο Διαδίκτυο και ποιοί είναι οι βασικοί κανόνες που πρέπει να ακολουθήσουν για να επιτευχθεί κάτι τέτοιο.

Πρώτα από όλα, πρέπει γίνει κατανοητό ότι ο διαδικτυακός φίλος των παιδιών στην ουσία είναι ένας απολύτως άγνωστός και μπορεί να απέχει πολύ από αυτό που δηλώνει για ταυτότητα και ιδιότητα. Για το λόγο αυτό, τα παιδιά πρέπει να αποφεύγουν να δίνουν προσωπικές πληροφορίες και λεπτομέρειες για την ζωή τους, στοιχεία και δεδομένα όπως αριθμούς τηλεφώνων, κωδικούς, διευθύνσεις και φωτογραφίες. Να είναι επιφυλακτικά και να μην εμπιστεύονται εύκολα αυτά που τους παρουσιάζουν οι άλλοι χρήστες για πραγματικότητα.

Ιδιαίτερη προσοχή χρειάζεται στην παραλαβή αρχείων, e-mail, ακόμα και ηλεκτρονικές συνδέσμων. Συχνά είναι σκόπιμα μολυσμένα με διαφόρων τύπων ιών, ώστε να συλλέξουν προσωπικά δεδομένα από τον υπολογιστή. Εφόσον το παιδί δεν είναι σίγουρο για την αξιοπιστία των αρχείων που αποδέχεται από τον συνομιλητή του, καλό είναι να απορρίπτει αυτή την ανταλλαγή.

Μεγάλη προσοχή χρειάζεται όταν ένας άγνωστος συνομιλητής προτρέψει το παιδί να συναντηθούν σε φυσικό χώρο, διότι οι προθέσεις του ενδέχεται να είναι διαφορετικές από αυτές που ισχυρίζεται και πραγματικός του σκοπός να είναι η

παραπλάνηση / αποπλάνηση του παιδιού. Οι συναντήσεις αυτές θα πρέπει να αποφεύγονται όπως και η εμπλοκή σε συζητήσεις περί αυτού, εκτός εάν ο γονιός είναι ενημερωμένος, εγκρίνει και επιθυμεί μια τέτοια συνάντηση σε ένα δημόσιο μέρος, συνοδεύοντας το παιδί του. Το βασικότερο που μπορούν να πράξουν τα παιδιά όταν νιώσουν άβολα ή κάποια παρενόχληση από το συνομιλητή τους, είναι να αποθηκεύσουν την συνομιλία τους, να την διακόψουν άμεσα και να κλείσουν το αντίστοιχο πρόγραμμα ή εφαρμογή.

Παιδιά ηλικίας κάτω των 13 ετών είναι αναγκαίο να ζητάνε την άδεια των γονέων τους πριν χρησιμοποιήσουν προγράμματα άμεσων μηνυμάτων όπως το «Windows Live Messenger» και το «Yahoo Messenger», καθώς πρώτα απαιτείται η εγγραφή σε ηλεκτρονικούς λογαριασμούς της αντίστοιχης υπηρεσίας. Ο λογαριασμός αυτός θα πρέπει να συμπληρώνεται με την βοήθεια των γονέων, καθοδηγώντας τα με υπευθυνότητα και ενθάρρυνση για την προστασία του απορρήτου.

Η δυνατότητα αυτή του Διαδικτύου, θα πρέπει να βασίζεται στην επικοινωνία των παιδιών με φίλους τους που βρίσκονται μακριά και τους οποίους τα παιδιά ήδη γνωρίζουν, και όχι ως μέσο νέων γνωριμιών.

Σε γενικές γραμμές, οι γονείς μπορούν να διαπιστώσουν εάν το δωμάτιο συνομιλίας που χρησιμοποιεί το παιδί τους είναι ασφαλές, με βάση τα παρακάτω ερωτήματα:

Αυτό το δωμάτιο συνομιλίας προορίζεται για παιδιά; Στα δωμάτια συνομιλίας που προορίζονται για παιδιά, υπάρχει μικρότερη πιθανότητα να συναντήσει ο χρήστης ανάρμοστα θέματα ή συμπεριφορές.

Είναι το δωμάτιο συνομιλίας εποπτευόμενο;

Μερικές φορές τα δωμάτια συνομιλίας έχουν εθελοντές επόπτες, που διαχειρίζονται τα ακατάλληλα μηνύματα επικοινωνίας και που μπορούν να αποκλείσουν τους «νταήδες» και τους άλλους ταραξίες από το δωμάτιο

συνομιλίας. Εάν η εποπτεία δεν είναι ενεργή, το δωμάτιο συνομιλίας θα πρέπει να περιέχει τουλάχιστον ένα κουμπί για επικοινωνία με το διαχειριστή.

Υπάρχει η δυνατότητα να αποκλείονται κάποιοι χρήστες;

Υπάρχει. Αποκλεισμός σημαίνει να μην επιτρέπεται η δημοσίευση στο δωμάτιο συνομιλίας των μηνυμάτων που προέρχονται από κάποιο συγκεκριμένο πρόσωπο. Αν κάποιο πρόσωπο αποκλειστεί, τα μηνύματά του δεν εμφανίζονται πλέον στην οθόνη.

Η ρίζα της λύσης όμως βρίσκεται στη σωστή επικοινωνία μεταξύ παιδιών και γονέων. Τα παιδιά χρειάζεται να συζητάνε με τους γονείς, να τους μιλάνε για τους διαδικτυακούς τους φίλους και στην περίπτωση που υποστούν οποιουδήποτε είδους παρενόχληση, να τους ενημερώνουν άμεσα.

3.7 Κοινωνική δικτύωση[48]

Ο όρος κοινωνική δικτύωση (social networking) αναφέρεται σε ψηφιακούς χώρους και κοινότητες διαπροσωπικών επαφών. Η «φιλοσοφία» των ιστοσελίδων κοινωνικής δικτύωσης, στηρίζεται στη διασύνδεση μεταξύ των χρηστών και στην από κοινού δημιουργία και συντήρηση του περιεχομένου τους, χωρίς να χρειάζονται εξειδικευμένες τεχνικές γνώσεις.

Πιο συγκεκριμένα, οι χρήστες, δηλώνοντας τα στοιχεία τους, δημιουργούν ένα προσωπικό προφίλ στο οποίο έχουν την αποκλειστική ευθύνη διαχείρισης. Οι υπηρεσίες κοινωνικής δικτύωσης στοχεύουν στη δημιουργία διαδικτυακών κοινοτήτων και στην επικοινωνία μεταξύ ανθρώπων με κοινά ενδιαφέροντα και δραστηριότητες. Μερικά από τα δημοφιλέστερα κοινωνικά δίκτυα στην Ελλάδα είναι το Facebook, το MySpace, και το Hi5.

Οι ιστοσελίδες κοινωνικής δικτύωσης επιτρέπουν στο χρήστη να δημιουργήσει και να σχεδιάσει την προσωπική του ιστοσελίδα, blog ή ημερολόγιο, χρησιμοποιώντας γραφικά, χρώμα, μουσική και εικόνες ώστε να της δώσει

[48] http://archive.enet.gr/online/online_text/c=110,dt=24.08.2008,id=74017000
http://www.dpa.gr/portal/page?_pageid=33,32920&_dad=portal&_schema=PORTAL

ξεχωριστό χαρακτήρα και ταυτότητα. Οι χρήστες μπορούν να δημοσιοποιούν και να μοιράζονται το περιεχόμενο τους, όπως και προσωπικές πληροφορίες με άλλες ομάδες χρηστών σε ένα ευρύ δίκτυο ατόμων, ακόμα και σε παγκόσμιο επίπεδο. Ειδικότερα, σε αυτούς τους ιστοχώρους οι χρήστες ανταλλάσσουν σκέψεις και πληροφορίες σχετικά με τα ενδιαφέροντά τους, τα χόμπι τους, δημοσιεύουν και ανταλλάσουν την μουσική τους, δέχονται σχόλια από φίλους και επισκέπτες, δημοσιεύουν εικόνες και βίντεο δικά τους ή φίλων τους και συνδέονται με τις ιστοσελίδες άλλων χρηστών.

Κάθε χρήστης μπορεί να συνδεθεί με κάποιον άλλο, αν δηλώσει στον ιστότοπο ότι είναι «φίλος» του και με την προϋπόθεση ότι και ο άλλος χρήστης θα αποδεχθεί αυτή τη πρόσκληση. Έτσι, αποκτούν πρόσβαση ο ένας στον προσωπικό χώρο του άλλου. Οι χρήστες μπορούν να επεκτείνουν διαρκώς το δίκτυο των γνωριμιών τους, δημιουργώντας συνδέσεις με φίλους των φίλων τους ή με άλλους ανθρώπους με κοινά ενδιαφέροντα. Σε πολλά κοινωνικά δίκτυα, οι χρήστες μπορούν να επικοινωνήσουν με φίλους τους σε πραγματικό χρόνο, μέσω υπηρεσιών άμεσων μηνυμάτων και μπορούν να γνωρίσουν νέους φίλους, να παίξουν παιχνίδια online, να συμμετάσχουν σε κοινότητες όπου έχουν τη δυνατότητα να συζητήσουν με άλλους και να λάβουν μέρος σε διαγωνισμούς και κουίζ.

3.7.1 Κοινωνική δικτύωση και έφηβοι[49]

Η κοινωνική δικτύωση δεν είναι δημοφιλής μόνο στους μεγάλους χρήστες του Διαδικτύου, αλλά και στους εφήβους, οπού πολλές φορές κατέχει σημαντική θέση στην ζωή τους. Αποτελεί εργαλείο αλληλεπίδρασης με υπάρχοντες φίλους, αλλά και γνωριμίας νέων διαδικτυακών φίλων.

Η πλειονότητα των εφήβων έχει χρησιμοποιήσει τουλάχιστον μια φορά τις σελίδες αυτές με σκοπό την επικοινωνία. Μέσω των εργαλείων που

[49] http://endelexis.blogspot.com/2010/01/blog-post_28.html
http://www.dpa.gr/portal/page?_pageid=33,32920&_dad=portal&_schema=PORTAL
http://www.etpe.gr/files/proceedings/26/1286267686_85.pdf

προσφέρονται, βοηθούν τον έφηβο χρήστη να επικοινωνεί ευκολότερα με τους ανθρώπους του περιβάλλοντός του και παράλληλα να δημιουργεί νέες επαφές.
Όπως αναφέρουν οι ίδιοι, ο λόγος που η κοινωνική δικτύωση είναι τόσο δημοφιλής, οφείλεται στο ότι βρίσκουν αυτή την ασχολία διασκεδαστική. Ειδικότερα οι έφηβοι οι οποίοι βρίσκονται σε μία ευαίσθητη και μεταβατική φάση της ζωής τους, προσελκύονται έντονα από το γεγονός της δυνατότητας να δημιουργήσουν τον προσωπικό τους ιστοχώρο, όπως και από το γεγονός να γνωρίσουν και να επικοινωνήσουν με άλλα άτομα ανεξαρτήτως απόστασης. Ο διαμοιρασμός φωτογραφιών και βίντεο με φίλους και συμμαθητές τους, η ανταλλαγή ιστοριών και σχολίων, δημιουργεί έναν προσωπικό «κόσμο» στον οποίο βρίσκουν την ευκαιρία να πειραματιστούν με την προσωπική τους ταυτότητα, που μόλις έχει αρχίσει να διαμορφώνεται.
Να σημειωθεί ότι η δημιουργία νέων φίλων μπορεί να βοηθήσει στην κοινωνικοποίηση του νέου, παρόλα αυτά είναι επίφοβη. Η φυσική επιθυμία του ανθρώπου να επικοινωνεί, σε συνδυασμό με τις τεχνολογίες διασύνδεσης που προσφέρουν οι ιστοσελίδες κοινωνικής δικτύωσης, ενδέχεται να κάνουν τον χρήστη επιρρεπή στο να χαμηλώνει τον πήχη των κριτηρίων που θέτει στον φυσικό κόσμο, προκειμένου να δημιουργήσει φιλικές σχέσεις με κάποιο άτομο. Αυτό συμβαίνει σε μεγαλύτερο βαθμό στους νέους, οι οποίοι δεν αναλογίζονται τους κινδύνους που ελλοχεύουν. Έτσι, γίνονται ευάλωτοι και εύκολα θύματα από επιτηδείους, οι οποίοι αποσκοπούν στην ικανοποίηση των ιδιοτελών σκοπών τους.(παιδική πορνογραφία, παιδοφιλία, παρενόχληση, κ.λπ.).

Αποτελέσματα από έρευνα που πραγματοποιήθηκε σε 237μαθητές: (116 αγόρια, 121 κορίτσια) **από 4 λύκεια** (3 στη Θεσσαλονίκη, 1 στην Πτολεμαΐδα) **για την χρήση του Facebook.** [50]

Η πρώτη επισήμανση είναι ότι το 96% των μαθητών κάνει χρήση του Διαδικτύου, έχοντας ξεκινήσει, οι περισσότεροι, από την ηλικία των 14 ετών.

[50] http://www.etpe.gr/files/proceedings/26/1286267686_85.pdf

Επιπλέον, προκύπτει ότι όσο μεγαλώνουν τα παιδιά, τόσο αυξάνεται και η συχνότητα σύνδεσής τους. Εξίσου διαδεδομένη είναι η χρήση ιστοχώρων κοινωνικής δικτύωσης, με το 75% των μαθητών του δείγματος που απαντά θετικά στο αντίστοιχο ερώτημα. Σχεδόν όλοι (96% όσων χρησιμοποιούν τέτοιες υπηρεσίες) προτιμούν το Facebook. Δεν είναι ασήμαντο όμως και το ποσοστό των εφήβων που δε χρησιμοποιούν υπηρεσίες κοινωνικής δικτύωσης (25%), δηλώνοντας ότι δεν τους ενδιαφέρει ή ότι θεωρούν πως πρόκειται για χάσιμο χρόνου. Η συντριπτική πλειοψηφία αυτών προέρχεται από οικογένειες μέσου και υψηλού βιοτικού επιπέδου.

Περίπου 4 στα 10 παιδιά συνδέονται σχεδόν καθημερινά στο Facebook, κυρίως μέσω της σύνδεσης που υπάρχει στο σπίτι τους (68%) ή από ένα Internet café (45%). Επιπλέον, συνδέονται από τα σπίτια φίλων τους, το σχολείο τους, ή ακόμα και το κινητό τους τηλέφωνο.

Αξιοσημείωτο είναι το γεγονός ότι περίπου οι μισοί μαθητές (52%) παραδέχονται ότι έχουν αμελήσει σχολικές υποχρεώσεις, για να αφιερώσουν περισσότερο χρόνο στην ενασχόληση με το Facebook. Επιπλέον, περίπου 1 στους 4 (26%) παραδέχεται ότι έχει αμελήσει και την προσωπική του ζωή για τον ίδιο λόγο, προτιμώντας τη διαδικτυακή παρέα από τους πραγματικούς του φίλους.

Πίνακας 3: Λόγοι Χρήσης του Facebook

Λόγοι που χρησιμοποιούν το Facebook	**Ποσοστό %**
Επικοινωνία με φίλους	57.8
Για να κάνω νέους φίλους	42.6
Για τα παιχνίδια	19.4
Είναι μόδα	18.6
Βοηθά στην εξωστρέφεια	16.5
Τρόπος ζωής - απαραίτητο	8.9
Σύναψη ερωτικής σχέσης	7.2

Φαίνεται λοιπόν, ότι οι νέοι προτιμούν περισσότερο το εικονικό περιβάλλον για να «χτίσουν» ευκολότερα γέφυρες επικοινωνίας με τους συνομηλίκους τους, αντί της προσωπικής, άμεσης επαφής.

Από τις υπηρεσίες που προσφέρει το Facebook, κυρίαρχη θέση στις προτιμήσεις των νέων έχει η δημοσίευση φωτογραφιών (προσωπικών ή μαζί με φίλους), με ποσοστό 65%. Άξιο αναφοράς είναι το ποσοστό των εφήβων (18%) που παραδέχεται ότι θέλει να προκαλεί, δημοσιεύοντας τολμηρές φωτογραφίες (π.χ. με μαγιώ), αναδεικνύοντας έτσι την εξωτερική του εμφάνιση. Εξίσου σημαντική υπηρεσία φαίνεται να είναι για τους νέους η δυνατότητα σχολιασμού φωτογραφιών, τόσο δικών τους όσο και φίλων τους, με το 62% αυτών να την αξιοποιούν. Τέλος, υψηλή θέση (60%) κατέχει η δημιουργία νέων φίλων και η διαδικτυακή συνομιλία (chat).

Μελετώντας την κοινωνική συμπεριφορά των μαθητών, παρατηρήθηκε ότι έχουν κατά μέσο όρο 500-600 διαδικτυακούς φίλους. Τα κριτήρια για την επιλογή αυτών είναι κυρίως:

- η ύπαρξη κοινών φίλων (61%)
- η εξωτερική εμφάνιση (40%)
- το φύλο (21%)

Όταν έχουν ένα νέο αίτημα φιλίας, οι μαθητές εξετάζουν αν ο αιτών είναι ήδη χαρακτηρισμένος ως «φίλος» από τους υπόλοιπους φίλους τους, για να τον αποδεχτούν. Συνήθως αυτό είναι αρκετό, ενώ σημαντικά κριτήρια είναι η εξωτερική εμφάνιση και το φύλο του αιτούντος, κυρίως για τα αγόρια. Ένα στα τρία αγόρια επιλέγει τους διαδικτυακούς του φίλους με βάση το φύλο, ενώ το 50% αυτών στηρίζεται κυρίως στην εξωτερική εμφάνιση. Αυτό πιθανόν να οφείλεται στην αφαιρετική ιδιότητα του Διαδικτύου που εξαφανίζει τις πληροφορίες μη λεκτικής επικοινωνίας, οι οποίες παίζουν σημαντικό ρόλο στην κατά πρόσωπο επικοινωνία. Έτσι, απλοποιείται η προσέγγιση, κυρίως με παιδιά του αντίθετου φύλου.

Αντιπαραβάλλοντας τα στοιχεία αυτά με τα δεδομένα της πραγματικής ζωής των νέων, διαπιστώνεται ότι εκεί κατά μέσο όρο έχουν 50 φίλους. Επιπλέον, τα κριτήρια επιλογής φίλων στην πραγματική ζωή διαφέρουν. Τα παιδιά βασίζονται κυρίως στην ύπαρξη κοινών ενδιαφερόντων (58%) και την εκτίμησή τους για το χαρακτήρα του εν δυνάμει φίλου τους (57%). Στην πραγματική ζωή, μόλις το 9% των ερωτηθέντων χρησιμοποιεί το φύλο και η εξωτερική εμφάνιση σαν κριτήριο επιλογής φίλων. Και στην περίπτωση αυτή, μεγαλύτερη χρήση αυτού του κριτηρίου γίνεται από τα αγόρια (15%) , έναντι των κοριτσιών (5%).

Διαφορές ανάμεσα στη διαδικτυακή και την πραγματική ζωή παρατηρούνται και κατά τη διακοπή μιας φιλικής σχέσης. Οι μισοί μαθητές δήλωσαν ότι έχουν διαγράψει κατά μέσο όρο 15 διαδικτυακούς φίλους, λόγω:

- εξύβρισης (40%)
- κάποιου είδους απειλή (34,6%)
- σεξουαλικής παρενόχλησης (38,4%).

Μελετώντας τα δεδομένα, αποκαλύπτεται διαφοροποίηση, ανάλογα με το φύλο του ερωτούμενου. Τα αγόρια δηλώνουν ότι θα προέβαιναν σε διαγραφή διαδικτυακών φίλων κυρίως λόγω εξύβρισης, ενώ τα κορίτσια κυρίως σε περίπτωση εξαπάτησης ή αν δεν είχαν τακτική επαφή και αλληλεπίδραση. Αντίθετα, στην πραγματική ζωή, οι μισοί από τους μαθητές παραδέχονται πως συχνά έρχονται σε αντιπαράθεση με φίλους τους, λόγω διαφορετικών απόψεων και διχογνωμιών, αλλά σχεδόν πάντα συμφιλιώνονται. Αν όμως αποφάσιζαν να διακόψουν τη φιλία τους, αυτό θα γινόταν κυρίως λόγω εξαπάτησης (60%) ή εξύβρισης (28%).

Πίνακας 4: Πιθανοί λόγοι για την υποβολή καταγγελίας στις αρχές

Λόγοι καταγγελίας	**Ποσοστό %**
Απειλή	42.2
Σεξουαλική παρενόχληση	41.4
Εξύβριση	15.2
Κλοπή προσωπικών στοιχείων	6.3
Κακόβουλη χρήση προσωπικών στοιχείων	5.7

Ο δεύτερος άξονας, στον οποίο στηρίχθηκε ο σχεδιασμός της παρούσας έρευνας, ήταν οι κίνδυνοι που διατρέχουν οι νέοι και η ενημέρωση που έχουν γι αυτούς. Η πλειοψηφία των μαθητών (65,4%) επιλέγει να δημοσιεύσει πραγματικά προσωπικά στοιχεία στο Facebook, θεωρώντας ότι πρέπει να είναι ειλικρινείς. Παράλληλα, θεωρούν ότι με τον τρόπο αυτό διευκολύνουν τους φίλους τους να τους εντοπίσουν και να αλληλεπιδράσουν μαζί τους.

Παρά τις διαφορές αυτές, η πλειοψηφία των ερωτηθέντων (60%), θεωρεί ότι τελικά δεν είναι ασφαλείς στους ιστοχώρους κοινωνικής δικτύωσης. Η ανασφάλεια αυτή αποτυπώνεται σε ένα βαθμό και στη ρητή δήλωση του 45% των ερωτηθέντων, ότι είναι αντίθετοι με τη δημιουργία σχέσης με άτομο του αντίθετου φύλου που θα γνώριζαν μέσω του Facebook. Όμως, δεν είναι ασήμαντο το ποσοστό των παιδιών (16,5%), που παραδέχεται ότι έχει συναντηθεί προσωπικά, κατά μέσο όρο, με 15 άτομα που έχει γνωρίσει μέσα από το Facebook. Αυτό είναι σε αντιστοιχία με σχετική έρευνα που διεξήχθη το 2009 από την οργάνωση «N.E.O.I.», με τη συμμετοχή 2176 παιδιών, ηλικίας 13-18 ετών.

Διερευνώντας τους πιθανούς κινδύνους που διατρέχουν οι νέοι, διαπιστώθηκε ότι το 16% του δείγματος είχε κάποια δυσάρεστη εμπειρία κατά την ενασχόλησή του με το Facebook. Πρόκειται κυρίως για περιπτώσεις:

- εξύβρισης και σεξουαλικής παρενόχλησης (10%)
- εξαπάτησης (6%)
- αξιοποίησης πληροφοριών για ευκολότερη προσέγγιση (2,1%)
- απειλής (1,7%)

Ενθαρρυντικό είναι το γεγονός ότι περίπου 1 στα 3 παιδιά του δείγματος δήλωσε ότι διέγραψε πληροφορίες από το προσωπικό του προφίλ στο Facebook, θορυβημένο από περιστατικά που είδε μέσα από τηλεοπτικές εκπομπές ή δελτία ειδήσεων. Ερωτούμενοι αν έχουν απευθυνθεί στις αρχές για οποιαδήποτε καταγγελία αφορά τους ίδιους, όλοι οι μαθητές του δείγματος απάντησαν αρνητικά. Ένα μικρό ποσοστό όμως (5%), δήλωσε πως γνωρίζει άτομα που το έπραξαν, για λόγους όπως: σεξουαλική παρενόχληση, απειλή, κλοπή και κακόβουλη χρήση προσωπικών στοιχείων, εξύβριση και δημιουργία προφίλ εν αγνοία των ιδίων. Στην περίπτωση αυτή, είναι δύσκολο να διακρίνει κανείς αν μέρος του ποσοστού αυτού αφορά τα ίδια τα παιδιά, αλλά δίσταζαν να το παραδεχτούν μέσα από το ερωτηματολόγιο.

Άλλωστε, ερωτώμενα τα παιδιά για το που θα απευθύνονταν αν τους συνέβαινε ένα δυσάρεστο περιστατικό, το 40% απαντά πως θα απευθυνόταν αρχικά στους φίλους τους. Το 25,3% θα απευθύνονταν στους γονείς και μόνο ένα 3,8% στις αρχές. Διακρίνεται δηλαδή ένας δισταγμός στην επαφή με τις αστυνομικές αρχές, ο οποίος μπορεί να οφείλεται σε φόβο, ντροπή ή ακόμα και αμφιβολία για την αποτελεσματικότητα μιας τέτοιας ενέργειας. Αυτό το επιβεβαιώνουν και οι αξιωματικοί του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος Θεσσαλονίκης, υποστηρίζοντας ότι οι νέοι δύσκολα καταφεύγουν στις αρχές, διότι φοβούνται ή ντρέπονται.

Είναι κοινά αποδεκτό, ότι σε ζητήματα όπως οι κίνδυνοι από αξιόποινες ενέργειες τρίτων μέσα από υπηρεσίες κοινωνικής δικτύωσης, είναι σημαντικός ο προληπτικός ρόλος της έγκαιρης και έγκυρης ενημέρωσης. Τα μηνύματα που καταγράφονται προς την κατεύθυνση αυτή, από την παρούσα έρευνα, είναι θετικά. Μεγάλο ποσοστό των μαθητών (46%) πιστεύει ότι είναι σημαντική η ύπαρξη κατάλληλου θεσμικού φορέα για την έγκυρη και συνεχή ενημέρωσή τους για την κοινωνική δικτύωση και τα ζητήματα ασφαλείας που την αφορούν. Αυτό το ρόλο θεωρούν ότι μπορεί να έχει το σχολείο και οι γονείς τους, με ισόποσο ποσοστό (18%). Έπειτα ακολουθούν τα δελτία ειδήσεων (11%) και τέλος το Διαδίκτυο και τα περιοδικά. Τα έντυπα προτιμώνται περισσότερο από 18χρονους μαθητές και λιγότερο από τους νεότερους.

Σε ερώτηση για το ποιον θεωρούν περισσότερο αξιόπιστο φορέα ενημέρωσης, η σειρά παραμένει η ίδια, αλλά τα ποσοστά μεταβάλλονται ελαφρά.

Πίνακας 5: Ποιος θεωρείται πιο αξιόπιστος φορέας ενημέρωσης από τους μαθητές

Φορέας	**Ποσοστό %**
Σχολείο	44.3
Γονείς	29.1
Μ.Μ.Ε.	27.4
Διαδίκτυο	21.5
Έντυπα	21.1
Δεν ενδιαφέρομαι	13.1

Αξιοσημείωτη είναι η διαφοροποίηση στον τρόπο επιλογής φίλων ανάμεσα στην πραγματική και την εικονική ζωή, αλλά και το πλήθος αυτών. Το γεγονός αυτό, δείχνει μια πιο επιπόλαια προσέγγιση των εφήβων στο ζήτημα της έκθεσης των προσωπικών τους δεδομένων και στιγμών σε κοινή θέα. Επίσης, δεν περνά απαρατήρητο το 16% των παιδιών που παραδέχτηκε ότι είχε τουλάχιστον μία δυσάρεστη εμπειρία μέσα από το Facebook.

Σημαντικό συμπέρασμα που προκύπτει, είναι η θετική στάση των εφήβων, για την ύπαρξη θεσμικών μηχανισμών και την έγκυρη ενημέρωσή τους. Θεωρούν

ότι αυτό το ρόλο μπορεί να επιτελέσει το σχολείο και οι γονείς τους, κατά κύριο λόγο. Επιπλέον, είναι εμφανές ότι τα παιδιά δεν έχουν πλήρη επίγνωση των κινδύνων που ελλοχεύουν, από την αβίαστη δημοσιοποίηση προσωπικών τους πληροφοριών.

3.7.1.1 Αποτελέσματα έρευνας: «Παρενόχληση και ασφάλεια προσωπικών δεδομένων σε ιστοσελίδες κοινωνικής δικτύωσης»[51]

Ιδιαίτερο ενδιαφέρον παρουσιάζει η παρουσίαση των αποτελεσμάτων της πανελλαδικής έρευνας που πραγματοποίησε η οργάνωση N.E.O.I. το 2009 με θέμα: «Παρενόχληση και ασφάλεια προσωπικών δεδομένων σε ιστοσελίδες κοινωνικής δικτύωσης». Η έρευνα αναφορικά με τη γνώμη των νέων για το Διαδίκτυο, τις ιστοσελίδες κοινωνικής δικτύωσης και τη σεξουαλική παρενόχληση στο Διαδίκτυο στο σύνολο των 2176 ερωτηθέντων ανέδειξε τα παρακάτω:

- Σχεδόν 9 στους 10 χρησιμοποιούν το Διαδίκτυο κάθε μέρα ενώ μόνο το 3% δεν το χρησιμοποιεί καθόλου.
- Το μεγαλύτερο ποσοστό των ερωτηθέντων χρησιμοποιεί καθημερινά:
  - instant messenger για να επικοινωνούν με φίλους (46,3%)
  - ιστοσελίδες κοινωνικής δικτύωσης (46,4%)
  - ιστοσελίδες που αφορούν μουσική (43,8%)
  - ανταλλαγή αρχείων (31,9%)
  - ειδήσεις (79,1%)
- Σχεδόν 6 στους 10 μπαίνουν στο Διαδίκτυο από το σπίτι, 2 στους 10 ερωτηθέντες δηλώνουν το σημείο πρόσβασης είναι από το χώρο της εργασίας τους και το κινητό τους τηλέφωνο, ενώ λιγότερο από το 10% μπαίνουν από το σχολείο, Internet cafe ή αλλού.

[51] http://www.ditiki.gr/index.php/Απόψεις/Διαδίκτυο-Νέοι.html

- από το 56% που μπαίνει στο Διαδίκτυο από το σπίτι μόνο το 43% έχει τον υπολογιστή του στο σαλόνι, ενώ το 36% έχει τον υπολογιστή του στο υπνοδωμάτιο.
- Το μεγαλύτερο ποσοστό επικοινωνεί με τους φίλους του:
  - από κινητό (20,9%)
  - με e-mail (14%)
  - με SMS (11,1%)
  - με instant messenger (18%)
- Σχεδόν το 26% έχει παρενοχληθεί διαδικτυακά, γεγονός που ανέφεραν κυρίως σε φίλους γιατί το θεώρησαν αστείο και λιγότερο σε γονείς, λόγω του ότι ένιωσαν φοβισμένοι και προσβεβλημένοι.
- Κανένας από τους ερωτηθέντες δεν ανέφερε ότι απευθύνθηκε στις αρμόδιες αρχές όπως η Δίωξη Ηλεκτρονικού Εγκλήματος.
- Το 34% των ερωτηθέντων έχει συναντήσει από κοντά κάποιον που γνώρισε στο Διαδίκτυο και από το παραπάνω ποσοστό το ίδιο ποσοστό (34%) έχει πάει μόνο του χωρίς έστω κάποιο φίλο, είτε γιατί θεωρούσε ότι είχε αναπτύξει φιλική σχέση με το συγκεκριμένο άτομο και ένιωθε ασφάλεια, είτε γιατί είχε ενημερώσει τους φίλους του για τη συγκεκριμένη συνάντηση, είτε γιατί είχαν γνωριστεί με βιντεοκλήση και θεώρησε ότι δεν υπάρχει κανένας κίνδυνος.
- Μεγάλο ποσοστό των ερωτηθέντων έχει δώσει προσωπικά του στοιχεία στο Διαδίκτυο, όπως ηλικία (27,9%), ονοματεπώνυμο και κινητό (20% αντίστοιχα), ενώ διεύθυνση και τηλέφωνο σπιτιού έδωσαν το 6,4% και 8,6% αντίστοιχα.
- Όσον αφορά τα θετικά στοιχεία της χρήσης του Διαδικτύου, το 90% δηλώνει ότι χρησιμοποιεί το Διαδίκτυο για ενημέρωση, το 55% για επικοινωνία και το 21% για διασκέδαση ενώ στον αντίποδα ως αρνητικά του στοιχεία το 95% θεωρεί ότι είναι η παραπλάνηση, το 89% ο εθισμός,

το 71% η παραπληροφόρηση και το 59% η έλλειψη επικοινωνίας πράγμα το οποίο έρχεται σε αντίθεση με τα παραπάνω αποτελέσματα.

- Το γενικότερο συμπέρασμα της έρευνας υποδηλώνει ότι οι νέοι επιλέγουν να δείχνουν ριψοκίνδυνες συμπεριφορές αναφορικά με την πλοήγησή τους στο Διαδίκτυο (διάθεση προσωπικών δεδομένων, συναντήσεις με άτομα που γνωρίζουν μέσω του Διαδικτύου κ.α.) γνωρίζοντας παράλληλα ότι ελλοχεύουν κίνδυνοι.

3.7.2 Διαμόρφωση του χαρακτήρα[52]

Δεν είναι λοιπόν παράξενο ότι, όταν τόσοι πολλοί νέοι χρησιμοποιούν τις ιστοσελίδες κοινωνικής δικτύωσης, κάποιες φορές δημιουργούνται σοβαρά προβλήματα. Ακραίες περιπτώσεις έχουν εμφανιστεί κατά καιρούς σε τέτοιου είδους ιστότοπους, όπως διακίνηση ναρκωτικών από έφηβους, θύματα έντονης παρενόχλησης, ακόμα και δημιουργία ομάδων οι οποίες σχεδιάζουν και προωθούν μαζικές αυτοκτονίες.

Αλλά ακόμα και αν υπάρχει η δυνατότητα προστασίας των νέων από τα άτομα που τους παρενοχλούν, υπάρχει ένα άλλο μείζον θέμα που θα πρέπει να απασχολήσει τους ενήλικες: πώς μπορεί να επιδράσει στη διαμόρφωση του χαρακτήρα ενός νέου ατόμου, η «ζωή» μέσα σε έναν εικονικό κόσμο κοινωνικής δικτύωσης.

Μέσα στους εικονικούς κόσμους η συμμετοχή σε ιστοχώρους κοινωνικής δικτύωσης μπορεί να εξελιχθεί σε έναν γιγαντιαίο διαγωνισμό δημοτικότητας, που δεν αντιστοιχεί στην αλήθεια. Καθώς μιλάμε για εικονικούς κόσμους, δεν διασφαλίζεται η αξιοπιστία του προφίλ και των λεγομένων των χρηστών. Ο καθένας μπορεί να δηλώσει οποιαδήποτε ηλικία εξυπηρετεί τους σκοπούς του και να γράψει φανταστικές ιστορίες, για να ανεβάσει την δημοτικότητά του.

Ορισμένοι χρήστες των ιστοχώρων αυτών, τείνουν να ζουν στον προσωπικό τους μικρόκοσμο και η υπερβολική χρήση μπορεί αλλοιώσει την συμπεριφορά

[52] http://www.saferinternet.gr/

τους στον πραγματικό κόσμο, ανάμεσα στους φίλους και την οικογένειά τους. Παράλληλα, παραμελείται η σωστή γραφή και χρήση της γλώσσας λόγω της χρήσης συντομογραφιών και ξενικών όρων. Για αυτό τον λόγο, είναι πολύ σημαντικό να προωθείται η φυσική επικοινωνία, τόσο μέσα στον οικογενειακό χώρο όσο και εκτός αυτού.

Για ορισμένα άτομα οι ιστοχώροι αυτοί μπορούν να αποτελέσουν ένα αληθινό εμπόδιο στην γνήσια επικοινωνία με τον φυσικό κόσμο. Όλοι αυτοί που ψάχνουν τους νέους τους φίλους μέσα από τους ιστοχώρους κοινωνικής δικτύωσης και παραμελούν τους αληθινούς τους φίλους, μπορεί τελικά να ξεχάσουν την πολύτιμη εμπειρία της γνήσιας, χειροπιαστής φιλίας και της προσωπικής επικοινωνίας. Όπως είναι φυσικό, η ηλεκτρονική επικοινωνία, όσα τεχνικά μέσα και αν έχει στη διάθεσή της (εικόνα, ήχο, βίντεο, κείμενο), δεν μπορεί σε καμία περίπτωση να αποδώσει τον πλούτο των συναισθημάτων της διαπροσωπικής επαφής.

Βλέποντας αυτές τις πλατφόρμες από την πλευρά της ασφάλειας, δεν υπάρχει κάποια διαφοροποίηση σε σχέση με τα βασικά θέματα γύρω από τους πιθανούς κινδύνους. Ως υπεύθυνοι σε θέματα ενημέρωσης γύρω από την ασφαλή χρήση των νέων ψηφιακών, διαδραστικών μέσων, πρέπει να προωθηθούν οι ικανότητες των νέων να προστατεύουν την ιδιωτική τους ζωή, να χειρίζονται σωστά θέματα παρενόχλησης, πνευματικών δικαιωμάτων, επιβλαβούς υλικού και να κάνουν με ηθική και με μέτρο, χρήση των μέσων αυτών.

Ταυτόχρονα όμως, οι υπηρεσίες αυτές προσδίδουν και μια καινούργια διάσταση στην έννοια του «προσωπικού χώρου», δημιουργώντας σοβαρές ανησυχίες για παραβίαση της ιδιωτικότητας των χρηστών τους, των οποίων τα προσωπικά δεδομένα δημοσιοποιούνται στο Διαδίκτυο με πρωτοφανή τρόπο και ποσότητα.

Ένα ισχυρό παράδειγμα είναι αυτό του Facebook, όπου έχει υπολογισθεί ότι κάθε μέρα ανεβαίνουν από τους χρήστες, περίπου 25 εκατομμύρια φωτογραφίες.

3.7.3 Ζητήματα ασφάλειας[53]

Όπως ισχύει σε κάθε μορφή ηλεκτρονικής επικοινωνίας, έτσι και στους ιστοχώρους κοινωνικής δικτύωσης, η γνώση θεμελιωδών κανόνων ασφάλειας και η ανάπτυξη κριτικής σκέψης είναι καθοριστικοί παράγοντες στην προστασία από κακόβουλους χρήστες, απατεώνες ή ακόμα και από ασυνείδητους επιχειρηματίες, ώστε καταστεί εφικτή η απόλαυση των δυνατοτήτων ψυχαγωγίας, επικοινωνίας και διασκέδασης που παρέχονται.

Όπως εύστοχα αναφέρει ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), οι ιστοσελίδες κοινωνικής δικτύωσης είναι σαν ένα ψηφιακό κοκτέιλ πάρτι. Όσους περισσότερους γνωστούς έχει κάποιος, τόσο πιο δημοφιλής είναι και τόσο μεγαλύτερη επιρροή ασκεί. Ωστόσο σε αντίθεση με ένα πραγματικό πάρτι, τα μέλη των ιστοσελίδων κοινωνικής δικτύωσης αποκαλύπτουν περισσότερες πληροφορίες, είτε από επιλογή τους, είτε κατά λάθος, στους άλλους χρήστες.

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών εξέδωσε αναφορά, στην οποία παραθέτει τα βασικότερα σημεία που θα πρέπει να προσέξουν οι χρήστες των ιστοσελίδων κοινωνικής δικτύωσης και παράλληλα, προτείνει πολιτικές που πρέπει να ακολουθηθούν από τους αρμόδιους φορείς για την αντιμετώπισή τους. Τα σημαντικότερα από αυτά είναι:

Ψηφιακοί φάκελοι προσωπικών δεδομένων: Τα ηλεκτρονικά προφίλ στις ιστοσελίδες κοινωνικής δικτύωσης μπορούν να αποθηκευτούν από τρίτους και να αποτελέσουν μέρος ψηφιακών φακέλων προσωπικών δεδομένων. Μάλιστα, κάποιες προσωπικές πληροφορίες μπορούν να συλλεχθούν μέσω μιας απλής αναζήτησης, εκτός και αν οι χρήστες αλλάξουν τις προεπιλεγμένες ρυθμίσεις ασφάλειας στο προφίλ τους.

[53] http://www.saferinternet.gr/

Δευτερεύοντα δεδομένα: Εκτός των πληροφοριών τις οποίες οι χρήστες αναρτούν με τη θέλησή τους, τα μέλη τέτοιου είδους ιστοσελίδων αποκαλύπτουν αυτόματα δευτερεύοντα στοιχεία, τα οποία αφορούν τον τρόπο που χρησιμοποιούν τις προσφερόμενες υπηρεσίες: π.χ. τη χρονική διάρκεια μιας επικοινωνίας, τις επισκέψεις σε προφίλ άλλων χρηστών και τα μηνύματα που έχουν αποσταλεί μέσω του δικτύου. Στις πολιτικές απορρήτου γνωστών ιστοσελίδων κοινωνικής δικτύωσης που επισκέφθηκε ο Ελληνικός Κόμβος Ασφαλούς Διαδικτύου, παρατηρείται ότι δεν διευκρινίζεται επαρκώς ποιος μπορεί να έχει πρόσβαση στα δεδομένα αυτά και δεν είναι σαφώς καθορισμένο τι αποτελεί προσωπικό δεδομένο και τι όχι. Τα δεδομένα αυτά είναι πολύ πιθανό να χρησιμοποιηθούν για την απόκτηση οικονομικού οφέλους από την μεταπώλησή τους σε τρίτους.

Αναγνώριση προσώπου: Οι φωτογραφίες που χρησιμοποιούνται στα εικονικά προφίλ αποτελούν μια ψηφιακή ταυτότητα του εκάστοτε χρήστη. Μέσω των προηγμένων τεχνολογιών αναγνώρισης προσώπου (face recognition) μπορούν αυτές οι φωτογραφίες να συνδεθούν με πληροφορίες από άλλους ιστοχώρους και υπηρεσίες, όπου ο ίδιος χρήστης έχει δημοσιεύσει άλλα στοιχεία του, οδηγώντας τελικά στην συλλογή πολύ περισσότερων προσωπικών δεδομένων για τον χρήστη, από ότι ο ίδιος είχε στο μυαλό του να αποκαλύψει μέσα από την κοινωνική δικτύωση.

Εντοπισμός στο φυσικό κόσμο: Μέσω νέων τεχνολογικών επιτευγμάτων, από τις φωτογραφίες που δημοσιεύονται είναι δυνατή η άντληση δεδομένων που παραπέμπουν στον εντοπισμό του χρήστη στον πραγματικό κόσμο (όπως για παράδειγμα μια φωτογραφία μπροστά από το σπίτι του). Οι χρήστες δεν αντιλαμβάνονται συχνά πόσο σημαντικό είναι να μη δημοσιεύουν φωτογραφίες όπου η τοποθεσία γίνεται εύκολα αντιληπτή.

Μεταδεδομένα: Πολλές πλατφόρμες κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες τους να μαρκάρουν με μεταδεδομένα (metadata) τις φωτογραφίες τους. Τα μεταδεδομένα μπορούν να είναι σύνδεσμοι σε προφίλ ή

διευθύνσεις e-mail. Αυτό ενέχει κινδύνους για ανεπιθύμητη διασύνδεση των φωτογραφιών με προσωπικά δεδομένα. Ακόμα και αν οι χρήστες τηρούν τα μέτρα ασφάλειας σε ότι αφορά τις προσωπικές τους φωτογραφίες, οι ιστοσελίδες κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες τους να μαρκάρουν τις φωτογραφίες άλλων χρηστών, μάλιστα όχι πάντα με την συναίνεσή τους.

Αδυναμία πλήρους διαγραφής του προφίλ: Οι χρήστες που επιθυμούν να διαγράψουν το λογαριασμό τους από μια ιστοσελίδα κοινωνικής δικτύωσης δεν μπορούν να διαγράψουν τις δευτερεύουσες πληροφορίες που συνδέονται με το προφίλ τους, όπως τα δημόσια σχόλια.

Social networking spam: Είναι ένα πολύ διαδεδομένο φαινόμενο. Ανεπιθύμητα μηνύματα προωθούνται στους χρήστες μέσω των εφαρμογών που προσφέρονται στις ιστοσελίδες κοινωνικής δικτύωσης. Για παράδειγμα, υπάρχουν μηχανισμοί που αποστέλλουν μαζικά στους χρήστες αίτημα για να τους εντάξουν στους «φίλους» τους, ώστε να έχουν δικαίωμα ανάρτησης σχολίων στο προφίλ τους. Τα σχόλια αυτά συχνά έχουν διαφημιστικό περιεχόμενο ή αποτελούν συνδέσμους προς ιστοσελίδες με πορνογραφικό περιεχόμενο.

Social networking phishing: Η ύπαρξη προσωπικών προφίλ και εικονικών «φιλικών κύκλων» που δεν έχουν περιορίσει την πρόσβαση τρίτων και είναι πολύ εύκολα προσβάσιμα στους ιστοχώρους κοινωνικής δικτύωσης, ευνοεί την άντληση πολλών έγκυρων προσωπικών δεδομένων και πληροφοριών από επιτήδειους οι οποίοι τα χρησιμοποιούν για εξειδικευμένη επίθεση phishing. Η επιτυχία της μεθόδου είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες, το 70% όσων έλαβαν εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιέχονταν σε αυτό και συμπλήρωσε τα στοιχεία του σε εικονική ιστοσελίδα.

Παρενόχληση: Οι επιτήδειοι έχουν τη δυνατότητα να επικοινωνούν επανειλημμένα με τα εν δυνάμει θύματά τους με τα ηλεκτρονικά μέσα που τους προσφέρονται μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης. Πολλές από τις

εφαρμογές που φιλοξενούν αυτές οι πλατφόρμες ενδέχεται να διευκολύνουν περιστατικά παρενόχλησης. Η απειλή της κλοπής ταυτότητας είναι επίσης ιδιαίτερα σημαντική: ψεύτικα προφίλ δημιουργούνται με σκοπό την προσβολή και τον εξευτελισμό άλλων ατόμων. Ακόμη, δημιουργούνται προφίλ που χρησιμοποιούν ονόματα γνωστών εταιρειών ή προσωπικοτήτων με σκοπό την απόκτηση κέρδους από την εκμετάλλευση της φήμης τους.

Κακόβουλο Λογισμικό: Οι ιστοσελίδες κοινωνικής δικτύωσης περιλαμβάνουν μικρές εφαρμογές «widgets», οι δημιουργοί των οποίων δεν έχουν πάντα επαρκείς πιστοποιήσεις. Σε τέτοια περίπτωση, αυτές οι εφαρμογές ενδέχεται να περιέχουν κακόβουλο λογισμικό.

3.7.3.1 Facebook places[54]

Το Facebook είναι ένας από τους πιο δημοφιλής ιστοχώρους κοινωνικής δικτύωσης το οποίο πρωτοεμφανίστηκε το 2004 και το καλοκαίρι του 2010 ξεπέρασε τους 500.000.000 χρήστες. Σύμφωνα με τις ιστοσελίδες www.facebakers.com και www.checkfacebook.com οι οποίες μελετάνε τα στατιστικά χρήσης του Facebook, στην Ελλάδα οι χρήστες φτάνουν τους 2.898.180 (Σεπτέμβριος 2010).

Το Facebook places είναι μια εφαρμογή την οποία ανακοίνωσε η δημοφιλής ιστοσελίδα κοινωνικής δικτύωσης (Σεπτέμβριος 2010), η οποία επιτρέπει στον χρήστη να δηλώνει το γεωγραφικό σημείο στο οποίο βρίσκεται ανά πάσα στιγμή, όπως και το να μοιράζεται σχόλια και αξιολογήσεις. Για τη χρήση της εφαρμογής χρειάζεται η κατοχή ενός έξυπνου τηλεφώνου (smart phone). Σε πρώτη φάση η υπηρεσία είναι ήδη έτοιμη για το iPhone, ενώ πολύ σύντομα αναμένεται να ανακοινωθούν οι αντίστοιχες για τα κινητά με λειτουργικό σύστημα Android αλλά και τις συσκευές Blackberry.

[54] http://www.deasy.gr/fresh-fish/1094,Facebook+places.html
http://www.imerisia.gr/article.asp?catid=14049&subid=2&pubid=52281147
http://news.kathimerini.gr/4dcgi/_w_articles_world_1_29/08/2010_413088

Η συγκεκριμένη εφαρμογή γεννά νέα προβλήματα και ερωτήματα για την ασφάλεια των προσωπικών δεδομένων. Το να γνωρίζουν κάποιοι άλλοι άνθρωποι πού βρίσκεται ο χρήστης, σημαίνει ότι ξέρουν και πού δεν βρίσκεται. Το πιο προβληματικό σημείο της λειτουργίας της, είναι ότι κάποιος που τη χρησιμοποιεί για να δηλώσει πού βρίσκεται, μπορεί να ενημερώσει και ποιοι άλλοι είναι μαζί του.

Τα διευθυντικά στελέχη του Facebook, αναφέρουν ότι τα προσωπικά δεδομένα και σε αυτή την εφαρμογή προστατεύονται, καθώς ο κάθε χρήστης είναι ελεύθερος να επιλέξει αν θα χρησιμοποιήσει την εφαρμογή ή όχι και σε περίπτωση που τη χρησιμοποιήσει, μπορεί να επιλέξει εάν η τοποθεσία στην οποία βρίσκεται θα γνωστοποιηθεί σε ολόκληρο το Διαδίκτυο, μόνο στους φίλους του ή και στους φίλους των φίλων του.

Η αναγγελία του Facebook places, έγινε δεκτή με έντονες επιφυλάξεις από πολλές μη κυβερνητικές οργανώσεις και ιδρύματα, τα οποία θεωρούν πως έτσι ο διαδικτυακός «Μεγάλος Αδελφός» γίνεται ακόμη μεγαλύτερος. Πάντως, ακόμη κι αν κανείς δεχθεί να παραχωρήσει σε μια ιδιωτική εταιρεία τόσο ευαίσθητα προσωπικά δεδομένα , όπως το πού συχνάζει ή ποιο κατάστημα επιλέγει για τις αγορές του, προειδοποιούν πως θα πρέπει να είναι ιδιαίτερα προσεκτικός σε ποιους από τα άλλα τα μέλη του δικτύου τα αποκαλύπτει, έχοντας πάντα κατά νου πως οι συγκεκριμένες πληροφορίες μπορούν κάλλιστα να διοχετευθούν και εκτός του γκρουπ των «φίλων» του. Επίσης, η Ένωση Πολιτικών Ελευθεριών των ΗΠΑ (ACLU), επισημαίνει πως το Facebook places παρουσιάζει κενά ασφαλείας, όπως π.χ. το γεγονός ότι, όταν ένας χρήστης κάνει «check-in» σε κάποιο κατάστημα, μπορεί να επιλέξει είτε να παραμείνει εντελώς «αόρατος» είτε να είναι «ορατός» σε όλα ανεξαιρέτως τα μέλη του Facebook που βρίσκονται στον ίδιο χώρο.

Οι υπεύθυνοι του Facebook από την πλευρά τους, απαντούν πως οι ρυθμίσεις που προβλέπει η εφαρμογή, παρέχουν προστασία στα μέλη σε κάθε περίπτωση. Για παράδειγμα, ακόμη κι αν κανείς μετανιώσει που επέτρεψε σε κάποιον φίλο

του να ενημερώσει την προσωπική του ιστοσελίδα για το ότι βρίσκονται μαζί, μπορεί οποιαδήποτε στιγμή να διαγράψει τη σχετική είδηση. Εξάλλου, συμπληρώνουν, το Facebook places ενεργοποιείται μόνο αν το επιλέξει ο ίδιος ο χρήστης.

3.7.4 Πολιτικές προστασίας[55]

Στις 9/2/2010 η Ευρωπαϊκή Επιτροπή χαιρέτησε τα μέτρα προστασίας των παιδιών που είναι χρήστες ιστοτόπων κοινωνικής δικτύωσης, τα οποία έλαβαν οι 20 εταιρίες που υπέγραψαν το 2009 για ασφαλέστερη κοινωνική δικτύωση. Οι περισσότερες από τις εταιρίες αυτές, έδωσαν στους ανήλικους χρήστες τη δυνατότητα να αντιμετωπίσουν τους διαδικτυακούς κινδύνους, καθώς διευκόλυναν την αλλαγή των προσωπικών ρυθμίσεων, τον αποκλεισμό χρηστών ή τη διαγραφή ανεπιθύμητων σχολίων και περιεχομένου. Κατά την άποψη της Επιτροπής όμως, χρειάζονται περισσότερες προσπάθειες για την προστασία των παιδιών στο Διαδίκτυο. Λιγότερες από τις μισές εταιρείες κοινωνικής δικτύωσης (40%) έχουν φροντίσει ώστε το προφίλ των χρηστών ηλικίας κάτω των 18 ετών να είναι προσβάσιμο μόνο από τους προεπιλεγμένους φίλους τους, ενώ μόνο το ένα τρίτο των εταιριών αυτών απάντησαν σε αναφορές χρηστών που ζητούσαν βοήθεια.

Την ημέρα ασφαλέστερης χρήσης του Διαδικτύου του 2009, οι εταιρείες κοινωνικής δικτύωσης αναγνώρισαν ότι οι νεαροί χρήστες, καθώς και οι γονείς τους, χρειάζεται να αισθάνονται ασφάλεια κατά την κοινωνική διαδικτυακή συναναστροφή και συνυπέγραψαν τις αρχές για ασφαλέστερη κοινωνική δικτύωση. Οι αρχές αυτές προέκυψαν από τις συζητήσεις που δρομολόγησε η Ευρωπαϊκή Επιτροπή τον Απρίλιο του 2008 με ιστοτόπους κοινωνικής δικτύωσης και ερευνητές. Τον Φεβρουάριο του 2009 υπέγραψαν τις αρχές για ασφαλέστερη κοινωνική δικτύωση 18 εταιρίες, στις οποίες προστέθηκαν άλλες δύο τον Ιούνιο του 2009.

[55] http://saferinternet.gr/index.php?parentobjId=Page75&p=10

Ένα έτος αργότερα, η Επιτροπή δημοσίευσε έκθεση σχετικά με την εφαρμογή των αρχών στους 25 ιστοτόπους τους οποίους διαχειρίζονται οι εταιρείες που τις υπέγραψαν – Arto, Bebo, Dailymotion, Facebook, Giovani.it, YouTube, Hyves, Windows Live, Xboxlive, Myspace, Nasza-klaza.pl, Netlog, One.lt, Piczo, Rate.ee, Skyrock, SchülerVZ StudiVZ MeinVZ, Habbo, IRC Galleria, Tuenti, Yahoo!Answers, Flickr και Zap.lu.

Διαπιστώθηκε ότι 19 από 23 ιστοτόπους[56] παρέχουν συμβουλές για την ασφάλεια και πληροφορίες που απευθύνονται ειδικά στα παιδιά ή/και στους εφήβους (αυτό δεν ισχύει για 2 υπηρεσίες). Αυτές οι πληροφορίες είναι ευπρόσιτες και εύκολα κατανοητές σε 14 ιστοτόπους: YouTube, Habbo Hotel, Hyves, IRC Galleria, MySpace, nasza-klasa, Netlog, One, Rate, SchülerVZ, Skyrock, Yahoo!Answers, Yahoo!Flickr, Zap.

Από την έκθεση προκύπτει επίσης ότι οι περισσότερες εταιρίες παρέχουν στους ανήλικους χρήστες τη δυνατότητα να αντιμετωπίζουν ενδεχόμενους διαδικτυακούς κινδύνους και υιοθετούν ασφαλή προσέγγιση όσον αφορά την ιδιωτικότητα:

- Διευκολύνοντας τους χρήστες στον αποκλεισμό άλλων χρηστών και στην αφαίρεση σχολίων από το προφίλ τους.
- Διευκολύνοντας τη ρύθμιση των σχετικών με την ιδιωτικότητα επιλογών, ώστε να μπορούν να επιλέξουν οι χρήστες εάν στο περιεχόμενο που αναρτούν στο Διαδίκτυο θα έχουν πρόσβαση μόνον οι φίλοι τους ή οι πάντες.
- Παρέχοντας στους χρήστες τη δυνατότητα να ελέγχουν την απεικόνιση της διαδικτυακής τους κατάστασης (δηλαδή να επιτρέπουν ή όχι στους άλλους χρήστες να βλέπουν πότε είναι συνδεδεμένοι στο Διαδίκτυο).

[56] Ο αριθμός των ιστότοπων κάθε αναφοράς επί συνόλου 25 διαφοροποιείται ανάλογα με τον αριθμό αυτών που έδιναν τη δυνατότητα αξιολόγησης της αντίστοιχης λειτουργίας ασφάλειας.

Ωστόσο, άλλα εξίσου σημαντικά μέτρα προστασίας της ιδιωτικότητας εφαρμόστηκαν λιγότερο συστηματικά:

- Μόνο στο 40% των ιστοτόπων κοινωνικής δικτύωσης, τα προσωπικά στοιχεία των ανηλίκων είναι προσβάσιμα μόνο από τους προεπιλεγμένους φίλους τους, και συγκεκριμένα στους: SchülerVZ, Facebook, Tuenti, Giovani, Flickr, Yahoo Answers, One, Habbo, Windows Live και MySpace·
- Μόνο σε 11 από 22 ιστοτόπους είναι αδύνατη η ανεύρεση, μέσω μηχανής αναζήτησης, του ιδιωτικού προφίλ ανηλίκων. Πρόκειται για τους: Arto, Bebo, Facebook, YouTube, MySpace, Piczo, SchülerVZ, Windows Live, Yahoo! Answers, Yahoo!Flickr και Zap·
- Ενώ 19 ιστότοποι, επί συνόλου 25, περιλαμβάνουν σύνδεσμο για αναφορές, προσβάσιμο ανά πάσα στιγμή, μόνο 9 (από 22) απάντησαν σε καταγγελίες που υποβλήθηκαν κατά την αξιολόγηση, συγκεκριμένα οι: Arto, Dailymotion, YouTube, Habbo Hotel, Hyves, IRC Galleria, MySpace, Rate, Windows Live. Χρειάζεται, επομένως, επειγόντως βελτίωση των υπηρεσιών απάντησης στις αναφορές των χρηστών που ζητούν βοήθεια.

3.8 Κινητά τηλέφωνα[57]

Σήμερα στον κόσμο υπάρχουν περισσότεροι από 3 δισεκατομμύρια συνδρομητές κινητής τηλεφωνίας. Μέσα σε περίπου 2 δεκαετίες, τα κινητά τηλέφωνα κατάφεραν να φτάσουν σε επίπεδα διείσδυσης, που σε πολλές χώρες ξεπερνούν αυτά που έχει πετύχει η σταθερή τηλεφωνία, σε πάνω από εκατό χρόνια λειτουργίας. Το κινητό τηλέφωνο αναδεικνύεται σε παιδιά και νέους ως η πιο δημοφιλής από τις νέες τεχνολογίες.

[57] «Παιδί & INTERNET», 09/09/2009
http://www.saferinternet.gr/
http://www.chatdanger.com/mobiles/
www.ekato.org

Τα κινητά έχουν πάψει πλέον να είναι απλά τηλέφωνα. Τώρα πια ό,τι μπορεί να κάνει κανείς μέσω ενός υπολογιστή συνδεδεμένου με το Διαδίκτυο μπορεί να κάνει και μέσω ενός κινητού με δυνατότητα σύνδεσης στο Διαδίκτυο. Τα τελευταία μοντέλα και ειδικά τα τηλέφωνα 3ης γενιάς, προσφέρουν πρόσβαση σε πληθώρα ηλεκτρονικών και ψυχαγωγικών υπηρεσιών, ανάμεσα στις οποίες λήψη φωτογραφιών και βίντεο, ραδιόφωνο και μουσική, παιχνίδια, πλοήγηση στο Διαδίκτυο και εφαρμογές όπως SMS, MMS, μηνύματα video, chat, υπηρεσίες γνωριμιών και άλλες υπηρεσίες ενηλίκων.

Καθώς το κινητό τηλέφωνο είναι ένα προσωπικό εργαλείο, ο γονικός έλεγχος του παιδιού σε σχέση με τη χρήση του κινητού του δεν είναι τόσο απλός. Μάλιστα, το κινητό τηλέφωνο έχει γίνει κοινωνικό status για πολλά παιδιά, μέχρι που να μην μπορούν χωρίς αυτό ούτε στιγμή. Ήδη το 2007, 9 στα 10 Ελληνόπουλα ηλικίας 12 έως 15 ετών είχαν στην κατοχή τους κινητό τηλέφωνο και μάλιστα το 91,7% αυτών έκανε καθημερινή χρήση.

Τα προβλήματα που μπορεί να προκύψουν είναι αρκετά σοβαρά. Η ενδεχόμενη ανεξέλεγκτη πρόσβαση σε ακατάλληλο υλικό, ή παρενόχληση του παιδιού από κακόβουλους ή παιδόφιλους, η αλόγιστη χρήση του τηλεφώνου από το παιδί, η κλοπή του κινητού και χρήση των προσωπικών δεδομένων που είναι αποθηκευμένα στη μνήμη του ή η ακούσια έκθεση σε διαφημιστικό υλικό χωρίς το παιδί να είναι σε θέση να αντιδράσει, είναι τα κυριότερα από τα προβλήματα αυτά. Κατά συνέπεια θα πρέπει να ληφθούν τα ίδια μέτρα προστασίας που εφαρμόζονται και κατά την πλοήγησή στο Διαδίκτυο μέσω ενός ηλεκτρονικού υπολογιστή.

3.8.1 Παρενόχληση μέσω κινητού τηλεφώνου

Η παρενόχληση μέσω κινητού γίνεται μέσω της αποστολής προσβλητικού και ακατάλληλου υλικού με γραπτά μηνύματα (SMS) και μηνύματα πολυμέσων (MMS). Το υλικό αυτό μπορεί να είναι είτε ένα ρατσιστικό ή προσβλητικό κείμενο είτε η φωτογραφία ενός παιδιού που κακοποιείται. Τα παιδιά, όντας

πλήρως εξοικειωμένα με τις νέες τεχνολογίες, χρησιμοποιούν κατά κόρον τις παραπάνω πρακτικές αφού τις βρίσκουν ιδιαίτερα διασκεδαστικές.

Ένα άλλο φαινόμενο που έχει εμφανιστεί και απασχολεί έντονα αρκετές Ευρωπαϊκές χώρες και ειδικά τη Μεγάλη Βρετανία, είναι το «happy slapping». Ο όρος αναφέρεται στη διαδικασία φωτογράφησης ή βιντεοσκόπησης σκηνών παρενόχλησης και ανταλλαγής αυτών. Το happy slapping είναι στενά συνδεδεμένο με το cyberbullying, δηλαδή την παρενόχληση μέσω Διαδικτύου, ένα πρόβλημα που φαίνεται ότι αντιμετωπίζουν ένα στα τέσσερα παιδιά σε πανευρωπαϊκό επίπεδο. Μάλιστα σύμφωνα με έρευνα του Πανευρωπαϊκού Δικτύου Εθνικών Κόμβων Ασφαλούς Διαδικτύου Insafe που πραγματοποιήθηκε το 2007, το 35% των παιδιών ηλικίας κάτω των 10 ετών, θα προωθούσε σε φίλους του μέσα από το κινητό του τηλέφωνο, φωτογραφίες συμμαθητών του που ξυλοκοπούνται από άλλα παιδιά, γιατί θα το έβρισκε αστείο.

Μερικοί τρόποι πρόληψης και αντιμετώπισης της παρενόχλησης μέσω κινητού τηλεφώνου είναι οι εξής:

- Οι νέοι οφείλουν να προσέχουν πολύ σε ποιους δίνουν τον αριθμό του κινητού τους τηλεφώνου. Ακόμα και αν ένα άτομο στο οποίο οι ίδιοι έχουν δώσει τον αριθμό τους δεν τους παρενοχλήσει, είναι πιθανόν να δώσει τον αριθμό τους σε τρίτους.
- Καλό θα είναι να μην απαντάνε ποτέ σε ενοχλητικά μηνύματα που λαμβάνουν. Τα μηνύματα αυτά θα πρέπει να φυλάσσονται, ώστε σε περίπτωση καταγγελίας να μπορέσουν να αποδείξουν την παρενόχληση.
- Το συμβάν δεν θα πρέπει να υποβαθμίζεται. Η παρενόχληση μπορεί να μην μείνει μόνο στο ηλεκτρονικό επίπεδο και να εξελιχθεί σε κάτι πολύ σοβαρό αν δεν δοθεί η πρέπουσα σημασία.
- Αν η παρενόχληση είναι πολύ σοβαρή και συστηματική, οι γονείς θα πρέπει να απευθυνθούν στην εταιρία κινητής τηλεφωνίας.

Όσον αφορά τις φωτογραφίες μέσω κινητών τηλεφώνων και την ανταλλαγή τους, οι γονείς θα πρέπει να προσέξουν τα εξής:

- Να σιγουρεύουν ότι το παιδί γνωρίζει πως πρέπει πρώτα να ζητάει την άδεια των φίλων ή των γνωστών του πριν τραβήξει κάποια φωτογραφία τους.
- Να υπενθυμίζουν στο παιδί ότι δεν πρέπει ποτέ να στέλνει φωτογραφίες του σε αγνώστους μέσω του κινητού του ή να τις ανεβάζει στο Διαδίκτυο. Σε καμία περίπτωση δε, δεν πρέπει να στέλνει φωτογραφίες άλλων ανθρώπων εάν αυτοί δεν το γνωρίζουν και δεν έχουν συναινέσει για αυτό.
- Να εξηγήσουν στα παιδί ότι δεν έχουν υπό τον έλεγχό τους τις φωτογραφίες που διακινούν μέσω του κινητού τηλεφώνου. Τις φωτογραφίες δε που δημοσιεύονται στο Διαδίκτυο, μπορεί να τις δει οποιοσδήποτε στον κόσμο. Ακόμα, θα πρέπει να μιλήσουν σε αυτά για τις πιθανές συνέπειες (εντοπισμός στο φυσικό κόσμο, παραποίηση και ανάρτηση σε τρίτους ιστοχώρους).
- Να θυμίζουν στο παιδί ότι η χρήση φωτογραφικών μηχανών απαγορεύεται αυστηρά σε κάποιους χώρους, όπως π.χ. στα αποδυτήρια.
- Εάν ο τρόπος που κάποιο τρίτο άτομο χρησιμοποιεί το κινητό του και την ενσωματωμένη κάμερα, κάνει το παιδί να νιώθει άβολα, θα πρέπει να ενημερώσει άμεσα τους γονείς του.
- Να διδάξουν στο παιδί να μην αποστέλλει και να μη δημοσιεύει φωτογραφίες που απεικονίζουν προσωπικές στιγμές και που θα το έφερναν σε δύσκολη θέση.

3.8.2 Bluetooth[58]

Η τεχνολογία Bluetooth παρέχει τη δυνατότητα ασύρματης σύνδεσης μεταξύ υπολογιστών γραφείου και φορητών υπολογιστών, κινητών τηλεφώνων, βιντεοτηλεφώνων, εκτυπωτών, ψηφιακής κάμερας, με την παραπάνω λίστα να μεγαλώνει συνεχώς. Η ασύρματη τεχνολογία Bluetooth χρησιμοποιεί μια παγκοσμίως διαθέσιμη ζώνη συχνότητας (2.4GHz) με διεθνή συμβατότητα. Η τεχνολογία αυτή απαιτεί ελάχιστη ενέργεια, για να λειτουργήσει και είναι απλή στη χρήση.

Εκμεταλλευόμενοι αυτή τη τεχνολογία, μερικοί κακόβουλοι χρήστες έχουν αναπτύξει τεχνικές επιθέσεων στις συσκευές που χρησιμοποιούν Bluetooth. Με αυτού του είδους τις επιθέσεις, μπορεί κανείς να συνδεθεί με μια συσκευή με σκοπό να υποκλέψει δεδομένα (αριθμούς τηλεφώνων, μηνύματα, φωτογραφίες), να διαχειριστεί τις κλήσεις ακόμα και να παρακολουθήσει συνομιλίες σε χώρους γύρω από την συσκευή.

Για να αποτραπεί η δράση των κακόβουλων χρηστών υπάρχουν απλές λύσεις προστασίας που μπορεί ο καθένας να λάβει. Αρχικά, η λήψη αρχείων ή μηνυμάτων μέσω Bluetooth, θα πρέπει να αποφεύγεται σε περίπτωση άγνωστου αποστολέα. Επίσης, χρήσιμο είναι να υπάρχει ένας κωδικός PIN πριν από την σύνδεση με το Bluetooth. Συνήθως υπάρχει η δυνατότητα απόκρυψης της συσκευής ακόμα και όταν το Bluetooth είναι ενεργοποιημένο, παρόλα αυτά είναι προτιμότερο ο δέκτης της συσκευής να είναι κλειστός όταν δεν χρησιμοποιείται, αποτρέποντας την πρόσβαση σε αυτή.

3.9 Συμπεράσματα[59]

Το Διαδίκτυο είναι ένα εξαιρετικά χρήσιμο εργαλείο, αναπόσπαστο πλέον κομμάτι της ζωής μικρών και μεγάλων. Δεν θα πρέπει να αποτελεί φόβητρο σε όλα τα προβλήματα που προκύπτουν από την λανθασμένη χρήση του και τα

[58] https://www.microsoft.com/hellas/protect/yourself/mobile/bluetooth.mspx
http://www.saferinternet.gr

[59] Καλμαντή Μ., Μαρκάκη Ε.Α. (2010), «Ο εθισμός στο Διαδίκτυο», περιοδικό «Γιατρεύω», τεύχος 15, σελ. 14-21

οποία μπορούν να αποφευχθούν με σωστή ενημέρωση. Η απαγόρευση της χρήσης του είναι ανώφελη, καθώς οι έφηβοι μπορούν να έχουν πρόσβαση μέσω των Internet café και σαφώς μπορεί να επιφέρει τα αντίθετα αποτελέσματα.

Για τα παιδιά όλου του κόσμου, το Διαδίκτυο προσφέρει τεράστιες και πολλές φορές εκρηκτικές δυνατότητες μόρφωσης και ψυχαγωγίας, καθώς και τη δυνατότητα να μάθουν και να υλοποιήσουν πράγματα που θέλουν να κάνουν, έστω και από απόσταση. Το Διαδίκτυο μπορεί να απελευθερώσει τη δημιουργικότητα των παιδιών, να ενισχύσει την παραγωγικότητά τους και να τα φέρει κοντά στα βέλτιστα όρια του δυναμικού τους. Οι θεμελιώδεις αρχές του δικαίου, όπως η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, πρέπει να συνιστούν τις ακρογωνιαίες αρχές της λειτουργίας του Διαδικτύου.

4. Ο ΡΟΛΟΣ ΤΩΝ ΕΝΗΛΙΚΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΑΙΔΙΩΝ

Η πλοήγηση των ανηλίκων στο Διαδίκτυο ενέχει πολλούς κινδύνους, όπως παρουσιάστηκαν αναλυτικότερα στο προηγούμενο κεφάλαιο. Η ταχύτητα της σύγχρονης εποχής και της διάδοσης της χρήσης του Διαδικτύου έχει άμεσες επιδράσεις στα παιδιά, που μεγαλώνουν συχνά σε ένα περιβάλλον με ελάχιστη επίβλεψη, σε ένα αποστειρωμένο σχολείο και με έντονες επιρροές από φίλους και τηλεόραση.

Η ψηφιακή ασφάλεια των παιδιών είναι εξίσου σημαντική με την ασφάλεια των υπόλοιπων καθημερινών δραστηριοτήτων και πρόκειται να γίνει ακόμα σημαντικότερη στο άμεσο μέλλον. Η μείωση των κινδύνων για τα παιδιά που πλοηγούνται στο Διαδίκτυο εξαρτάται σε μεγάλο βαθμό από το οικογενειακό περιβάλλον, το εκπαιδευτικό και άλλους φορείς. Για αυτό, καθίσταται αναγκαία η ουσιαστική παρουσία των ενηλίκων στην «διαδικτυακή» ζωή των παιδιών, τόσο για την ενημέρωση και την πρόληψη, όσο και για την άμεση προστασία και την αντιμετώπιση των κινδύνων αυτών.

Η έννοια της ασφάλειας στο Διαδίκτυο πρέπει να επανακαθορίζεται σύμφωνα με τα σύγχρονα ψηφιακά και τεχνολογικά δεδομένα. Θα πρέπει επομένως, να συντονιστούν οι προσπάθειες ενημέρωσης και προστασίας των παιδιών τόσο από το οικογενειακό περιβάλλον όσο και από το εκπαιδευτικό, ενώ πολύ σημαντικό ρόλο παίζει και η αυτόνομη σφαίρα δράσης των ανηλίκων.

Την παραπάνω δομή παρουσίασης ακολουθεί το παρόν κεφάλαιο και αναλύει τον ρόλο που οφείλουν να έχουν οι ενήλικοι στην ασφάλεια και στην προστασία των παιδιών. Τέλος, προτείνονται τρόποι αντιμετώπισης των κινδύνων που πηγάζουν από τη σχέση παιδιού - Διαδικτύου.

4.1 Οικογενειακό περιβάλλον[60]

Ο ρόλος της οικογένειας στη διαπαιδαγώγηση του παιδιού, στην ανάδειξη της κριτικής σκέψης, στην απόκτηση σωστής συμπεριφοράς απέναντι στον συνάνθρωπο, είτε στον φυσικό είτε στους εικονικούς κόσμους, είναι καταλυτικός. Οι γονείς έχουν καθήκον όσον αφορά την εκπαίδευση για ασφαλή πλοήγηση και την προστασία των παιδιών κατά την χρήση του Διαδικτύου. Δεν είναι λίγες οι περιπτώσεις όπου τα παιδιά γνωρίζουν πολύ περισσότερα πράγματα από τους γονείς τους για τους υπολογιστές, την τεχνολογία και το Διαδίκτυο. Όταν όμως εμφανίζονται οι κίνδυνοι που κρύβονται στον εικονικό κόσμο, η άγνοια των γονέων μπορεί να δημιουργήσει μεγαλύτερα προβλήματα, καθώς δεν είναι εξοικειωμένοι με το μέσο, ώστε να μπορούν να αντιμετωπίσουν αυτές τις απειλές.

Ενδιαφέρον παρουσιάζουν τα στοιχεία της έρευνας του Ευρωβαρόμετρου (10/02/2009), για την ασφάλεια του Διαδικτύου, τα οποία εκφράζουν την κατάσταση αλλά και την δράση των γονέων για τους κινδύνους της χρήσης του Διαδικτύου.[61]

- 5 στους 10 Έλληνες γονείς δεν έχουν χρησιμοποιήσει ποτέ το Διαδίκτυο (45,8%, τελευταία θέση Ε.Ε.27), ενώ δηλώνουν για τα παιδιά τους ότι:
  - 3 στα 10 παιδιά ηλικίας 6-10 ετών
  - 6 στα 10 παιδιά ηλικίας 11-14 ετών
  - 8 στα δέκα παιδιά ηλικίας 15-17 ετών κάνουν χρήση του μέσου.
- Σε σχέση με το κινητό τηλέφωνο:
  - 10% των παιδιών ηλικίας 6-10 ετών
  - 67% των παιδιών ηλικίας 11-14 ετών

[60] http://www.0-18.gr/downloads/saferinternet_gr_eisigisi_synigoros.pdf
http://www.saferinternet.gr/index.php?childobjId=Text509&parentobjId=Category23&objId=Category119
Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.231, 232

- 95% των παιδιών ηλικίας 15-17 ετών, διαθέτουν δικό τους κινητό τηλέφωνο. Το δε 4% των παιδιών διαθέτουν κινητό με πρόσβαση στο Διαδίκτυο.

- Το 27% των γονέων δηλώνει ότι τα παιδιά του έχουν πρόσβαση στο Διαδίκτυο από Internet café (πρώτη θέση Ε.Ε.27, με την Κύπρο να ακολουθεί με 11%, και με όλες τις άλλες χώρες να έχουν μονοψήφια ποσοστά).
- 3 στους 10 Έλληνες γονείς δεν κάθονται ποτέ μαζί με τα παιδιά τους όταν αυτά σερφάρουν. Ωστόσο, 8 στους 10 γονείς ρωτάνε πάντα ή πολύ συχνά τα παιδιά τους για τις δραστηριότητές τους στο Διαδίκτυο. Το 36% ελέγχει πάντα το ιστορικό πλοήγησης αφού τα παιδιά τελειώσουν την πλοήγηση (πρώτη θέση Ε.Ε.27) και ένα 29% πάντα τα ηλεκτρονικά μηνύματα και τις υπηρεσίες instant messaging (πρώτη θέση Ε.Ε.27).
- Το 35% των γονέων δεν θέτει κανένα περιορισμό στις διαδικτυακές δραστηριότητες των παιδιών τους.
- Μόνο ένας στους δέκα Έλληνες γονείς, απαγορεύει το κατέβασμα μουσικής, ταινιών και παιχνιδιών.
- 7 στα 10 Ελληνόπουλα δεν έχουν ζητήσει ποτέ βοήθεια από τους γονείς τους, σε σχέση με πιθανά προβλήματα που αντιμετώπισαν στο Διαδίκτυο.
- Οι Έλληνες ανησυχούν πιο πολύ από όλους τους Ευρωπαίους για το ενδεχόμενο να αποκαλύψουν τα παιδιά τους τα προσωπικά τους δεδομένα στο Διαδίκτυο (52%).
- Οι Έλληνες γονείς είναι πρώτοι στην Ευρώπη αναφορικά με το βαθμό ανησυχίας για το ενδεχόμενο απομόνωσης από την πολύωρη ενασχόληση με το Διαδίκτυο (66%).
- Από τις μεγαλύτερες ανησυχίες των Ελλήνων γονέων φαίνεται πως είναι το ενδεχόμενο τα παιδιά τους να συναντήσουν ακατάλληλο σεξουαλικό

ή βίαιο περιεχόμενο στο Διαδίκτυο (81%) ή μέσω κινητού (75%), ή περιεχόμενο στο Διαδίκτυο ή το κινητό τηλέφωνο που παρακινεί στην ανορεξία, στον αυτο-τραυματισμό και την αυτοκτονία (76%).

- 56% των Ελλήνων γονέων έχουν εγκατεστημένο λογισμικό φιλτραρίσματος του διαδικτυακού περιεχομένου και / ή λογισμικό ελέγχου των διαδικτυακών δραστηριοτήτων. Όμως, το 32% δεν λαμβάνει κανένα είδους μέτρο, με την αιτιολογία ότι είτε εμπιστεύεται το παιδί του (53%), είτε ότι δεν ξέρει πώς να χρησιμοποιήσει τέτοιο είδους λογισμικό (27%).
- Μεγάλη ανησυχία προξενεί επίσης και το ενδεχόμενο σεξουαλικής αποπλάνησης του παιδιού μέσω Διαδικτύου (grooming) (78%) και το ενδεχόμενο να πέσει το παιδί θύμα ηλεκτρονικής παρενόχλησης από άλλα παιδιά είτε μέσω Διαδικτύου (83%) είτε μέσω κινητού τηλεφώνου (78%).
- 95% των Ελλήνων γονιών πιστεύουν ότι περισσότερη / καλύτερη εκπαίδευση και καθοδήγηση σχετικά με το Διαδίκτυο μέσα από το σχολείο, θα βοηθούσε τα παιδιά να πλοηγούνται με περισσότερη ασφάλεια.
- 94% των Ελλήνων γονιών πιστεύουν ότι περισσότερες καμπάνιες ενημέρωσης για τους πιθανούς διαδικτυακούς κινδύνους, θα βοηθούσε αυτούς και τα παιδιά τους να χρησιμοποιούν το Διαδίκτυο με περισσότερη ασφάλεια.

Δικαιολογημένη ή αδικαιολόγητη, η απουσία των γονέων από μια τόσο σημαντική δραστηριότητα για τις σύγχρονες ανάγκες και συνήθειες των παιδιών, όπως είναι η ενασχόληση με το Διαδίκτυο, μπορεί να δημιουργήσει σοβαρό κενό στην ανατροφή και διαπαιδαγώγησή τους. Αντιθέτως, αρκετοί φορείς, από τους εκπαιδευτικούς, έως τους παροχείς δικτυακών υπηρεσιών και τους οργανισμούς προώθησης του ασφαλούς Διαδικτύου, τονίζουν το πόσο

σπουδαίο έχει γίνει οι γονείς να περνούν χρόνο με τα παιδιά τους στο Διαδίκτυο και να επισκέπτονται αξιόλογες ιστοσελίδες μαζί. Όλοι αυτοί οι φορείς υποδεικνύουν ότι η παρέμβαση των γονέων σε τούτο το επίπεδο, μπορεί να βοηθήσει τα παιδιά να υιοθετήσουν μια σωστή χρήση του Διαδικτύου και να ανοίξουν οι ορίζοντες τους για μόρφωση, ενημέρωση και υγιή επικοινωνία. Επιπλέον, ορισμένοι φορείς αναφέρουν μια καινούργια συνιστώσα, σύμφωνα με την οποία το Διαδίκτυο μπορεί να αποτελέσει μια καινούργια και διασκεδαστική οικογενειακή δραστηριότητα. Σε μια εποχή που δεν είναι πλέον εύκολες οι οικογενειακές σχέσεις και ιδίως η επικοινωνία γονιών / παιδιών, το Διαδίκτυο μπορεί να μετατραπεί σε ένα νέο ενοποιητικό στοιχείο της οικογένειας.

Το μόνο ίσως ενθαρρυντικό σε όλα αυτά, είναι ότι οι Έλληνες γονείς αναγνωρίζουν την άγνοιά τους επί του θέματος και σύμφωνα με την προαναφερόμενη έρευνα του Ευρωβαρομέτρου, 9 στους 10 δηλώνουν την ανάγκη να αποκτήσουν περισσότερες πληροφορίες, γύρω από τους τρόπους που μπορούν να προστατεύσουν τα παιδιά τους από τους κινδύνους του Διαδικτύου. Το Διαδίκτυο δε θα πρέπει να είναι φόβητρο για τους γονείς. Θα πρέπει όμως να μπορούν να προσαρμόζονται στις νέες συνθήκες και να εκπαιδεύουν τα παιδιά τους στη χρήση του.

Το όριο ηλικίας στο οποίο τα παιδιά χρησιμοποιούν το Διαδίκτυο συνεχώς χαμηλώνει. Ουσιαστικά, ο ταχύτερα αναπτυσσόμενος τομέας χρηστών του Διαδικτύου είναι τα παιδιά της προσχολικής ηλικίας. Πολλά παιδιά χρησιμοποιούν το Διαδίκτυο στο σχολείο σε ηλικία 6 ετών, οπότε πιθανόν να θέλουν να συνδεθούν στο Διαδίκτυο από το σπίτι, σε αυτήν περίπου την ηλικία. Τα παιδιά ηλικίας κάτω των 10 ετών, ωστόσο, γενικά δεν έχουν την απαιτούμενη κριτική σκέψη για να χρησιμοποιούν το Διαδίκτυο μόνα τους. Για τον λόγο αυτό, όταν παιδιά νεότερα των 10 ετών χρησιμοποιούν το Διαδίκτυο, θα πρέπει οι γονείς να βρίσκονται συνεχώς μαζί τους ώστε να έχουν την επίβλεψη τους. Οι γονείς πρέπει να συνοδεύουν τα παιδιά τους στο Διαδίκτυο

τις πρώτες φορές, να διδάξουν την σωστή χρήση, την επιφυλακτικότητα και την αποφυγή ανεπίτρεπτων συμπεριφορών.
Μία χρήσιμη συμβουλή προς τους γονείς, είναι να τοποθετούν τον ηλεκτρονικό υπολογιστή σε ανοιχτό χώρο, όπου μπορούν να επιβλέπουν τα παιδιά και τις δραστηριότητες τους. Αυτό ισχύει ιδιαιτέρως για παιδιά αρκετά μικρής ηλικίας.
Τέλος, πολύ σημαντικό ρόλο έχει η ενημέρωση των γονέων για τις σύγχρονες τεχνολογίες, την δικτυακή πραγματικότητα, τους κινδύνους που κρύβονται, τις ασχολίες των παιδιών τους στο Διαδίκτυο και τον σκοπό που το χρησιμοποιούν. Όταν γνωρίζουν το μέσο το οποίο έχουν να αντιμετωπίσουν, μπορούν να το χειριστούν καλύτερα, εποικοδομητικότερα και με λιγότερους κινδύνους.

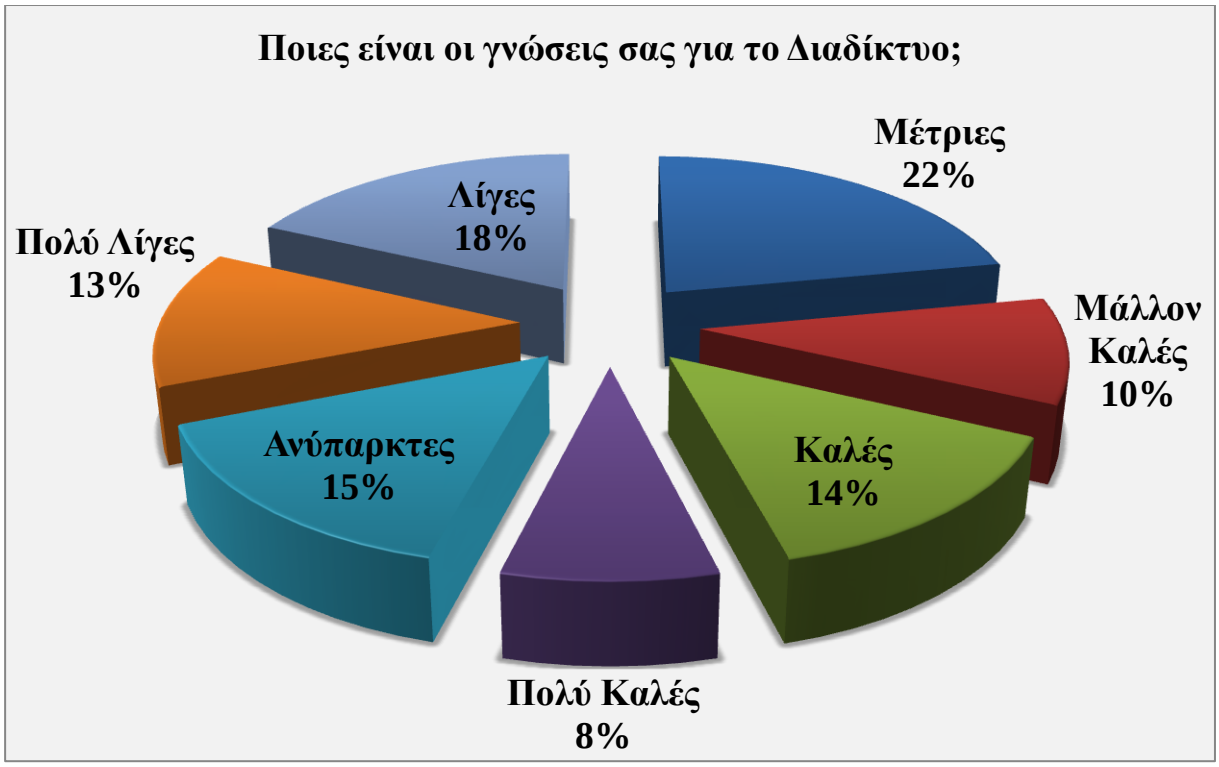
Στα σχήματα που ακολουθούν, παρουσιάζονται οι απαντήσεις 469 γονέων σχετικά με το Διαδίκτυο, σε ερωτήσεις που τους τέθηκαν μέσω έρευνας του Ινστιτούτου Οπτικοακουστικών Μέσων το διάστημα 2006-2007.

Στο Σχήμα 19 φαίνεται ότι το 8% των γονέων θεωρεί ότι το Διαδίκτυο είναι «απολύτως απαραίτητο», ενώ ένα 41% των γονέων θεωρεί ότι είναι απαραίτητο και ένα 34% θεωρεί ότι είναι μάλλον απαραίτητο. Συνολικά, πάνω από οκτώ στους δέκα γονείς θεωρούν ότι το Διαδίκτυο είναι απαραίτητο σε διάφορες διαβαθμίσεις.

Σχήμα 19 – Γνώμη γονέων για την χρησιμότητα του Διαδικτύου[62]

[62] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.382

Οι γνώσεις τους όμως σχετικά δεν ακολουθούν την ίδια κατανομή: στο Σχήμα 20 παρατηρείται ότι περίπου ο ένας στους δύο γονείς (46%) θεωρεί τις γνώσεις του για το Διαδίκτυο κυμαίνονται από «ανύπαρκτες» μέχρι «λίγες». Περίπου ο ένας στους τέσσερις (22%) θεωρεί τις γνώσεις του «μέτριες» και μόλις ένα 32% (το ένα τρίτο) θεωρεί ότι έχει επάρκεια («μάλλον καλές», «καλές» και «πολύ καλές» μαζί).



Σχήμα 20 – Γνώσεις Ελλήνων Γονέων για το Διαδίκτυο[63]

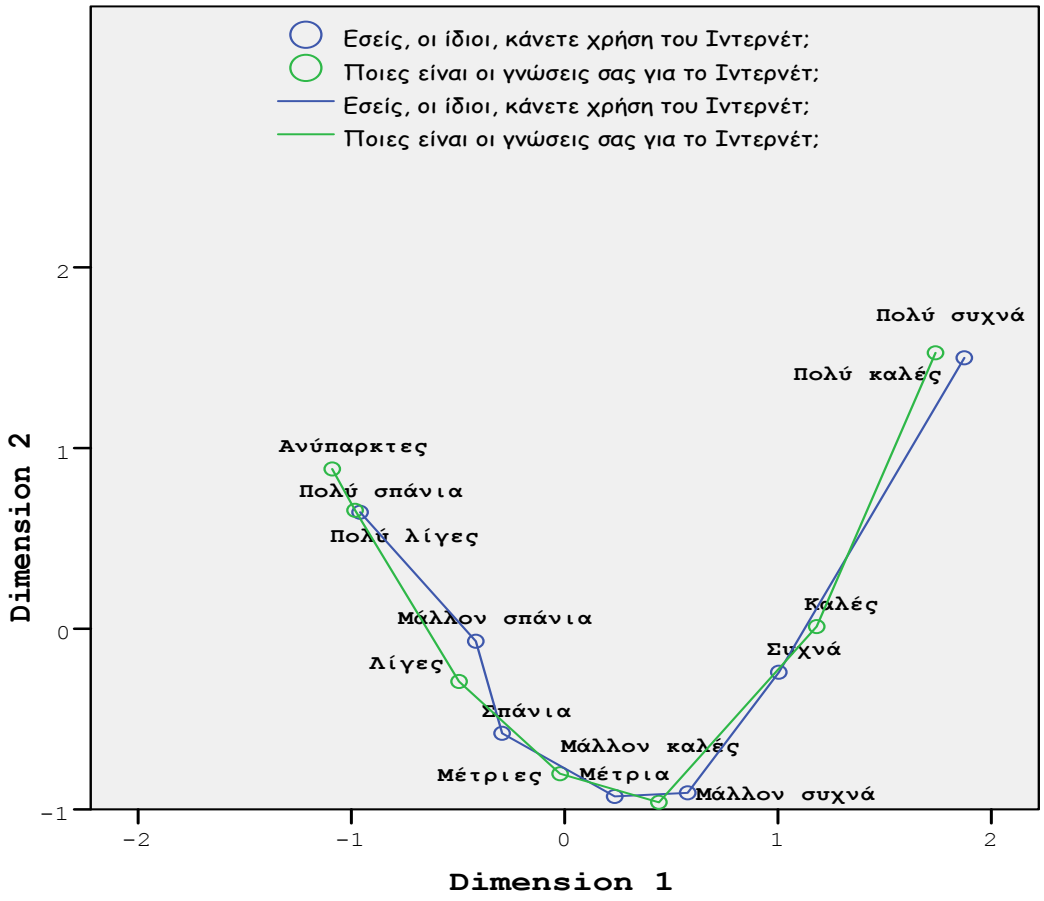
[63] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.383

Επίσης, όπως παρουσιάζεται στο Σχήμα 21, πάνω από το 50% των γονέων (55%) δεν χρησιμοποιεί ιδιαίτερα το Διαδίκτυο όπως δηλώνουν οι ίδιοι (απαντήσεις «πολύ σπάνια», «σπάνια» και «μάλλον σπάνια» μαζί). Ένα 15% το χρησιμοποιεί «μέτρια» όπως το αντιλαμβάνονται οι ίδιοι ενώ, τελικά, μόλις ένα 30% δηλώνουν ότι το χρησιμοποιούν είτε «μάλλον συχνά» είτε «συχνά» είτε «πολύ συχνά».

Σχήμα 21 – Συχνότητα χρήσης Διαδικτύου από τους γονείς[64]

[64] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.383

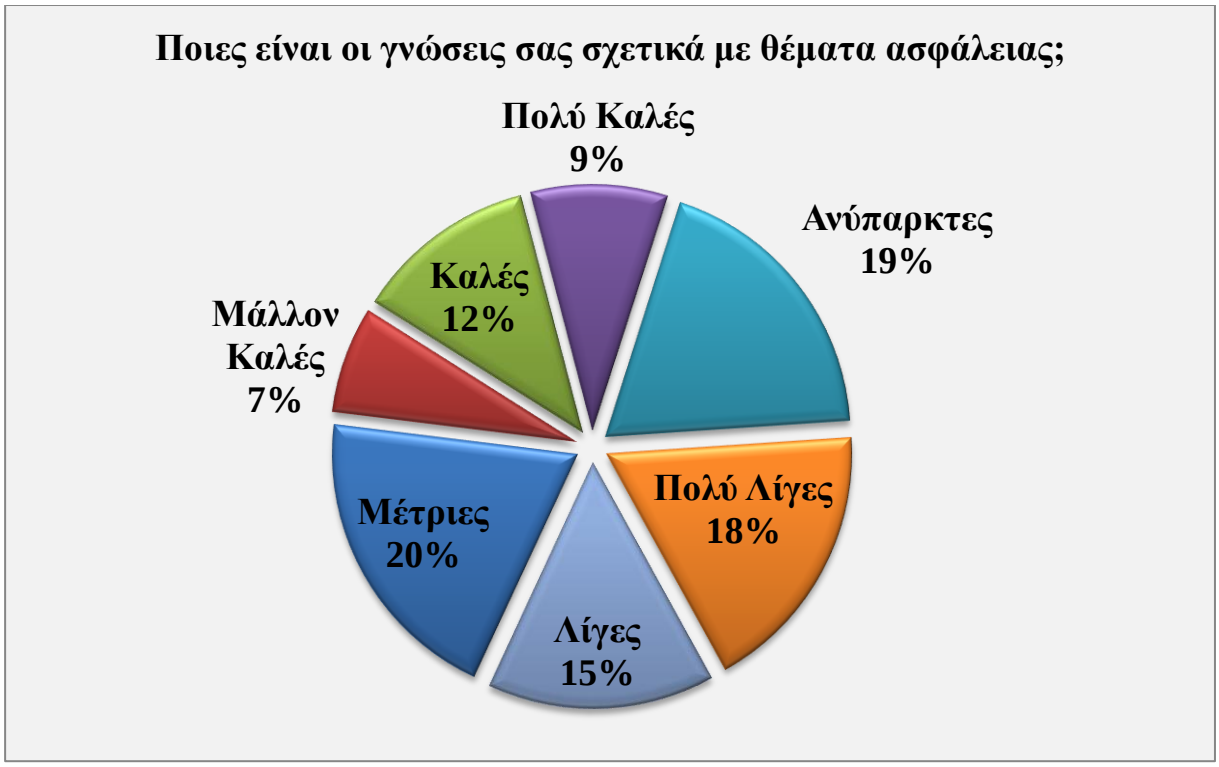
Όπως φαίνεται ξεκάθαρα στο Σχήμα 22, το ποσοστό χρήσης του Διαδικτύου συμβαδίζει περισσότερο με τις γνώσεις που έχουν γι' αυτό παρά με το βαθμό αποδιδόμενης ανάγκης χρήσης του (το πόσο «απαραίτητο» είναι). Έτσι, αν και η συντριπτική πλειοψηφία των γονέων θεωρεί ότι το Διαδίκτυο είναι απαραίτητο, δηλώνουν, επίσης πλειοψηφικά, ότι δεν έχουν επαρκείς γνώσεις και ότι, γενικά, δεν το χρησιμοποιούν ιδιαίτερα. Σε μια πρώτη φάση λοιπόν, σε επίπεδο προσωπικής χρήσης γονέων, το Διαδίκτυο παραμένει στην σφαίρα της προσδοκώμενης (ίσως και φαντασιακής) υπηρεσίας. Δηλαδή, «…θα πρέπει να το κάνω, αλλά…»



Σχήμα 22 – Ανάλυση αντιστοιχιών στον βαθμό γνώσης σχετικά με το Διαδίκτυο και την χρήση του Διαδικτύου[65]

[65] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.384

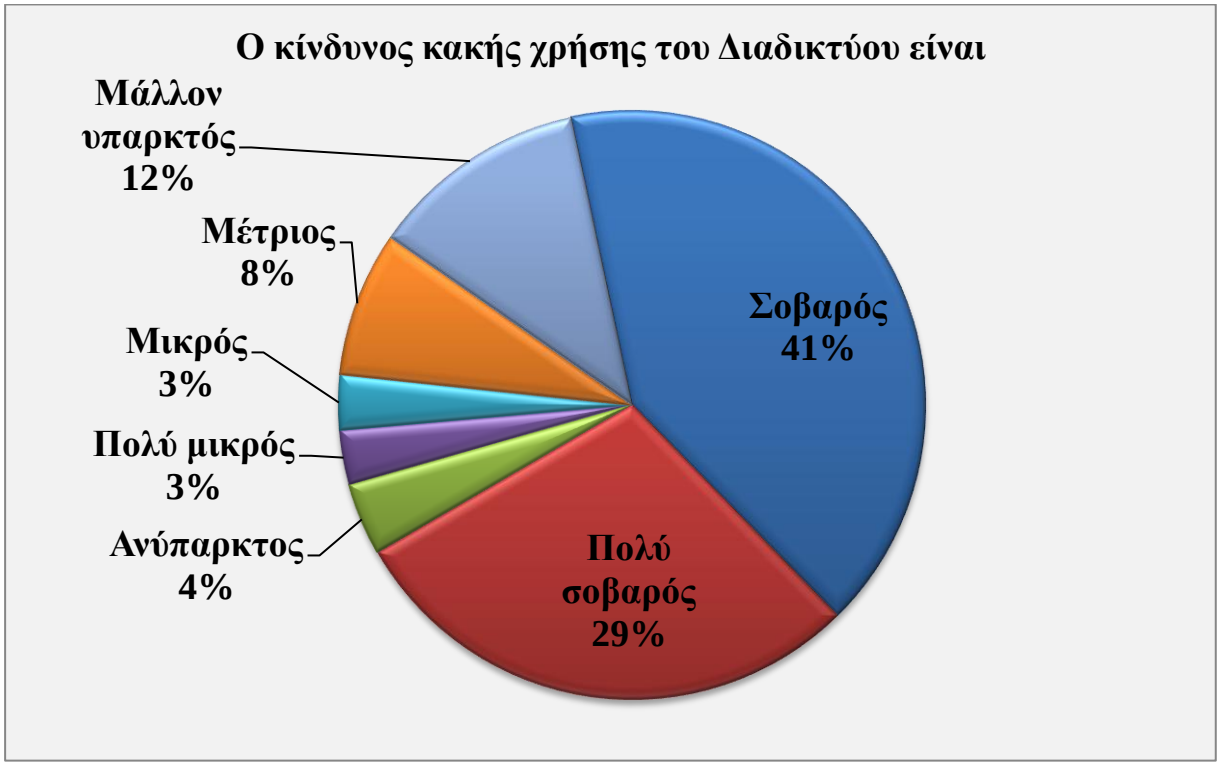
Το άλλο μεγάλο θέμα σε σχέση με το Διαδίκτυο είναι η ασφάλεια ή, μάλλον, η έλλειψη ασφάλειας. Έτσι, όπως παρουσιάζεται στο Σχήμα 23, μόλις το 27% των γονέων δηλώνει κάποιου βαθμού επάρκεια γνώσεων σχετικά με θέματα ασφαλείας στο Διαδίκτυο. Το 20% πιστεύει ότι έχει μέτριες γνώσεις και οι υπόλοιποι (52% δηλαδή πάνω από ένας στους δύο) θεωρούν ότι οι γνώσεις τους είναι μάλλον ανεπαρκείς όσον αφορά την ασφάλεια στο Διαδίκτυο.



Σχήμα 23 – Γνώσεις Ελλήνων Γονέων σε Θέματα Ασφαλείας[66]

[66] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.385

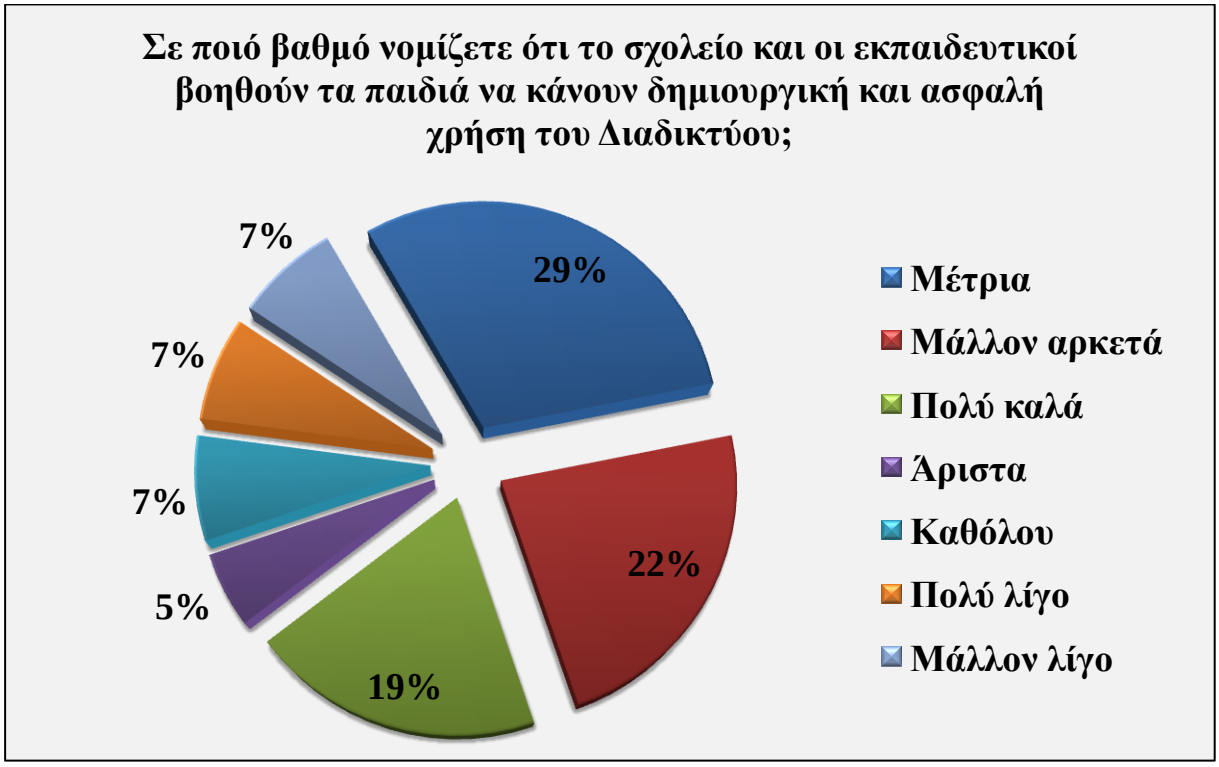
Από την άλλη πλευρά, οι μάλλον ανεπαρκείς γνώσεις συνοδεύονται και από μια αυξημένη αίσθηση απειλής: οι επτά από τους δέκα γονείς θεωρούν ότι ο κίνδυνος κακής χρήσης του Διαδικτύου είναι είτε «σοβαρός» είτε «πολύ σοβαρός». Ο συνδυασμός αυτών των δύο ερωτήσεων, δίνει την εικόνα μιας σχεδόν «φοβικής» αντιμετώπισης του Διαδικτύου από την πλευρά των γονέων: ενώ, όπως δηλώνουν, δεν έχουν επαρκείς γνώσεις για να προστατευθούν, νιώθουν ότι η απειλή μπορεί να είναι μέχρι και πολύ σοβαρή.



Σχήμα 24 – Γνώμη γονέων για τον κίνδυνο κακής χρήσης του Διαδικτύου[67]

[67] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.385

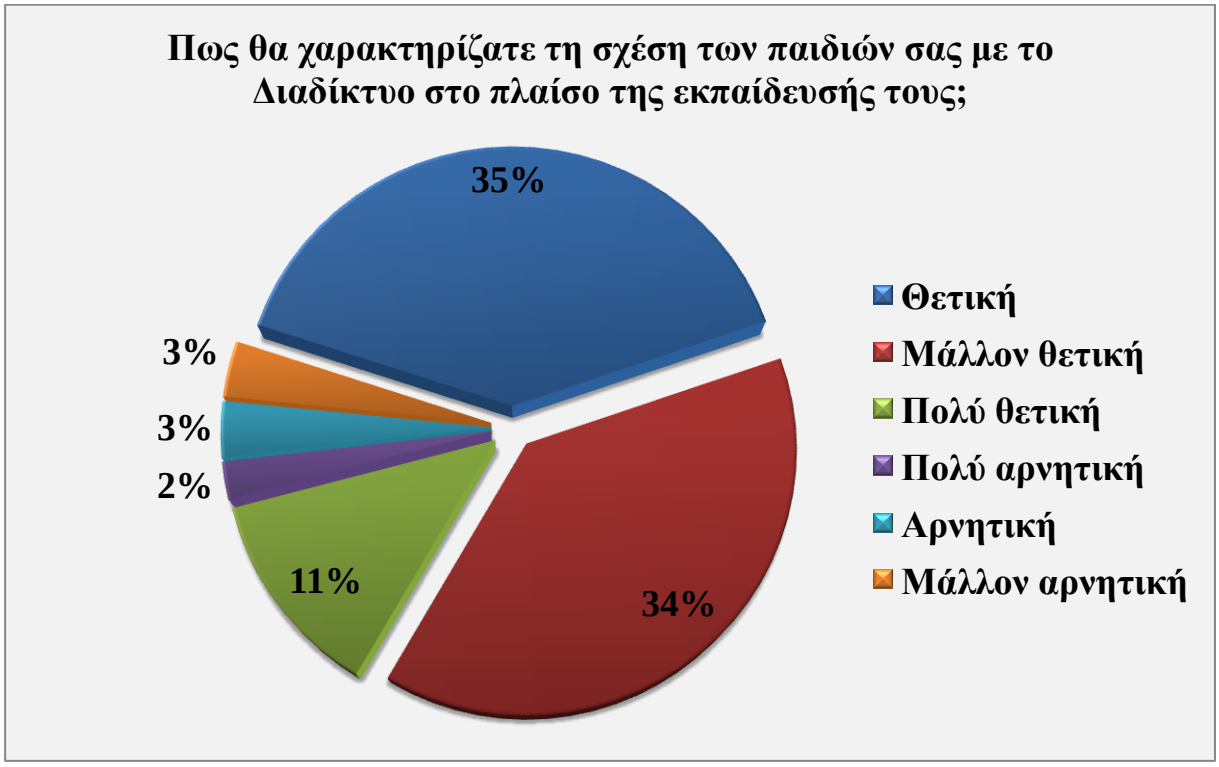
Στο Σχήμα 25 παρατηρείται ότι οι γονείς θεωρούν κατά περίπου 46%, ότι οι εκπαιδευτικοί στο σχολείο βοηθούν τα παιδιά να κάνουν δημιουργική και ασφαλή χρήση του Διαδικτύου σε επαρκή βαθμό (αρκετά, πολύ και πάρα πολύ-άριστα).Επίσης, ένα σημαντικό ποσοστό δηλώνει ότι οι εκπαιδευτικοί βοηθούν τα παιδιά μάλλον «μέτρια» (29%) ενώ, το υπόλοιπο (25%, ο ένας στους τέσσερις γονείς) δηλώνει ότι η βοήθεια των εκπαιδευτικών είναι μάλλον ανεπαρκής.



Σχήμα 25 – Γνώμη γονέων για τους εκπαιδευτικούς[68]

[68] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.386

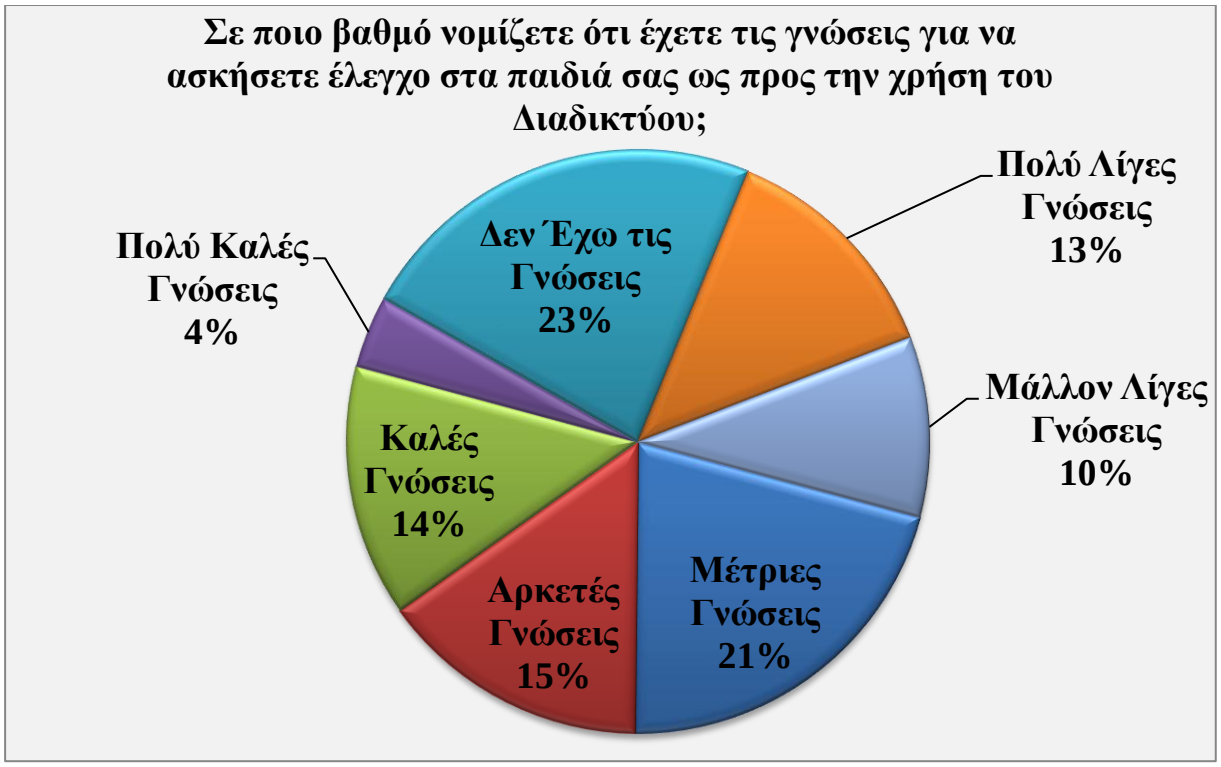
Όμως το θέμα παραμένει η «νέα γενιά»: αν, απ' ότι φαίνεται οι γονείς δεν χρησιμοποιούν ιδιαίτερα το Διαδίκτυο ούτε και έχουν επαρκείς γνώσεις για να το κάνουν, δεν το θεωρούν ιδιαίτερα ασφαλές ούτε και θεωρούν ότι έχουν επάρκεια γνώσεων για να προστατευθούν τότε γιατί να το θεωρούν απαραίτητο; Μια πρώτη απάντηση δίδεται στο Σχήμα 26: το 80% των γονέων θεωρεί ότι το Διαδίκτυο έχει μια θετική σχέση με την εκπαίδευση των παιδιών τους. Με άλλα λόγια, το Διαδίκτυο (ίσως αδιευκρίνιστο από τους περισσότερους το γιατί) θεωρείται ότι συμβάλλει στην εκπαίδευση των παιδιών τους ή, μάλλον το πιθανότερο, έχει πλέον επιβληθεί σαν ένα ακόμα «απαραίτητο εφόδιο» στην εκπαιδευτική εξέλιξη των παιδιών.



Σχήμα 26 – Γνώμη γονέων για το Διαδίκτυο στην εκπαίδευση[69]

[69] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.386

Όσον αφορά την ασφάλεια χρήσης του Διαδικτύου σε σχέση με τον έλεγχο που ασκούν στα παιδιά, περίπου ο ένας στους δύο γονείς (Σχήμα 27), το 46%, δηλώνουν ανεπάρκεια γνώσεων για να ασκήσουν έλεγχο (λίγες – πολύ λίγες – ανύπαρκτες γνώσεις). Μόλις το 32% δηλώνει σχετική επάρκεια γνώσεων (αρκετές – καλές – πολύ καλές γνώσεις), ενώ το 21% αυτό-τοποθετείται στις «μέτριες» γνώσεις.



Σχήμα 27 – Γνώσεις Ελλήνων Γονέων για Έλεγχο των Παιδιών στην Χρήση Διαδίκτυο[70]

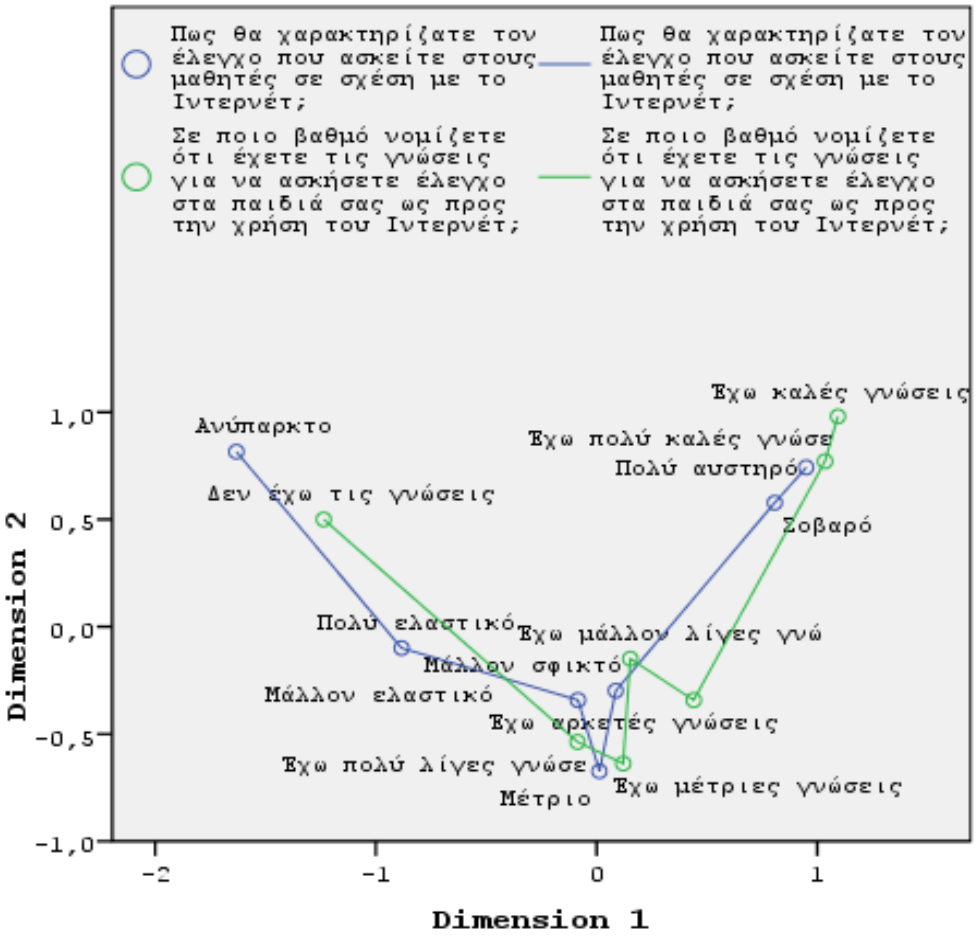
[70] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.387

Με τέτοιο επίπεδο γνώσεων, πως χαρακτηρίζουν τον έλεγχο που ασκούν στα παιδιά; Φαίνεται, ότι το 28% των γονέων θεωρούν ως μάλλον ανεπαρκή τον έλεγχο που ασκούν. Το 41% των γονέων εντούτοις, δηλώνει ότι ασκεί από «μάλλον σφικτό» έως «πολύ αυστηρό» έλεγχο. Τέλος, περίπου ο ένας στους τρεις (31%) δηλώνει «μέτριου» βαθμού έλεγχο.

Σχήμα 28 – Έλεγχος γονέων στα παιδιά σε σχέση με το Διαδίκτυο[71]

[71] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.388

Στο Σχήμα 29 διακρίνεται ότι: «χαμηλού επιπέδου» γνώσεις οδηγούν σε «ελαστικούς» ελέγχους, ενώ «υψηλού επιπέδου» γνώσεις συνάδουν με πιο «σφικτή» αντιμετώπιση. Με λίγα λόγια, όσο πιο ενημερωμένοι θεωρούν τους εαυτούς τους οι γονείς, τόσο πιο αυστηρό έλεγχο ασκούν. Με αυτήν την προϋπόθεση, μπορεί κανείς να υποθέσει, ότι εάν αυξηθεί η ενημέρωση των γονέων, θα υπάρξει βελτίωση στον έλεγχο που ασκείται από αυτούς.



Σχήμα 29 – Έλεγχος ανάλυση αντιστοιχιών στον βαθμό γνώσης σχετικά με την ασφάλεια στο Διαδίκτυο και την αυστηρότητα ελέγχου σχετικά με την χρήση του Διαδικτύου[72]

[72] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.388

4.1.1.1 Οικογενειακοί κανόνες

Μια απλή αλλά ταυτόχρονα ουσιαστική μέθοδος που θα μπορούσαν να εφαρμόσουν οι γονείς μαζί τα παιδιά, είναι η διαπραγμάτευση και η δημιουργία ενός οικογενειακού κώδικα συμπεριφοράς στον οποίο θα πρέπει όλοι να συμφωνήσουν. Η γνώμη των παιδιών είναι αρκετά σημαντική για την επιτυχία της συμφωνίας. Μέσα σε αυτό τον κώδικα θα καθορίζονται τα δικαιώματα και οι υποχρεώσεις σχετικά με τη χρήση του υπολογιστή και του Διαδικτύου στο σπίτι. Οι κανόνες μπορούν να είναι διαφορετικοί ανάλογα την ηλικία του κάθε παιδιού. Η συμφωνία αυτή, καλό θα ήταν να επικυρωθεί γραπτώς με μία υπογραφή από το κάθε μέλος της οικογένειας, δείχνοντας έτσι ότι κατανοούν τους όρους. Ύστερα, μπορούν να κολλήσουν τους κανόνες πλάι σε κάθε υπολογιστή του σπιτιού, ώστε να υπενθυμίζουν σε όλα τα μέλη τους οικογενειακούς κανόνες χρήσης και συμπεριφοράς. Οι γονείς θα πρέπει να αναθεωρούν και να ενημερώνουν τακτικά τη συμφωνία, καθώς τα παιδιά μεγαλώνουν.

4.1.2 Διασφαλίζοντας το απόρρητο

Καθοριστικό ρόλο στην σωστή και ασφαλή χρήση του Διαδικτύου είναι η κατανόηση από τα παιδιά του «προσωπικού απορρήτου». Οι γονείς θα πρέπει να διδάξουν στα παιδιά πώς να διαφυλάσσουν τα προσωπικά ή και οικογενειακά τους δεδομένα και να μην αποκαλύπτουν απερίσκεπτα πληροφορίες στο Διαδίκτυο.

Πιο συγκεκριμένα, οι γονείς οφείλουν να εξηγήσουν στα παιδιά, ότι σε καμία περίπτωση δεν πρέπει να γνωστοποιούν στοιχεία σε άγνωστους μέσω του Διαδικτύου, όπως e-mail, αριθμούς τηλεφώνων, διεύθυνση κατοικίας ή σχολείου, φωτογραφίες, και να μην αποκαλύπτουν τους κωδικούς πρόσβασης που χρησιμοποιούν στις διάφορες υπηρεσίες του Διαδικτύου. Ακόμα, οι γονείς μπορούν να βοηθήσουν τα παιδιά να δημιουργήσουν ένα ψευδώνυμο το οποίο θα χρησιμοποιούν στο Διαδίκτυο.

Σε περίπτωση που μια ιστοσελίδα ζητά προσωπικές πληροφορίες, οι γονείς θα πρέπει να σιγουρευτούν ότι η ιστοσελίδα είναι αξιόπιστη και πριν προχωρήσουν στην καταχώρηση των στοιχείων, καλό θα είναι να ρωτήσουν για ποιο λόγο τα χρειάζονται. Πάντα θα πρέπει να συμβουλεύονται τους όρους και προϋποθέσεις (terms and conditions) και την πολιτική απορρήτου (privacy statement) της εταιρίας που διαχειρίζεται τον ιστοχώρο.

4.1.3 Συμβουλές για γονείς[73]

Παράλληλα οι γονείς μπορούν να βοηθήσουν τα παιδιά τους να χρησιμοποιούν ασφαλέστερα το Διαδίκτυο εφαρμόζοντας τις ακόλουθες συμβουλές:

- Ενημέρωση των γονέων για την σύγχρονη δικτυακή πραγματικότητα, τις δυνατότητες και τους κινδύνους που υπάρχουν, για το τι κάνουν τα παιδιά τους στο Διαδίκτυο και με τι σκοπό το χρησιμοποιούν.
- Δημιουργία λίστας με προτεινόμενες παιδικές σελίδες και μηχανές αναζήτησης φιλικές στη χρήση τους για παιδιά.
- Έλεγχος των Αγαπημένων (bookmarks) και του Ιστορικού (history) του προγράμματος φυλλομετρητή ιστοσελίδων (browser) για να δουν ποιες σελίδες έχουν επισκεφτεί τα παιδιά τους.
- Ενημέρωση των γονέων περί λογισμικού γονικού ελέγχου το οποίο είναι διαθέσιμο και εξέταση της δυνατότητας εφαρμογής ενός φίλτρου προστασίας, στους υπολογιστές του σπιτιού.
- Οι γονείς θα πρέπει να διδάξουν στα παιδιά πώς να αξιολογούν πληροφορίες που βρίσκουν σε έναν ιστότοπο. Αν μια ιστοσελίδα έχει ωραία εμφάνιση δε σημαίνει ότι και το περιεχόμενό της είναι αληθινό.
- Παρότρυνση των παιδιών να μην ανοίγουν ποτέ μηνύματα, ή σελίδες από ανθρώπους που δεν τους γνωρίζουν, καθώς μπορεί να περιέχουν κακόβουλο λογισμικό.

[73] http://www.sch.gr/2010-04-07-09-22-34/2010-04-07-10-31-40/Σελίδα-4#content
http://www.alphait.gr/saferinternet.shtml
http://www.safeline.gr/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF-%CE%BA%CE%B1%CE%B9-%CE%B3%CE%BF%CE%BD%CE%B5%CE%AF%CF%82

- Οι γονείς χρειάζεται να μαθαίνουν για τους φίλους που έκαναν τα παιδιά τους στο Διαδίκτυο και συζητήσουν μαζί τους γι' αυτούς. Να βεβαιωθούν ότι δε θα τους συναντήσουν χωρίς την έγκριση και την παρουσία τους και να τους εξηγήσουν τον λόγο.
- Δημιουργία διαφορετικών λογαριασμών χρηστών στα Windows, με διαφορετικούς κωδικούς για τους γονείς (διαχειριστής) και τα παιδιά (χρήστης), ώστε οι γονείς να έχουν τον έλεγχο του υπολογιστή (π.χ. εγκατάσταση νέων προγραμμάτων, ώρες χρήσης υπολογιστή κ.α.)
- Θέσπιση κανόνων συμμετοχής σε ηλεκτρονικά παιχνίδια (κυρίως σχετικά με το χρόνο που μπορεί να αφιερώσει το κάθε μέλος της οικογένειας στο παιχνίδι).
- Εκμάθηση των παιδιών για τη χρήση ιστοσελίδων με επιμορφωτικό και ψυχαγωγικό περιεχόμενο κατάλληλο για την ηλικία τους.
- Οι γονείς θα πρέπει να μην χρησιμοποιούν τη χρήση του υπολογιστή για επιβράβευση ή τιμωρία.
- Ενημέρωση σχετικά με τις αρμόδιες αρχές, που μπορούν οι γονείς να επικοινωνήσουν σε περίπτωση που συναντήσουν βλαβερό ή παράνομο περιεχόμενο στο Διαδίκτυο.
- Θέσπιση απλών κανόνων για τη χρήση του Διαδικτύου στα παιδιά, τονίζοντας τις υποχρεώσεις τους στο σχολείο και ενθαρρύνοντας τις επιπλέον εξωσχολικές δραστηριότητές τους.

4.2 Εκπαιδευτικό περιβάλλον

Είναι γεγονός ότι η τεχνολογία έχει επιδράσει θετικά στην εκπαίδευση. Το Διαδίκτυο έχει ξεπεράσει τα εμπόδια της απόστασης, της ανταλλαγής πληροφοριών και δεδομένων, έχει διευκολύνει την εξόρυξη της γνώσης και την διευκόλυνση του εκπαιδευτικού έργου. Σίγουρα όμως, παρά την χρησιμότητα του, οι κίνδυνοι που υποκρύπτονται μπορούν να εκθέσουν τους μαθητές σε

παράνομες δραστηριότητες και υλικό, να τα οδηγήσουν στην εξαπάτηση, την παρενόχληση και την αποπλάνηση.

Για αυτούς τους λόγους είναι σημαντικό και αναγκαίο τα σχολεία να εκπαιδεύουν τους μαθητές με στόχο την σωστή και ασφαλή χρήση του Διαδικτύου. Οι εκπαιδευτικοί χρειάζεται να προωθούν ασφαλές μεθόδους και τακτικές και πάντα να έχουν την επίβλεψη των παιδιών κατά την διάρκεια της πλοήγησης στο Διαδίκτυο. Θα πρέπει να διδάξουν ότι ο συναρπαστικός αυτός κόσμος δημιουργεί μια ψευδαίσθηση ασφάλειας, η οποία μπορεί να πάρει άσχημη τροπή.

Πολύ καθοριστικό ρόλο κατέχει η ενημέρωση των εκπαιδευτικών σχετικά με τις τεχνολογικές εξελίξεις, το Διαδίκτυο και τους κινδύνους του, τις δραστηριότητες των μαθητών σε αυτό και τον σκοπό που το χρησιμοποιούν. Προτιμητέο είναι να γίνονται συζητήσεις μεταξύ μαθητών και εκπαιδευτικών για τα πλεονεκτήματα και τα μειονεκτήματα του Διαδικτύου, ώστε να δημιουργείται μια ανοιχτή και σφαιρική άποψη γύρω από το θέμα.

Ορισμένα σχολεία του εξωτερικού που προσπάθησαν να τιμωρήσουν μαθητές που διέπραξαν ηλεκτρονική παρενόχληση μετά το πέρας των μαθημάτων τους, δέχτηκαν μηνύσεις για κατάχρηση της εξουσίας τους. Αν και δεν μπορούν να δραστηριοποιηθούν για την αντιμετώπιση του φαινομένου, τα σχολεία οφείλουν και μπορούν να κάνουν πολλά για την πρόληψή του, μέσα από την παροχή σωστής και υπεύθυνης πληροφόρησης.

Επίσης, χρειάζεται άμεση αλλαγή νοοτροπίας από πλευράς των εκπαιδευτικών. Η νοοτροπία του «κακού λύκου που παραμονεύει» και η οποία οδηγεί σε απαγόρευση της χρήσης των ιστοσελίδων κοινωνικής δικτύωσης πρέπει να εκλείψει και στη θέση της πρέπει να υιοθετηθεί μια πιο ώριμη στάση που θα ενθαρρύνει τη λογική και ενσυνείδητη χρήση των ιστοσελίδων αυτών.

4.2.1 Ελλείψεις[74]

Η εκπαίδευση είναι το κατεξοχήν πεδίο όπου η επίσημη πολιτεία μπορεί να παρέμβει και να επηρεάσει παιδιά και νέους για μια δημιουργική και ασφαλή χρήση του Διαδικτύου. Σύμφωνα με τους διάφορους φορείς, η Ελληνική πολιτεία έχει μεν συνειδητοποιήσει την αναγκαιότητα και χρησιμότητα του Διαδικτύου στην εκπαίδευση, δημιουργώντας σχετικές υποδομές και προγράμματα. Ωστόσο, οι περισσότεροι φορείς θεωρούν ότι υπάρχουν σημαντικές ελλείψεις και μεγάλα περιθώρια για περαιτέρω ενσωμάτωση της χρήσης του Διαδικτύου εντός και εκτός των σχολικών αιθουσών, καθώς επίσης και για ευαισθητοποίηση των μαθητών σε θέματα ασφάλειας

Η υιοθέτηση νέων τεχνολογιών στο σύνολο του εκπαιδευτικού συστήματος της Ελλάδας, παρουσίασε ανάλογες χρονικές καθυστερήσεις, τόσο από πλευράς τεχνολογικών υποδομών, όσο και ως προς τη χρήση του Διαδικτύου ως εκπαιδευτικό μέσο. Σημαντικό παράγοντα για τους χαμηλούς ρυθμούς ανάπτυξης του Διαδικτύου στην Ελλάδα, αποτελεί επίσης η μη δέσμευση κρατικών πόρων για προγράμματα βελτίωσης δεξιοτήτων και ενίσχυση των εκπαιδευτικών και ερευνητικών δραστηριοτήτων.

Η αργοπορημένη ένταξη του Διαδικτύου στην εκπαίδευση αποτελεί σημαντικό λόγο χαμηλής χρήσης και ανάπτυξης του Διαδικτύου. Έχουν γίνει σημαντικά βήματα να αποκτήσουν τα σχολεία την απαραίτητη υποδομή όπως πχ. αγορά απαραίτητου εξοπλισμού για τη δημιουργία εργαστηρίων Πληροφορικής κ.λπ., πέρα όμως από τον εξοπλισμό, σημαντικό ρόλο κατέχει και η εκπαίδευση των μαθητών στη χρηστικότητα του Διαδικτύου ώστε να κατανοήσουν τις δυνατότητες γνώσης, πληροφόρησης, μάθησης, επικοινωνίας ή ακόμα και ψυχαγωγίας που τους παρέχει το Διαδίκτυο.

[74] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.223
«Πλάνο δράσης για την ανάπτυξη του Internet στην Ελλάδα», σελ.28

4.2.2 Προτάσεις[75]

Προτάσεις που θα μπορούσαν να βελτιώσουν στο ορατό μέλλον τη δημιουργική και ασφαλή ενασχόληση των παιδιών με το Διαδίκτυο στα πλαίσια του εκπαιδευτικού συστήματος:

- Παράδοση μιας ομαδικής - και όχι μόνο ατομικής - εργασίας, που θα απαιτεί την αναζήτηση πληροφοριών μέσω του Διαδικτύου, θα βοηθούσε τους νέους να αναπτύξουν μια δημιουργική σχέση με τον παγκόσμιο ιστό στα πλαίσια των σχολικών καθηκόντων τους αλλά και πέραν αυτών.
- Μεγάλη πρόοδος θα ήταν, αν το Υπουργείο Παιδείας μπορούσε σταδιακά να βάλει σε κάθε τάξη όλων των σχολείων έναν υπολογιστή που θα είναι συνδεμένος στο Διαδίκτυο και ο οποίος θα χρησιμοποιείται από τους μαθητές και τους εκπαιδευτικούς για την εύρεση πληροφοριών κατά τη διάρκεια της διδασκαλίας.
- Σημαντική θεωρείται από ορισμένες πλευρές, η αξιοποίηση των υπολογιστών και του Διαδικτύου στο πλαίσιο μιας διαθεματικής προσέγγισης των ποικίλων γνωστικών αντικειμένων και χωρίς κατακερματισμένη χρήση των Μέσων ανά γνωστικό αντικείμενο.
- Οι εκπαιδευτικοί της πρωτοβάθμιας εκπαίδευσης, υπογραμμίζοντας τη διαρκή μείωση της ηλικίας των παιδιών που ασχολούνται με τον υπολογιστή και το Διαδίκτυο, θέτουν το θέμα της ένταξης μαθήματος χρήσης υπολογιστή στο κανονικό ωρολόγιο πρόγραμμα για τις Δ΄, Ε΄ και ΣΤ΄ τάξεις του δημοτικού σχολείου και όχι μόνο στο πρόγραμμα του Ολοήμερου Δημοτικού.
- Μια κοινωνική οργάνωση όπως η ΕΕΧΙ, ζητά μείωση του κόστους παροχής υπηρεσιών Διαδικτύου, σε συνδυασμό με αύξηση των ταχυτήτων που διατίθενται στους χρήστες, εκσυγχρονισμό του δικτύου

[75] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.225-227 http://www.youth-health.gr/gr/index.php?I=6&J=2&K=42

πανελλαδικά και αύξηση των σημείων ασύρματης πρόσβασης σε όλη την περιφέρεια. Θέτει επίσης θέμα επιδότησης της αγοράς προσωπικού υπολογιστή σε ευαίσθητες κοινωνικές ομάδες, φοιτητές, μαθητές κ.λπ., ενίσχυσης των δημόσιων υπηρεσιών που προσφέρονται στους πολίτες στο Διαδίκτυο και ενημέρωσης του καταναλωτή για τις ευκολίες που παρέχει το Διαδίκτυο, αλλά και για τον τρόπο προστασίας του από κακόβουλες επιθέσεις.

- Τέλος, οι φορείς από το χώρο της εκπαίδευσης συμπληρώνουν ότι χρειάζεται αναβάθμιση των ταχυτήτων με τις οποίες είναι συνδεδεμένα τα περισσότερα σχολεία στο Διαδίκτυο, ένταξη των θεμάτων ασφάλειας στα μαθήματα πληροφορικής και στα σεμινάρια κατάρτισης των εκπαιδευτικών και εξέταση του ζητήματος πως μπορεί να δοθεί δωρεάν ή φθηνή παροχή σύνδεσης με το Διαδίκτυο στους μαθητές και εκτός σχολείου.
- Επιμόρφωση των εκπαιδευτικών πάνω σε θέματα ασφαλής πλοήγησης, διαδικτυακών κινδύνων και εξοικείωση αυτών με το μέσο.
- Εκπαίδευση των μαθητών για τις διάφορες εφαρμογές και τη διευκόλυνσή τους στη χρήση διαδικτυακών μηχανών αναζήτησης.
- Ενημέρωση των γονέων μέσω του σχολείου για το φαινόμενο και τα σημεία αναγνώρισης της προβληματικής χρήσης.

4.2.3 Οι εκπαιδευτικοί[76]

Οι εκπαιδευτικοί των διαφόρων ειδικοτήτων (και όχι ειδικά της πληροφορικής) έχουν τις γνώσεις και την κατάλληλη νοοτροπία για να προτρέψουν τους μαθητές τους στη δημιουργική και ασφαλή χρήση του Διαδικτύου; Έχουν οι εκπαιδευτικοί επίγνωση των προβλημάτων ασφάλειας ώστε να είναι σε θέση να ενημερώνουν και να συμβουλεύουν τα παιδιά; Είναι μερικές από τις ερωτήσεις που απασχολούν τους γονείς.

[76] Κατερέλος Ι., Παπαδόπουλος Π. (2009). *Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση*. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.227-229

Οι ίδιοι οι φορείς των εκπαιδευτικών απαντούν σχεδόν πλήρως αρνητικά και στα δύο ερωτήματα. Αναφέρουν, βεβαίως, ότι οι νεότεροι καθηγητές και δάσκαλοι είναι περισσότερο συμφιλιωμένοι με την τεχνολογία και την πληροφορική, αλλά ακόμη κι αυτοί δεν έχουν επαρκείς γνώσεις για να προτρέψουν τους μαθητές μεθοδικά σε μια πράγματι δημιουργική και ασφαλή χρήση του Διαδικτύου, καθώς και εναλλακτικών πηγών και μέσων (π.χ. οπτικοακουστικά μέσα). Εξαίρεση αποτελεί η περίπτωση εκπαιδευτικών που οι ίδιοι είναι τακτικοί χρήστες του Διαδικτύου. Ένας φορέας μάλιστα, όπως το ΚΕΜΕΤΕ επισημαίνει ότι ορισμένες έρευνες καταγράφουν και ένα είδος «τεχνοφοβίας» ανάμεσα σε εκπαιδευτικούς, ιδίως των μεγαλύτερων ηλικιών, διαπίστωση που είναι παρόμοια με αυτή που ισχύει και για την ευρύτερη Ελληνική κοινωνία.

Επιπλέον, η όποια επιμόρφωση γίνεται στους εκπαιδευτικούς για θέματα τεχνολογίας και πληροφορικής χαρακτηρίζεται από αρκετές πλευρές ως ανεπαρκής και τυπική σε σχέση με τις πραγματικές ανάγκες ενός εκπαιδευτικού λειτουργού. Χαρακτηριστικά η ΑΣΓΜΕ κρίνει ότι «οι εκπαιδευτικοί επιμορφώνονται στη χρήση ηλεκτρονικού υπολογιστή ως να είναι υπάλληλοι γραφείου ή λογιστές». Επίσης, η επιμόρφωση τους δεν ασχολείται με ερωτήματα όπως:

- με ποιο τρόπο μπορούν να αξιοποιούν τους Η/Υ και το Διαδίκτυο στο μάθημά τους
- ποιά ισορροπία πρέπει να έχει ο συνδυασμός Η/Υ, διδασκαλίας και βιβλίων
- αν οι Η/Υ πρέπει να είναι χωριστό μάθημα ή εργαλείο μάθησης σε κάθε μάθημα κ.λπ.

Επίσης, ένας φορέας όπως η ΕΕΧΙ, που βλέπει το ζήτημα από την πλευρά της κοινωνίας, με βάση τις δικές της επισκέψεις σε σχολεία διαπιστώνει ότι οι εκπαιδευτικοί, πλην εξαιρέσεων: εμμένουν στον παραδοσιακό τρόπο

διδασκαλίας και διστάζουν να προτρέψουν τους μαθητές στην χρήση του Διαδικτύου, λόγω της ανόμοιας οικονομικής τους κατάστασης που μπορεί να σημαίνει έλλειψη ηλεκτρονικού υπολογιστή ή Διαδικτύου στο σπίτι.

Όπως και να έχει, με την αλλαγή και μόνο των σχολικών εγχειριδίων, γίνεται επιβεβλημένη η χρήση του Διαδικτύου στη διδασκαλία, αφού έχει μπει στη διδακτική διαδικασία η χρήση πηγών του. Άλλωστε, δεν είναι πλέον λίγοι οι εκπαιδευτικοί που παίρνουν μόνοι τους την πρωτοβουλία να εισάγουν την τεχνολογία στην εκπαιδευτική διαδικασία και στο σχολικό περιβάλλον.

Ως προς τα θέματα της ασφάλειας του Διαδικτύου, το μεγαλύτερο ποσοστό των εκπαιδευτικών, εκτός των καθηγητών πληροφορικής, δε θεωρείται πως έχει τις κατάλληλες γνώσεις για την αντιμετώπιση του ζητήματος και άρα δεν είναι σε θέση να ενημερώσει και να συμβουλεύσει αρκούντως τους μαθητές. Ωστόσο, αρχίζουν να γίνονται μερικά βήματα προς την κατεύθυνση αυτή, περισσότερο με πρωτοβουλία ορισμένων ευαισθητοποιημένων εκπαιδευτικών και λιγότερο από τη μεριά της πολιτείας και ενός κεντρικού εκπαιδευτικού σχεδιασμού. Για το θέμα, πάντως, οι φορείς που εκπροσωπούν τους εκπαιδευτικούς υπογραμμίζουν ότι ο «χρησιμοθηρικός τρόπος» με τον οποίο είναι οργανωμένα τα μαθήματα στο σχολείο (αναλυτικό πρόγραμμα, τρόπος διδασκαλίας, εξετάσεις, βαθμοί, κ.λπ.), δεν αφήνει πολλά περιθώρια στους εκπαιδευτικούς να έχουν ικανοποιητική γνώση γύρω από το πρόβλημα της ασφάλειας, όπως και να αποκτήσουν εποικοδομητικό ρόλο για την αντιμετώπισή του.

4.2.3.1 Προτάσεις[77]

Για την εξασφάλιση της ασφαλούς πρόσβασης και της καλής χρήσης των υπηρεσιών του Διαδικτύου από τους μαθητές, και την αποτροπή τους από ανεπίτρεπτες συμπεριφορές, καταγράφονται κάποιες οδηγίες και προτάσεις που απευθύνονται ειδικά στους εκπαιδευτικούς:

[77] http://dide.ilei.sch.gr/keplinet/articles/saferinternet.php
Κατερέλος Ι., Παπαδόπουλος Π. (2009). *Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση*. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.37-38

- Οι εκπαιδευτικοί θα πρέπει να είναι ενημερωμένοι για το Διαδίκτυο, τις πολλές νέες δυνατότητες που παρέχει αλλά και τους κινδύνους που υπάρχουν. Να γνωρίζουν με τι ασχολούνται τα παιδιά στο Διαδίκτυο και με τι σκοπό το χρησιμοποιούν.
- Θα πρέπει να γνωρίζουν τις σχετικές συμβουλές ασφαλούς χρήσης προς τα παιδιά και προς τους γονείς, ώστε να μπορούν να συμβάλλουν και συμβουλευτικά στην αντιμετώπιση των κινδύνων από τη χρήση του Διαδικτύου.
- Θα πρέπει να επιβλέπουν τους μαθητές κατά τη χρήση του Διαδικτύου στο σχολικό εργαστήριο πληροφορικής. Με τις ενέργειες και το παράδειγμά τους μπορούν να προωθήσουν στην πράξη τις πρακτικές καλής χρήσης του Διαδικτύου.

Πρακτικά οι εκπαιδευτικοί μπορούν:

- Να κάνουν συζητήσεις με τους μαθητές τους στο επίπεδο της τάξης, και μια συμφωνία στη συνέχεια, για την χρήση του Διαδικτύου.
- Να διδάσκουν τους μαθητές να μη δίνουν ποτέ προσωπικά στοιχεία και πληροφορίες.
- Να επιβλέπουν πάντα τη χρήση των υπολογιστών με σύνδεση στο Διαδίκτυο από τους μαθητές τους.
- Να ελέγχουν τα Αγαπημένα (bookmarks) και το Ιστορικό (history) του προγράμματος φυλλομετρητή (browser) για να βλέπουν ποιες σελίδες επισκέπτονται οι μαθητές τους.
- Να δημιουργούν τη δική τους λίστα με προτεινόμενες σελίδες κατάλληλου περιεχομένου που θα αναδεικνύει τις ανθρώπινες αξίες και θα προάγει το γνωστικό και πνευματικό επίπεδο των μαθητών.

Αξίζει να σημειωθεί ότι σε έρευνα του Ινστιτούτου Οπτικοακουστικών Μέσων την περίοδο 2006-2007, το ποσοστό συμμετοχής (33%) των εκπαιδευτικών ήταν

αρκετά χαμηλό από το αναμενόμενο. Ωστόσο αυτό το φαινόμενο δεν είναι κάτι καινούργιο. Οι εκπαιδευτικοί είναι πολύ επιφυλακτικοί σε οποιαδήποτε έρευνα ακόμα κι αν προέρχεται από συναδέλφους τους (τις περισσότερες φορές αυτή είναι η περίπτωση). Σε παλαιότερες έρευνες έχει διαπιστωθεί ότι υπάρχουν δύο κυρίως αναφερόμενοι (από τους ίδιους τους εκπαιδευτικούς) λόγοι:

- Η πίστη στο ατελέσφορο των ερευνών που γίνονται. Κυριαρχεί η οπτική ότι τίποτα δεν μπορεί να αλλάξει στον ομολογουμένως τεράστιο αυτόν οργανισμό. Άρα, πρόκειται απλά για χαμένο χρόνο ή, ακόμα χειρότερα, για πρωτοβουλίες ορισμένων «δήθεν» ερευνητών με στόχο τις χρηματικές απολαβές που προκύπτουν για αυτούς.
- Η καχυποψία σχετικά με τα κίνητρα των ερευνητών. Πυκνά συχνά προκύπτουν δημοσιεύματα σε έντυπα ή και ηλεκτρονικά μέσα όπου παρουσιάζονται «έρευνες» που «αποδεικνύουν επιστημονικά» διάφορα χαρακτηριστικά στους εκπαιδευτικούς, μερικές φορές δε ακόμα και προσβλητικά. Έτσι, οι εκπαιδευτικοί παρουσιάζονται να «…παίρνουν κάτω από την βάση» ή να «…αδυνατούν να αντεπεξέλθουν στο έργο τους». Τέτοιου είδους κρίσεις θεωρούνται και είναι αρνητικές ως προς την ομαλή διεξαγωγή του έργου τους: οι μαθητές, που είναι οι έτεροι πρωταγωνιστές σε κάθε εκπαιδευτική σχέση, τους θεωρούν «αναξιόπιστους» ίσως και «ανίκανους» σε σχέση με το έργο τους. Επίσης, οι γονείς αρχίζουν να παρεμβαίνουν «δυναμικά» ακολουθώντας αυτή τη λογική και το απόλυτο επακόλουθο είναι μια χαοτική κατάσταση όπου, τελικά, η περισσότερη ενεργητικότητα τους διοχετεύεται στην επανόρθωση των διαπροσωπικών σχέσεων παρά στην μετάδοση γνώσης. Είναι λογικό λοιπόν, κάθε ερευνητική προσπάθεια να έχει μικρές πιθανότητες επιτυχίας, εφόσον θεωρείται εκ των προτέρων «ύποπτη» ως προς μια ενδεχόμενη «συκοφάντηση» της επαγγελματικής τους ταυτότητας.

Στα σχήματα που ακλουθούν, παρουσιάζονται οι απαντήσεις που έδωσαν 164 εκπαιδευτικοί, σε έρευνα του Ινστιτούτου Οπτικοακουστικών Μέσων το διάστημα 2006-2007.

Όπως φαίνεται στο Σχήμα 30 , πάνω από τους οκτώ στους δέκα εκπαιδευτικούς έχουν Διαδίκτυο στο σπίτι άρα, πέρα του σχολείου ενώ, όπως και οι γονείς (Σχήμα 19) στην συντριπτική πλειοψηφία τους πιστεύουν ότι το Διαδίκτυο είναι πλέον απαραίτητο (Σχήμα 31): περίπου 98% δηλώνει ότι είναι απαραίτητο (απαντήσεις «μάλλον απαραίτητο», «απαραίτητο» και «απολύτως απαραίτητο» μαζί).

Σχήμα 30 – Κατοχή Διαδικτύου στο σπίτι από εκπαιδευτικούς[78]

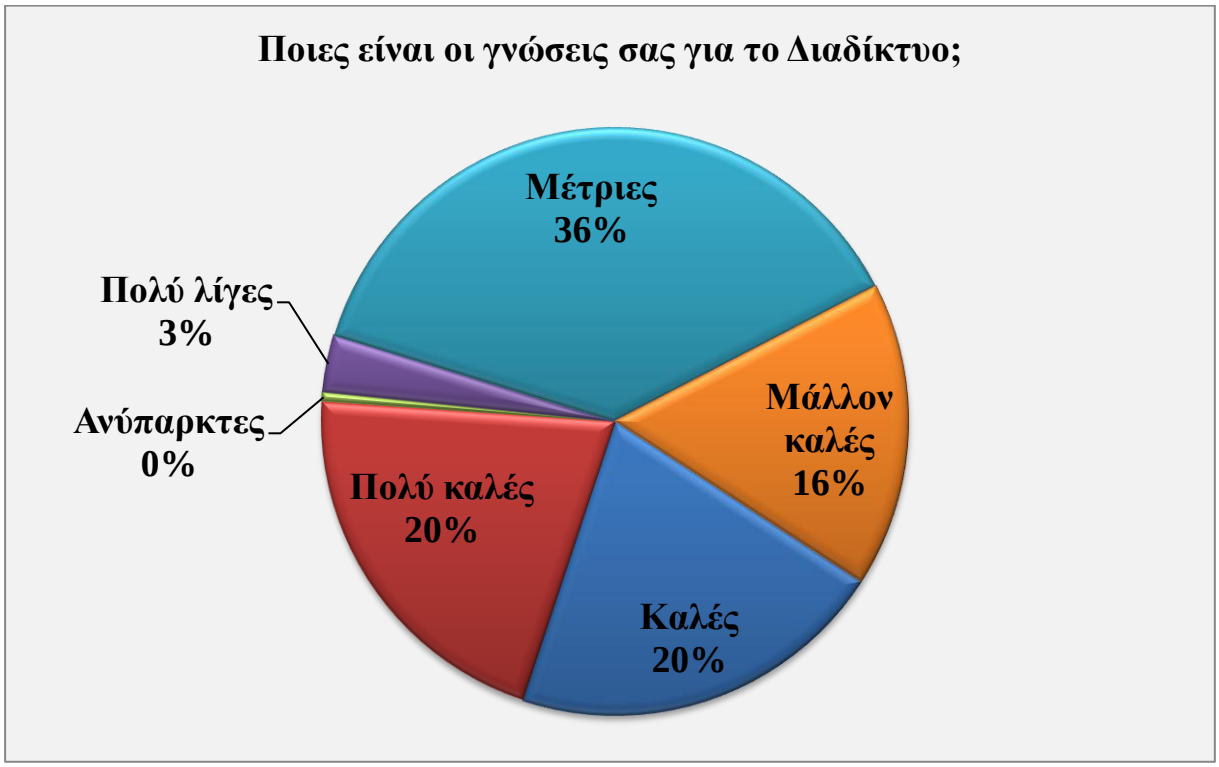
[78] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.389

Πρέπει να σημειωθεί, ότι οι εκπαιδευτικοί θεωρούν σε μεγαλύτερο ποσοστό ότι το Διαδίκτυο είναι απαραίτητο από ότι οι γονείς: σαφώς, η ευαισθητοποίηση σε σχέση με τις νέες τεχνολογίες είναι περισσότερη στους εκπαιδευτικούς.

Σχήμα 31 – Γνώμη εκπαιδευτικών για την χρησιμότητα του Διαδικτύου[79]

[79] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.389

Όπως φαίνεται στο Σχήμα 32, σχεδόν οι έξι στους δέκα εκπαιδευτικούς (56%) θεωρούν ότι έχουν επαρκείς γνώσεις σχετικά με το Διαδίκτυο (απαντήσεις «μάλλον καλές», «καλές» και «πολύ καλές» μαζί). Περίπου ο ένας στους τρεις (36%) δηλώνει «μέτριες» γνώσεις και μόλις το 8% δηλώνει ανεπάρκεια γνώσεων.

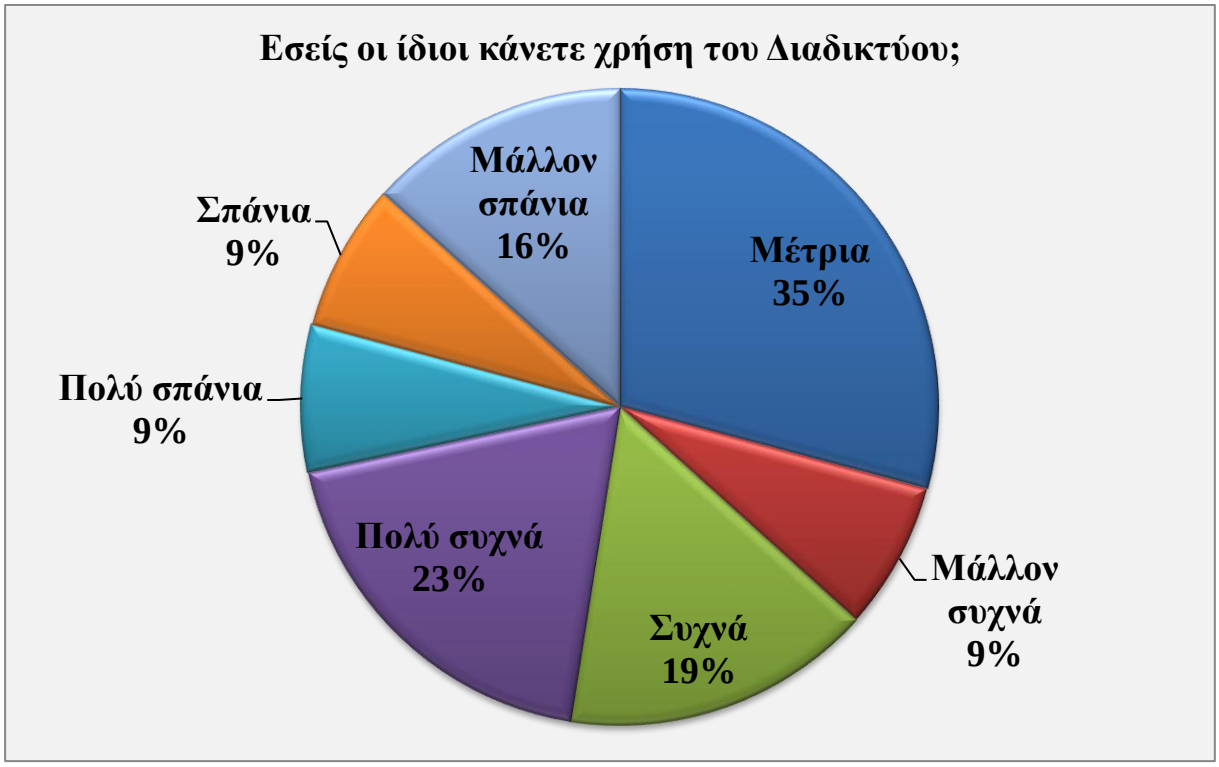


Σχήμα 32 – Γνώσεις εκπαιδευτικών για το Διαδίκτυο[80]

[80] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.390

Όπως φαίνεται στο

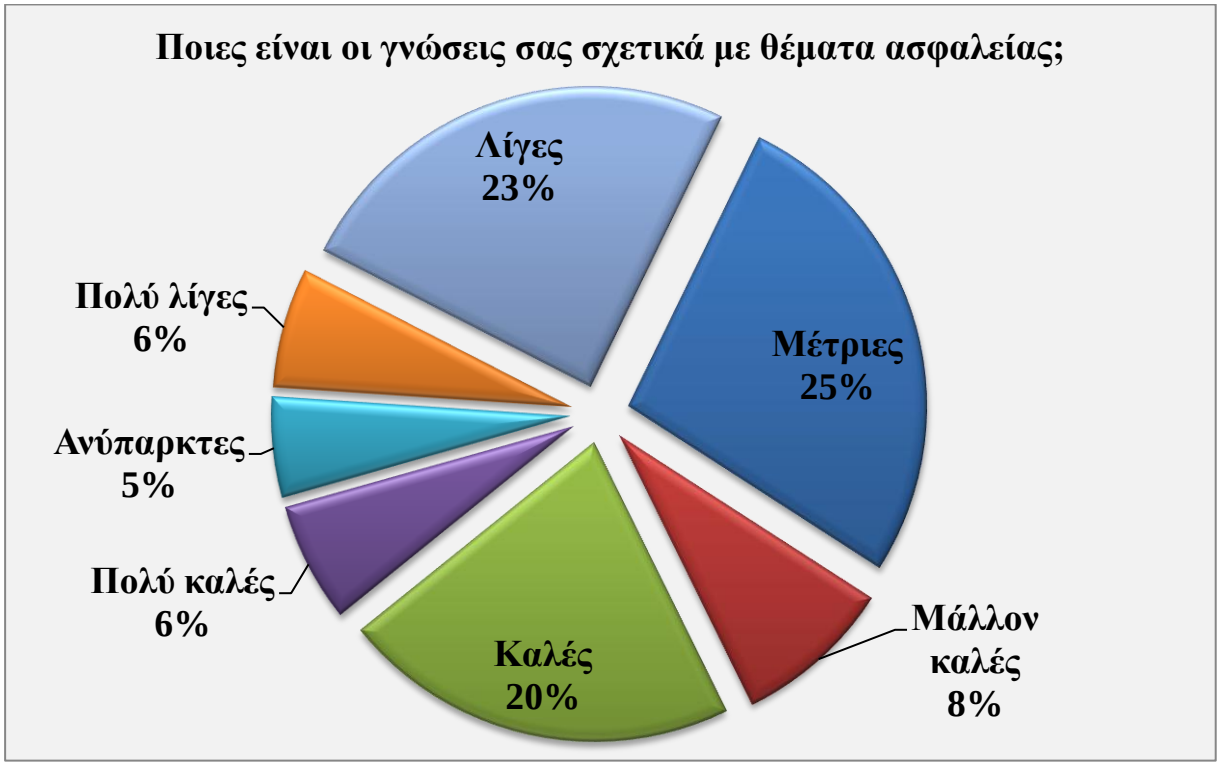
Σχήμα ***33***, πάνω από τους μισούς εκπαιδευτικούς (51%) δηλώνουν ότι χρησιμοποιούν το Διαδίκτυο από «μάλλον συχνά» έως «πολύ συχνά». Ο ένας στους τρεις το χρησιμοποιεί «μέτρια» (35%) και μόλις ένα 14% δηλώνει από «πολύ σπάνια» έως «μάλλον σπάνια» χρήση.



Σχήμα 33 – Χρήση του Διαδικτύου από εκπαιδευτικούς[81]

[81] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.390

Όμως και στις γνώσεις που αφορούν θέματα ασφάλειας στο Διαδίκτυο, οι εκπαιδευτικοί αναδίδουν μια εικόνα καλύτερη από αυτή των γονέων (Σχήμα 34): περίπου ο ένας στους τρεις δηλώνει επάρκεια γνώσεων (34%, απαντήσεις «μάλλον καλές», «καλές» και «πολύ καλές» μαζί)[82]. Εντούτοις, το ποσοστό αυτών που δηλώνουν «ανεπάρκεια» (απαντήσεις «λίγες», «πολύ λίγες» και «ανύπαρκτες» μαζί) είναι υψηλό: 41%. Οι «μέτριες» γνώσεις αφορούν περίπου τον ένα στους τέσσερις εκπαιδευτικούς.

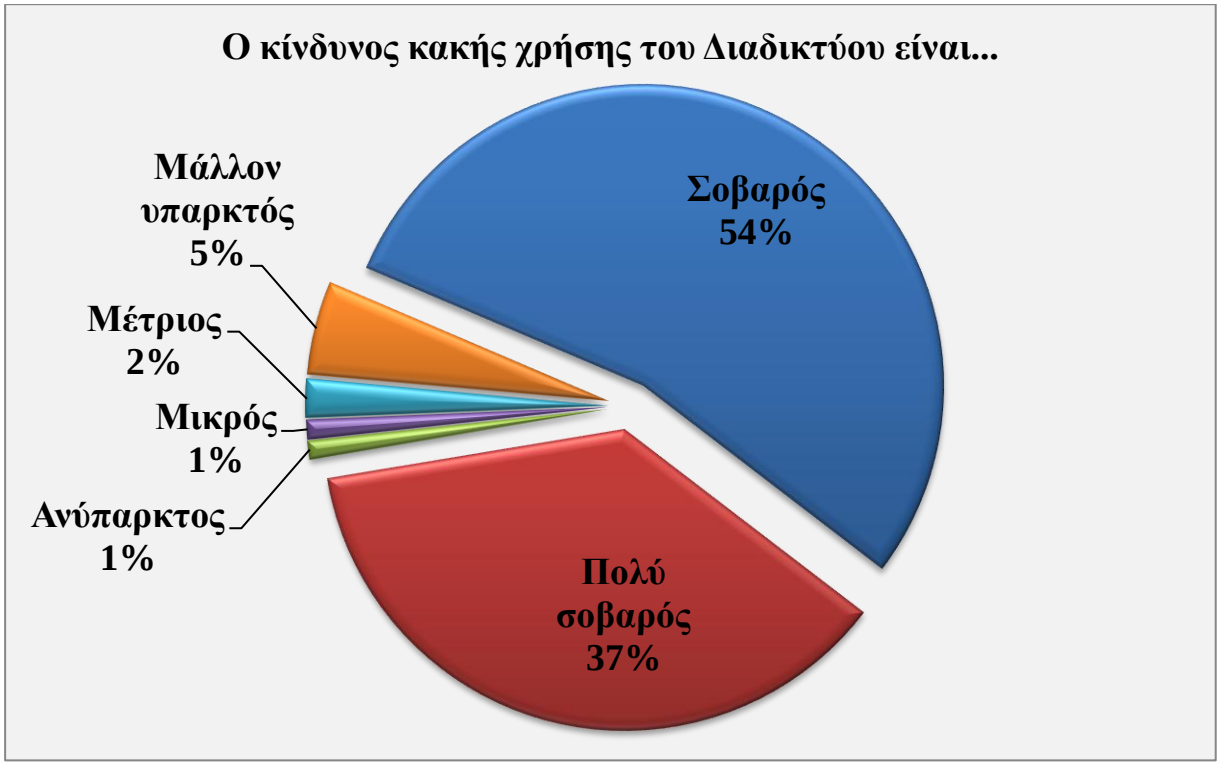


Σχήμα 34 – Γνώσεις εκπαιδευτικών σε θέματα ασφαλείας[83]

[82] Οι γονείς είχαν 27% στην ίδια κατηγορία

[83] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.391

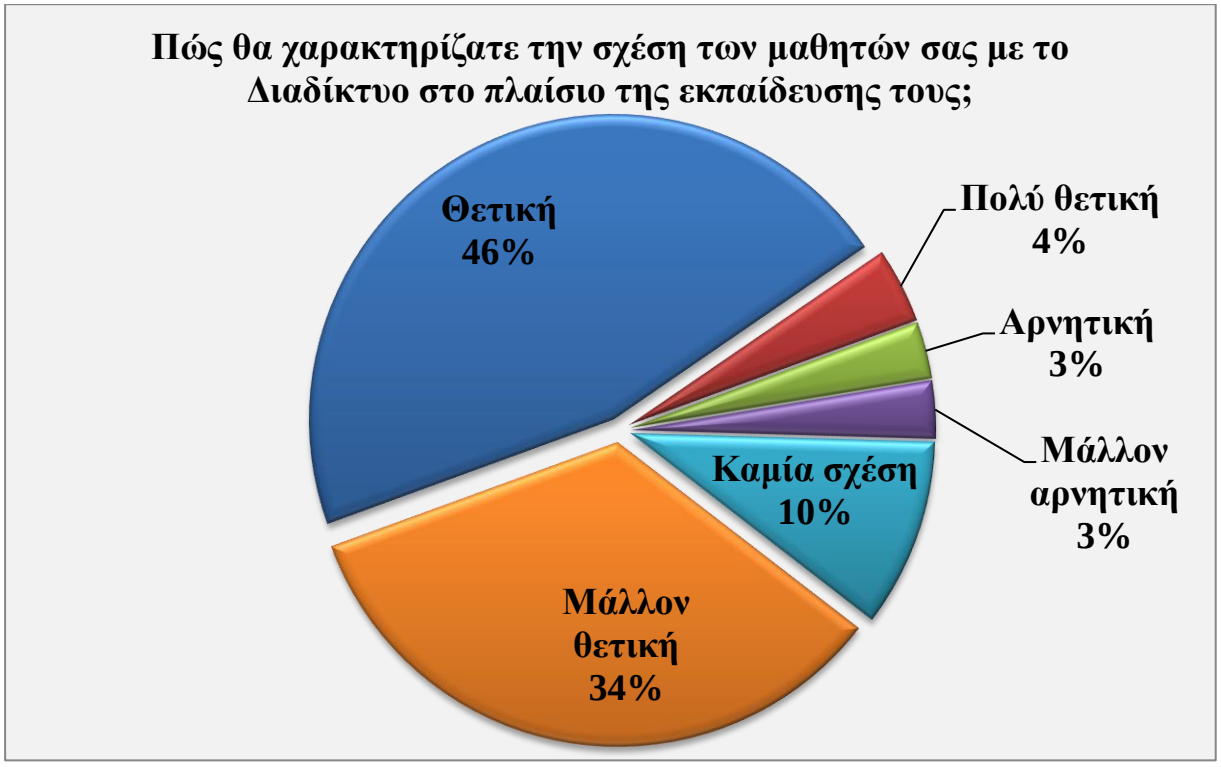
Στο Σχήμα 35 φαίνεται ότι οι εκπαιδευτικοί είναι πολύ ευαισθητοποιημένοι σε σχέση με την κακή χρήση του Διαδικτύου: το 91% δηλώνει ότι ο κίνδυνος κακής χρήσης είναι από «σοβαρός» έως «πολύ σοβαρός». Οι υπόλοιπες απαντήσεις απλά έχουν ποσοστά που δεν ξεπερνούν το 9% σε σύνολο.



Σχήμα 35 – Γνώμη εκπαιδευτικών τον κίνδυνο κακής χρήσης του Διαδικτύου[84]

[84] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.392

Εντούτοις, αν και έχουν πολύ σοβαρή αίσθηση του κινδύνου, περίπου οι 8 στους 10 (84%, Σχήμα 36) δηλώνουν ότι η σχέση των μαθητών με το Διαδίκτυο επηρεάζει θετικά («μάλλον θετικά», «θετικά» και «πολύ θετικά» μαζί) την εκπαίδευση τους.



Σχήμα 36 – Γνώμη εκπαιδευτικών για τη σχέση μαθητή - Διαδικτύου[85]

[85] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.392

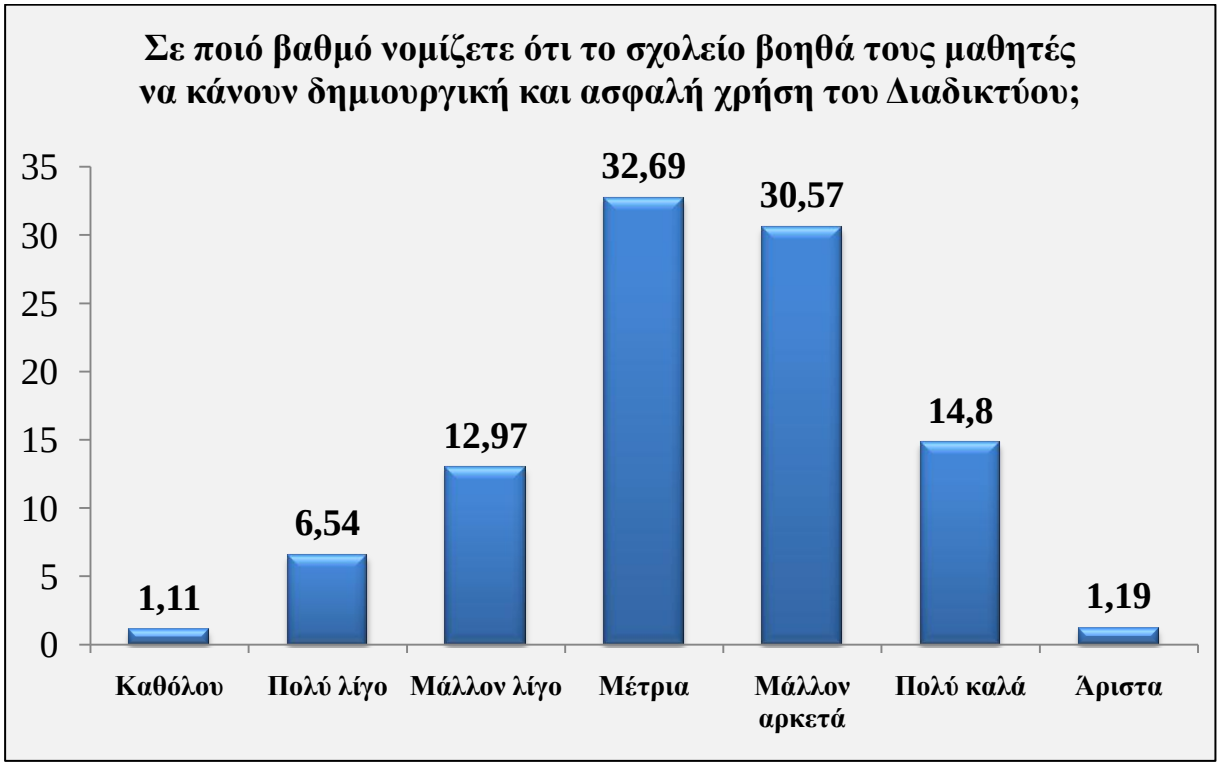
Σε ένα τέτοιο πλαίσιο θετικής αντίληψης σχετικά με την σχέση χρήσης Διαδικτύου και εκπαίδευσης των μαθητών, πάνω από οκτώ στους δέκα (82%) θεωρούν ότι τα σχολεία «πρέπει να συνδεθούν περισσότερο με το Διαδίκτυο και την χρήση υπολογιστών». Μόλις ένα 13% δηλώνει ότι «δεν χρειάζεται να συνδεθούν περισσότερο» και ένα 5% ότι «καλά είναι έτσι όπως είναι» (Σχήμα 37).

Σχήμα 37 – Γνώμη εκπαιδευτικών για τη σχέση σχολείου – Διαδικτύου[86]

[86] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.393

Σε ποιο βαθμό όμως θεωρούν ότι είτε οι ίδιοι (προσωπικά ως καθηγητές) είτε ο θεσμός (το σχολείο), βοηθούν τους μαθητές να κάνουν καλή και ασφαλή χρήση του Διαδικτύου; Στο Σχήμα 38 και στο Σχήμα 39 παρουσιάζονται οι απαντήσεις των εκπαιδευτικών τόσο για τους ίδιους, όσο και για τον θεσμό του σχολείου.

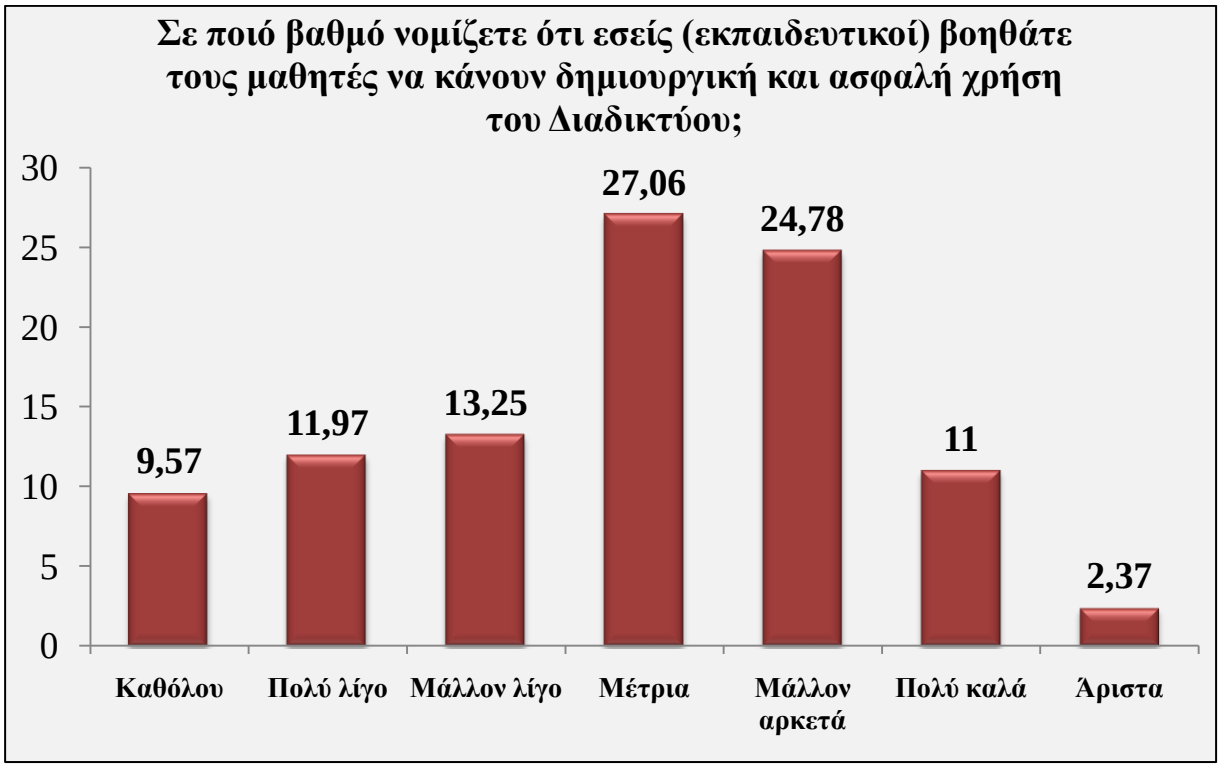
Όπως φαίνεται (Σχήμα 39), οι εκπαιδευτικοί αποδίδουν στον εαυτό τους μια μέτρια συνεισφορά στην δημιουργική και ασφαλή χρήση του Διαδικτύου ως προς τους μαθητές. Όσον αφορά τον σχολικό θεσμό (Σχήμα 38), πάλι του αποδίδουν μια «μέτρια» συνεισφορά, υπάρχει όμως μεγαλύτερη «συγκέντρωση» απαντήσεων στο «μέτρια» και στο «μάλλον αρκετά» απ' ότι στις απαντήσεις που αφορούν τους ίδιους.



Σχήμα 38 – Γνώμη εκπαιδευτικών για τη συνεισφορά του σχολείου στην δημιουργική και ασφαλή χρήση του Διαδικτύου[87]

[87] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.393

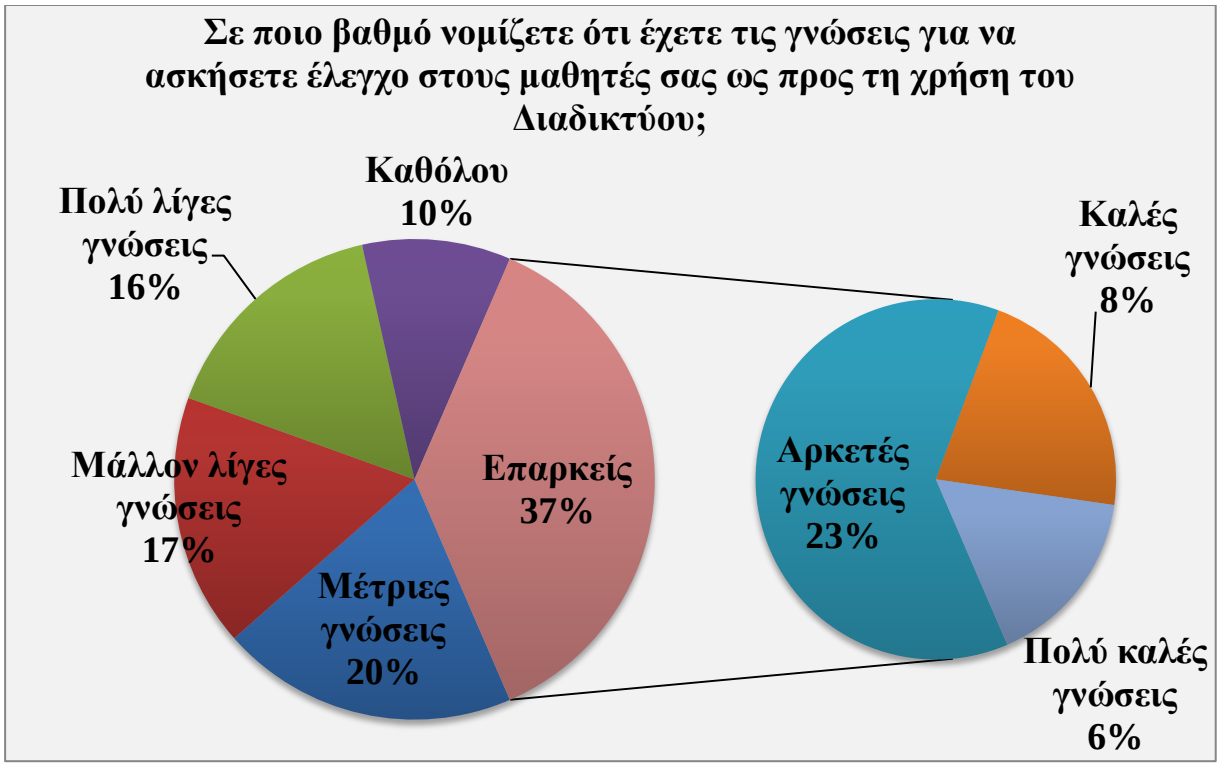
Επίσης, οι απαντήσεις που δηλώνουν «ανεπαρκή» συνεισφορά («καθόλου», «πολύ λίγο» και «μάλλον λίγο» μαζί) είναι περισσότερες όσον αφορά τους ίδιους τους εκπαιδευτικούς απ' ότι τον θεσμό του σχολείου (περίπου ο ένας στους τρεις (34,8%) θεωρεί ότι η συνεισφορά των εκπαιδευτικών είναι ανεπαρκής ενώ ο ένας στους πέντε (20,44%) θεωρεί την συνεισφορά του σχολείου ανεπαρκή. Συνεπώς, βγαίνει το συμπέρασμα, ότι ο εκπαιδευτικός θεωρεί ότι η συνεισφορά του είναι ελαφρά κατώτερη από αυτή του θεσμού τον οποίο υπηρετεί.



Σχήμα 39 – Γνώμη εκπαιδευτικών για τη συνεισφορά τους στην δημιουργική και ασφαλή χρήση του Διαδικτύου[88]

[88] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.393

Σε θέματα ασφάλειας, πάνω από το ένα τρίτο των εκπαιδευτικών (37%) δηλώνει ότι έχει επαρκείς (απαντήσεις «αρκετές γνώσεις», «καλές γνώσεις» και «πολύ καλές γνώσεις» μαζί) γνώσεις ώστε να ασκήσει έλεγχο στους μαθητές ως προς την χρήση του Διαδικτύου (Σχήμα 40). Πέραν του 20% που δηλώνει μέτριες γνώσεις, οι υπόλοιποι (43%), περίπου οι μισοί, θεωρούν ότι έχουν μάλλον ανεπαρκείς γνώσεις για να ασκήσουν έλεγχο στους μαθητές.



Σχήμα 40 – Γνώσεις εκπαιδευτικών για το Διαδίκτυο[89]

[89] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.394

Τα αποτελέσματα της προηγούμενης ερώτησης αναπαράγονται σχετικά με τον έλεγχο που ασκούν στους μαθητές σχετικά με το Διαδίκτυο. Στο Σχήμα 41 παρατηρείται ότι πάνω από ένας στους πέντε εκπαιδευτικούς ασκεί «ανύπαρκτο» έλεγχο στους μαθητές σχετικά με την χρήση του Διαδικτύου (21,7%). Περίπου ο ένας στους τρεις δηλώνει ότι ασκεί «μέτριο» έλεγχο (36,7%) ενώ από «μάλλον σφικτό» έως «πολύ αυστηρό» δηλώνει περίπου το 23%. Σαφώς, το μεγαλύτερο μέρος των εκπαιδευτικών (76,1%) θεωρεί ότι ο έλεγχος που ασκείται από αυτούς είναι από «ανύπαρκτος» μέχρι το πολύ «μέτριος» χωρίς να παραβλέπεται ότι το 91% των εκπαιδευτικών θεωρεί ότι ο κίνδυνος κακής χρήσης του Διαδικτύου είναι από «σοβαρός» έως και «πολύ σοβαρός» (Σχήμα 35).

Σχήμα 41 – Έλεγχος που ασκούν οι εκπαιδευτικοί στους μαθητές[90]

[90] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.394

Κρατώντας κατά νου μια τέτοια διαπίστωση, είναι ενδιαφέρον να εξεταστεί σε ποιο βαθμό προτρέπουν τους μαθητές να χρησιμοποιούν το Διαδίκτυο για εκπαιδευτικούς λόγους. Όπως παρουσιάζεται στο Σχήμα 42, το κύριο βάρος των εκπαιδευτικών δηλώνει ότι προτρέπει «αρκετά» έως «πάρα πολύ» (57,5%) τους μαθητές στο να χρησιμοποιούν το Διαδίκτυο. Περίπου ο ένας στους τέσσερις (26,16%) προτρέπει «ασθενώς» (απαντήσεις «καθόλου», «πολύ λίγο» και «λίγο» μαζί) και το 16,83% προτρέπει «μέτρια».

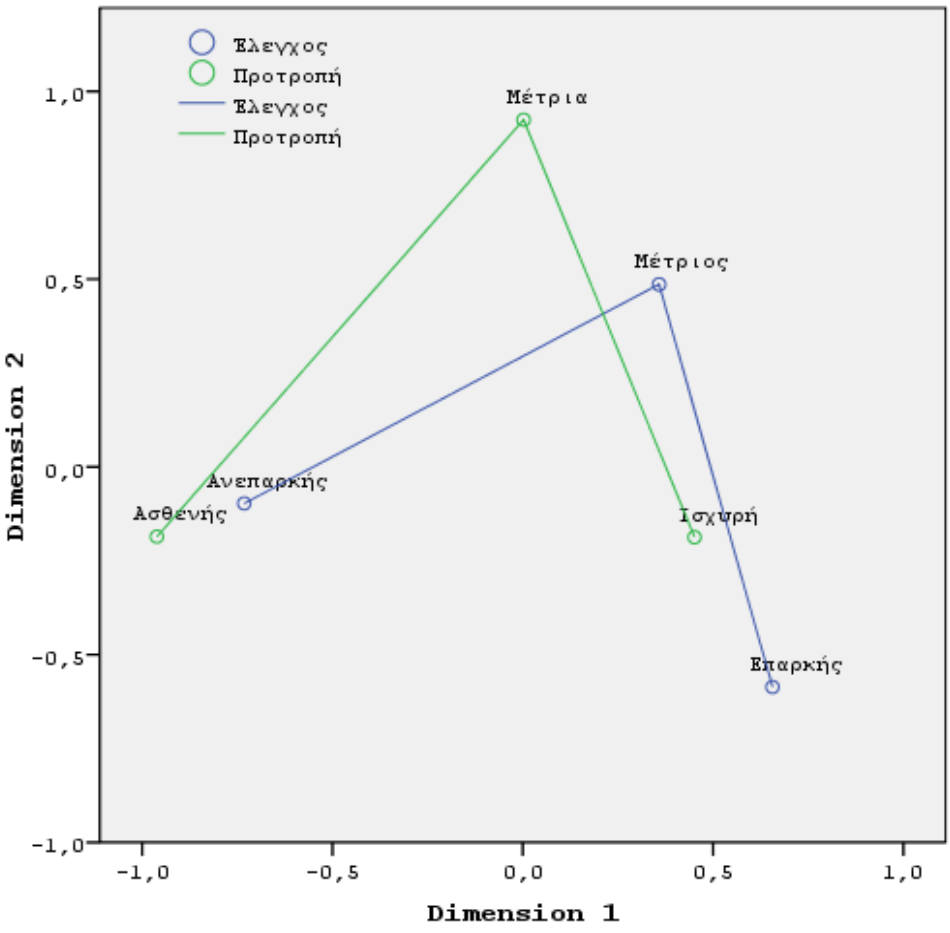
Σχήμα 42 – Παρότρυνση εκπαιδευτικών για χρήση του Διαδικτύου[91]

Το ερώτημα που προκύπτει μπορεί να διατυπωθεί ως εξής: εάν οι εκπαιδευτικοί νομίζουν ότι ο κίνδυνος χρήσης του Διαδικτύου είναι πολύ σοβαρός και, ταυτόχρονα ο έλεγχος που ασκούν στην χρήση του Διαδικτύου από τους μαθητές θεωρούν ότι είναι μάλλον ανεπαρκής, τότε πως πάνω από τους μισούς προτρέπουν τους μαθητές να χρησιμοποιούν το Διαδίκτυο για εκπαιδευτικούς λόγους;

[91] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.395

Με λίγα λόγια, το Διαδίκτυο μοιάζει να είναι σχεδόν ένα φοβικό αντικείμενο για τους εκπαιδευτικούς: σαφώς είναι κάτι το οποίο έχει μεγάλες δυνατότητες (εφόσον προτρέπουν στην χρήση του) αλλά, ταυτόχρονα, είναι και κάτι το οποίο «φοβούνται» (το 92% δηλώνει ότι ο κίνδυνος κακής χρήσης είναι σοβαρός) ενώ, συνολικά, δεν διατείνονται ότι μπορούν να το ελέγξουν στιβαρά.

Στο Σχήμα 43 βλέπει κανείς τις τάσεις που κυριαρχούν σε αυτήν την αντιφατική διατύπωση: αφού φτιάχτηκαν τρεις κατηγορίες απαντήσεων έναντι των αρχικών επτά, υποβλήθηκαν δύο ερωτήσεις σε ανάλυση αντιστοιχιών.



Σχήμα 43 – Ανάλυση Αντιστοιχιών στον βαθμό ελέγχου σχετικά με την ασφάλεια στο Διαδίκτυο και την προτροπή για την χρήση του Διαδικτύου σε εκπαιδευτικά πλαίσια[92]

[92] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.395

Παρατηρείται λοιπόν ότι οι εκπαιδευτικοί συνδέουν στενά τον έλεγχο που ασκούν στους μαθητές, με την προτροπή χρήσης του Διαδικτύου. Εάν ο εκπαιδευτικός θεωρεί ότι δεν μπορεί να ασκήσει επαρκή έλεγχο, τότε προτρέπει ασθενώς τους μαθητές στο να χρησιμοποιήσουν το Διαδίκτυο. Όσοι θεωρούν ότι μπορούν να ασκήσουν επαρκή έλεγχο αντίθετα, προτρέπουν ισχυρά τους μαθητές στην χρήση του Διαδικτύου. Επομένως, η οποιαδήποτε στρατηγική ενίσχυσης της χρήσης του Διαδικτύου από τους μαθητές, περνά αναγκαστικά από το προσλαμβανόμενο επίπεδο ελέγχου που έχουν οι εκπαιδευτικοί ως προς την χρήση του.

Στο Σχήμα 44 παρουσιάζεται η συχνότητα χρήσης του Διαδικτύου σχετικά με τα εκπαιδευτικά τους καθήκοντα. Παρατηρείται ότι περίπου το 40% το χρησιμοποιεί είτε «συχνά» είτε «πολύ συχνά». Περίπου ο ένας στους τρεις το χρησιμοποιεί μερικές φορές (35,5%) ενώ ο ένας στους τέσσερις μάλλον το χρησιμοποιεί από «ποτέ» μέχρι «σπάνια» (24,7%).

Σχήμα 44 – Χρήση Διαδικτύου από εκπαιδευτικούς για τα εκπαιδευτικά τους καθήκοντα[93]

[93] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.396

4.2.3.2 Η άποψη των εκπαιδευτικών[94]

Η Δράση Ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, πραγματοποίησε διαδικτυακή έρευνα για να συγκεντρώσει τις απόψεις των Ελλήνων εκπαιδευτικών, αναφορικά με τη διδασκαλία της ασφαλούς χρήσης του Διαδικτύου στα σχολεία. Η έρευνα πραγματοποιήθηκε την περίοδο Ιουνίου - Αυγούστου 2009 σε κλειστή λίστα εκπαιδευτικών ύστερα από πρόσκληση που απεστάλη με την πολύτιμη συμβολή και συνεργασία του Πανελλήνιου Σχολικού Δικτύου. Το ερωτηματολόγιο συμπλήρωσαν 679 εκπαιδευτικοί όλων των βαθμίδων από όλη την Ελλάδα.

Τα αποτελέσματα της έρευνας έχουν ως εξής:

- Το 99% των εκπαιδευτικών θεωρεί ότι η ασφαλής χρήση του Διαδικτύου πρέπει να διδάσκεται στο σχολείο.
- Η πρωτοβάθμια εκπαίδευση κρίνεται ως την πιο κατάλληλη βαθμίδα για να ξεκινήσει η εκπαίδευση στο Διαδίκτυο από το 70% των εκπαιδευτικών. Ένα ποσοστό 19% επιλέγει το Γυμνάσιο και ένα σημαντικό ποσοστό της τάξης του 11% θεωρεί ότι η εκπαίδευση στην ασφαλή χρήση του Διαδικτύου πρέπει να ξεκινά από το Νηπιαγωγείο.
- Αναφορικά με τη μορφή του μαθήματος, το 45% των εκπαιδευτικών θεωρεί ότι πρέπει να είναι ενσωματωμένο στο μάθημα της πληροφορικής, το 28% θεωρεί ότι πρέπει να είναι διαθεματικό, ενώ το 14% θεωρεί ότι πρέπει να έχει τη μορφή σεμιναρίου που θα λαμβάνει χώρα ανά τακτά διαστήματα. Μικρότερα ποσοστά (5%) συγκέντρωσαν επιλογές όπως: αυτόνομο με βαθμό και αυτόνομο χωρίς βαθμό.
- Τα πέντε πιο σημαντικά θέματα που θεωρούν ότι πρέπει να περιλαμβάνονται στην εκπαίδευση αυτή είναι:
    - Βασικές αρχές σωστής χρήσης του Διαδικτύου (72% των απαντήσεων)

[94] http://saferinternet.gr/index.php?parentobjId=Page75&p=20

- Προστασία προσωπικής ζωής (63%)
- Σωστή διαχείριση της επικοινωνίας μέσω Διαδικτύου (chat, forum, κ.λπ.) (57%)
- Αξιοπιστία διαδικτυακού περιεχομένου (44%)
- Αξιοποίηση της θετικής πλευράς του Διαδικτύου (41%)

- Το 81% των εκπαιδευτικών θεωρεί ότι χρειάζεται συνδυασμός εκπαιδευτικού υλικού (online και offline υλικό, επιμορφωτικά σεμινάρια και e-learning εφαρμογές) και όχι μεμονωμένες λύσεις ώστε να διδαχθεί ένα τέτοιο μάθημα.
- Στη ανοιχτή ερώτηση αναφορικά με τις ανάγκες των παιδιών σε σχέση με την εκπαίδευση στην ασφαλή χρήση του Διαδικτύου, οι εκπαιδευτικοί έδωσαν μεγάλη έμφαση στην ανάπτυξη της κριτικής ικανότητας και σκέψης, στην ανάπτυξη μηχανισμών αυτοπροστασίας, στην κατανόηση των κινδύνων, στην διαφύλαξη των προσωπικών δεδομένων, στη σωστή διαχείριση και χρήση διαδικτυακών μορφών επικοινωνίας και στην αξιοπιστία της διαδικτυακής πληροφορίας, τονίζοντας τη σημασία της βιωματικής εκπαίδευσης επάνω στα θέματα αυτά.
- Στην ερώτηση για τις αλλαγές που ενδεχομένως χρειάζεται να υλοποιηθούν στο Ελληνικό εκπαιδευτικό σύστημα ώστε να μπορέσει επιτυχώς να ενσωματωθεί στο σχολικό πρόγραμμα η εκπαίδευση της ασφαλούς χρήσης του Διαδικτύου, οι εκπαιδευτικοί επισήμαναν τις ανάγκες των σχολείων σε υλικοτεχνική υποδομή και ειδικότερα στην ανάγκη διασύνδεσής των σχολικών εργαστηρίων με το Διαδίκτυο σε διαρκή βάση. Πολλοί έκαναν λόγο για απαρχαιωμένα λειτουργικά συστήματα, για ελάχιστους υπολογιστές, ακόμα και για πλήρη απουσία εργαστηρίων. Τονίστηκε ακόμη, η ανάγκη ουσιαστικής επιμόρφωσης των εκπαιδευτικών που θα κληθούν να αναλάβουν ένα τέτοιου είδους μάθημα. Πολλοί ήταν οι εκπαιδευτικοί που αναφέρθηκαν στην ανάγκη

εισαγωγής του μαθήματος της πληροφορικής στο Δημοτικό καθώς πλέον τα παιδιά αποκτούν υπολογιστή πολύ νωρίτερα από ότι ξεκινούν τα μαθήματα πληροφορικής στο σχολείο. Τέλος, αρκετοί ζητούν την αύξηση των ωρών διδασκαλίας της πληροφορικής σε όλες τις βαθμίδες με τη χρήση του Διαδικτύου κατά τη διάρκεια όλων των μαθημάτων (διαθεματική προσέγγιση).

- Τέλος, αν και η πλειοψηφία των εκπαιδευτικών δεν θεωρεί ότι υπάρχουν ειδικές συνθήκες που διαφοροποιούν τα Ελληνόπουλα από τους μαθητές άλλων Ευρωπαϊκών χωρών, επισημαίνοντας ότι τα ζητήματα της ασφάλειας στο Διαδίκτυο είναι ως ένα βαθμό κοινά, αρκετοί εκπαιδευτικοί τονίζουν ότι η χαμηλή διείσδυση του Διαδικτύου στην Ελλάδα, καθώς και ο ψηφιακός αναλφαβητισμός γονέων και πολλών εκπαιδευτικών, αποτελούν τροχοπέδη στη σωστή και έγκαιρη εκπαίδευση.

4.3 Internet café[95]

Τα Internet café είναι ένας πολύ διαδεδομένος χώρος για παιδιά και εφήβους διότι σε αυτά έχουν την δυνατότητα να πλοηγηθούν στο Διαδίκτυο, αλλά και να παίξουν ηλεκτρονικά παιχνίδια χωρίς την επίβλεψη των γονιών τους και γενικότερα κάποιου ενήλικα.

Τη διαμόρφωση νομοθετικού πλέγματος σχετικά με τη λειτουργία των καταστημάτων Internet café, ώστε να προστατεύονται τα δικαιώματα των ανηλίκων που έχουν πρόσβαση σε αυτά, ζητάει από τα αρμόδια υπουργεία ο Συνήγορος του Παιδιού. Η ανεξάρτητη αρχή έλαβε σειρά αναφορών σχετικά με το ότι μεγάλος αριθμός ανηλίκων - σε πολλές περιπτώσεις κάτω των 12 ετών - κυρίως στην περιφέρεια παραμένουν πολλές ώρες σε Internet Cafe, διατρέχοντας έτσι σοβαρούς κινδύνους για τη σωματική και ψυχική τους υγεία,

[95] http://www.ethnos.gr/article.asp?catid=11424&subid=2&pubid=25694949

αφού συνήθως δεν υπάρχει έλεγχος των πληροφοριών, των εικόνων ή των παιχνιδιών στα οποία έχουν πρόσβαση.

Ο Συνήγορος του Παιδιού, αφού διαπίστωσε ότι δεν υπάρχουν νομοθετικές προβλέψεις για την είσοδο και χρήση υπηρεσιών από ανηλίκους στα συγκεκριμένα καταστήματα, ανέλαβε την πρωτοβουλία να θέσει το θέμα σε δημόσια διαβούλευση εστιάζοντας την προσοχή του ταυτόχρονα και στα δικαιώματα συμμετοχής και στα δικαιώματα προστασίας των παιδιών.

Ο Συνήγορος του Παιδιού είναι αντίθετος με μια γενική απαγόρευση της πρόσβασης ανηλίκων στα εν λόγω καταστήματα και της χρήσης των υπηρεσιών τους, οι οποίες - υπό προϋποθέσεις - μπορεί να αξιοποιούνται θετικά για την εκπαίδευση, ενημέρωση, επικοινωνία και ψυχαγωγία τους.

Ωστόσο, κρίνει ότι πρέπει να ληφθούν κατάλληλα μέτρα προστασίας των ανήλικων χρηστών, έτσι ώστε να αποκομίζεται το μέγιστο των ωφελημάτων με το ελάχιστο της διακινδύνευσης της ψυχοσωματικής υγείας και ομαλής ανάπτυξης και εξέλιξής τους.

Σε αυτό το πλαίσιο θέτει έξι βασικά μέτρα προστασίας, στα οποία καλούνται να τοποθετηθούν οι συμμετέχοντες στον διάλογο φορείς. Συγκεκριμένα ζητάει:

- Καθιέρωση της υποχρεωτικής έγγραφης έγκρισης των γονέων/κηδεμόνων των ανηλίκων κάτω των 14 χρόνων για την πρόσβαση στα Internet café και τη χρήση των υπηρεσιών τους.
- Απαγόρευση της πρόσβασης σε αυτά κάτω των 16 χρόνων κατά τις μεταμεσονύκτιες ώρες.
- Καθιέρωση συστήματος χρονοχρέωσης για ανηλίκους, με μέγιστο χρόνο χρήσης υπηρεσιών την ημέρα (ανά 24ωρο).
- Θεσμοθέτηση ειδικής διαδικασίας ελέγχου για την εφαρμογή και τήρηση της νομοθεσίας στα καταστήματα Internet café.
- Καθιέρωση κριτηρίων και διαδικασίας πιστοποίησης καταστημάτων «φιλικών στα παιδιά», με κατάλληλο πλαίσιο και περιβάλλον χρήσης για

ανηλίκους (π.χ. αυτοδέσμευση μέσω κώδικα δεοντολογίας, με χρήση φίλτρων, απαγόρευση καπνίσματος, ξεχωριστούς χώρους για ανηλίκους, παρουσία και επίβλεψη από κατάλληλα εκπαιδευμένους ενηλίκους κ.ά.).

- Εκστρατείες ενημέρωσης, ιδίως με τηλεοπτικά και ραδιοφωνικά μηνύματα, για την εφαρμογή όλων των μέτρων που τελικά θα ληφθούν σε τοπικό και πανελλαδικό επίπεδο.

4.4 Πάροχοι υπηρεσιών Διαδικτύου[96]

Σε ότι αφορά, επίσης, την καταπολέμηση του αναλφαβητισμού στην Ελλάδα γύρω από τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.), καθώς και την ευαισθητοποίηση του ευρύτερου κοινού γύρω από τα θέματα ασφάλειας στο Διαδίκτυο, ορισμένους ρόλους μπορούν να παίξουν και οι εταιρίες παροχής υπηρεσιών Διαδικτύου (ISPs), όπως αναγνωρίζουν και οι ίδιες. Αυτό πρώτα απ' όλα μπορεί να συμβεί με τη φθηνότερη παροχή εκ μέρους τους τέτοιων υπηρεσιών στο γενικό πληθυσμό. Επιπλέον, στα πλαίσια μιας «εταιρικής κοινωνικής ευθύνης» που πρέπει να διακρίνει σύγχρονες επιχειρήσεις αυτού του είδους και μεγέθους, οι ISPs δύνανται και οι ίδιες να αναλάβουν πρωτοβουλίες επιμόρφωσης ομάδων του πληθυσμού σε θέματα Τ.Π.Ε. και ενημέρωσής τους για τα ζητήματα ασφάλειας στη χρήση του Διαδικτύου. Ειδικά στο τελευταίο, μπορούν να παράσχουν την τεχνογνωσία αλλά και την τεχνολογική υποδομή τους για την υποστήριξη των σχετικών πληροφοριακών εκστρατειών.

Οι ISPs μπορούν επίσης να συνδράμουν στη δημιουργία επαγρύπνησης του κοινού αλλά και στην προστασία των χρηστών από ακατάλληλο υλικό. Οι ISPs, έχοντας την απαραίτητη τεχνογνωσία αλλά και πρόσβαση σε ένα ευρύ φάσμα του κοινού μέσω των υπηρεσιών που προσφέρουν, οφείλουν να κάνουν τις απαραίτητες ενέργειες για την προώθηση των πρωτοβουλιών που αναπτύσσονται στον τομέα της ασφαλούς χρήσης του Διαδικτύου.

[96] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.192, 233-234
http://www.microsoft.com/hellas/athome/security/children/kidsafetyfaq.mspx
http://www.e-yliko.gr/htmls/pc_use/snav2.aspx

Συγκεκριμένα μπορούν να παράσχουν την τεχνογνωσία αλλά και την τεχνολογική υποδομή τους για την υποστήριξη των πληροφοριακών εκστρατειών.

Ένας καλός παροχέας μπορεί να προσφέρει:

- φιλτράρισμα των ιστοσελίδων που επισκέπτεται ο χρήστης - πελάτης
- φιλτράρισμα των e-mail που δέχεται ο χρήστης-πελάτης

Ο χρήστης χρειάζεται να επιλέξει μια υπηρεσία παροχής Διαδικτύου που διαθέτει κατάλληλες πολιτικές χρήσης που απαγορεύουν την παρενόχληση, που εφαρμόζει αυστηρή πολιτική σε θέματα ασφάλειας και που προσπαθεί να εμποδίσει την ανεπιθύμητη αλληλογραφία.
Σχετικά με την ηλεκτρονική παρενόχληση των παιδιών στο Διαδίκτυο, εάν η παρενόχληση οφείλεται σε σχόλια που εμφανίζονται σε κάποια διαδικτυακή τοποθεσία, ο χρήστης μπορεί να επικοινωνήσει με τον παροχέα και να ζητήσει βοήθεια για να εντοπίσει τον ISP που φιλοξενεί τη διαδικτυακή τοποθεσία. Μπορεί, στη συνέχεια, να επικοινωνήσει με τον παροχέα και να τον ενημερώσει για τα σχόλια.

4.5 Μέσα Μαζικής Ενημέρωσης[97]

Σημαντικός μπορεί να αποβεί ο ενημερωτικός ρόλος των Μ.Μ.Ε. ειδικά σε ότι αφορά τα θέματα ασφάλειας του Διαδικτύου. Και στην Ελλάδα, όπως σε άλλες ευρωπαϊκές χώρες, μπορούν να αναπτυχθούν καμπάνιες με σύντομα σποτ στην τηλεόραση, τους κινηματογράφους, καθώς και καταχωρήσεις στα γραπτά μέσα, που να παρακινούν το ενδιαφέρον μικρών και μεγάλων για τα θέματα ασφάλειας, όταν χρησιμοποιούν τον ηλεκτρονικό υπολογιστή και όταν πλοηγούνται στον παγκόσμιο ιστό. Ήδη μια περιορισμένη τέτοια εκστρατεία

[97] Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.233, 234

ξεκίνησε από τις αρχές του φθινοπώρου 2007 στη δημόσια ραδιοτηλεόραση, με τη συμμετοχή των αρμόδιων φορέων Saferinternet και Safeline.

Επιπλέον, μέχρι σήμερα τα Μ.Μ.Ε έχουν παίξει ένα ρόλο εγρήγορσης των θεατών, ακροατών και αναγνωστών τους στον τομέα αυτό, φέρνοντας στο φως ορισμένες σοβαρές περιπτώσεις παραβίασης της ασφάλειας κατά τη χρήση του Διαδικτύου, εκμετάλλευσης παιδιών μέσω αυτού και έως και διενέργειας ηλεκτρονικών εγκλημάτων. Όμως, μερικές φορές υπάρχει μια τάση μεγαλοποίησης τέτοιων προβλημάτων ασφάλειας από τα Μ.Μ.Ε. Έτσι, εξαιτίας αρνητικά φορτισμένων ρεπορτάζ των Μ.Μ.Ε., οι γονείς φτάνουν στο σημείο να δαιμονοποιούν το Διαδίκτυο και σε κάποιες περιπτώσεις να στερούν από τα παιδιά τους ένα ιδιαίτερα χρήσιμο εργαλείο. Επιπλέον, με ανακριβή ρεπορτάζ υψηλών τόνων και με αδόκιμες καμπάνιες ενημέρωσης για θέματα ασφάλειας, ελλοχεύει ο κίνδυνος να γίνει διαφήμιση αντί για δυσφήμιση αυτών των αρνητικών πτυχών του Διαδικτύου.

5. ΛΟΓΙΣΜΙΚΟ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΓΟΝΙΚΟΥ ΕΛΕΓΧΟΥ

Στο προηγούμενο κεφάλαιο μελετήθηκε και παρουσιάστηκε ο ρόλος των ενήλικων στην προστασία των ανήλικων χρηστών από τους κινδύνους του Διαδικτύου. Η προστασία αυτή περιλάμβανε περισσότερο την πρόληψη, την σωστή πληροφόρηση, τον διάλογο και την σχέση εμπιστοσύνης μεταξύ των ανηλίκων και ενηλίκων χρηστών.

Στο παρόν κεφάλαιο παρουσιάζεται το λογισμικό προστασίας που μπορεί να χρησιμοποιηθεί για την «υγεία» του ηλεκτρονικού υπολογιστή, αλλά και το λογισμικό γονικού ελέγχου το οποίο επιτρέπει στους γονείς να ελέγχουν την πλοήγηση των παιδιών στο Διαδίκτυο.

Παρόλα αυτά, το λογισμικό γονικού ελέγχου δεν πρέπει να χρησιμοποιείται ως βασική προστασία, αλλά ως συμπληρωματική. Σκοπός του δεν είναι ο περιορισμός ή η απαγόρευση ενός τόσο χρήσιμου εργαλείου όπως το Διαδίκτυο, αλλά η προσφορά βοήθειας σε γονείς και καθηγητές ώστε να ελέγξουν τις δραστηριότητές των παιδιών και να προλάβουν τυχόν προβλήματα που μπορούν να δημιουργηθούν.

5.1 Λογισμικό antivirus[98]

Τα προγράμματα antivirus χρησιμοποιούνται για την πρόληψη, την ανίχνευση και απομάκρυνση του κακόβουλου λογισμικού, συμπεριλαμβανομένων ιών, σκουληκιών και δούρειων ίππων. Τα προγράμματα αυτά μπορούν επίσης να αποτρέψουν και να καταργήσουν λογισμικό υποκλοπής (spyware) , λογισμικό ανεπιθύμητων διαφημίσεων (adware), και άλλες μορφές κακόβουλου λογισμικού.

Η αντιμετώπιση των ιών έχει δύο σκέλη: τον εντοπισμό του ιού και την απάλειψη του. Τα προγράμματα antivirus πραγματοποιούν έλεγχο των αρχείων ενός υπολογιστή για τον εντοπισμό μολυσματικού λογισμικού. Τα αρχεία αυτά

[98] http://en.wikipedia.org/wiki/Antivirus_software
http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf

μπορεί να είναι αρχεία δεδομένων, αρχεία συστήματος, ή αρχεία εφαρμογών. Επίσης, μπορεί να είναι αποθηκευμένα σε κάποια μονάδα βοηθητικής μνήμης ή να εισέρχονται στο σύστημα μέσω δικτύου (LAN, Internet).

5.1.1 Ανίχνευση κώδικα ιού

Ο κώδικας κάθε ιού έχει ορισμένα χαρακτηριστικά που τον διαφοροποιούν από τους υπόλοιπους ιούς. Το τμήμα εκείνο του κώδικα ενός ιού που χαρακτηρίζει μοναδικά τον ιό ονομάζεται υπογραφή ή αποτύπωμα του ιού. Ένα πρόγραμμα antivirus τηρεί μια βάση δεδομένων με τις υπογραφές όλων των γνωστών ιών, και ελέγχει όλα τα εκτελέσιμα αρχεία ενός Η/Υ (κατά την αποθήκευση ή εκτέλεση τους) για τον εντοπισμό μιας υπογραφής που έχει ήδη αποθηκευτεί στη βάση δεδομένων. Εφόσον βρει κάποιο «ταίριασμα» (matching), το πρόγραμμα antivirus μπλοκάρει την εκτέλεση του κακόβουλου προγράμματος και ενημερώνει το χρήστη. Συνήθως προτρέπει το χρήστη να αποφασίσει αν επιθυμεί

- διαγραφή (delete)
- απομόνωση (isolation, quarantine)
- επιδιόρθωση (repair, clean) του μολυσμένου αρχείου.

5.1.2 Βασικά στοιχεία που πρέπει να έχει ένα λογισμικό antivirus:[99]

Εύχρηστο Interface και χαμηλή κατανάλωση πόρων: Το περιβάλλον της εφαρμογής πρέπει να είναι λιτό, και φιλικό προς τον χρήστη. Πολλά παράθυρα και πολύπλοκες ρυθμίσεις, μπορούν να έχουν εντελώς αντίθετα αποτελέσματα και να θέσουν σε ρίσκο την ασφάλεια του συστήματος. Επίσης, ένα πρόγραμμα antivirus θα πρέπει να προσφέρει τις υπηρεσίες του, δεσμεύοντας μικρό μόνο ποσοστό από τους πόρους του υπολογιστή (μνήμη και υπολογιστική δύναμη).

Προστασία σε πραγματικό χρόνο: Τα προγράμματα antivirus συνήθως διαθέτουν ένα υποσύστημα διάγνωσης και προστασίας σε πραγματικό χρόνο (real-time protection). Το antivirus φορτώνεται στην κεντρική μνήμη κατά την

[99] http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf

εκκίνηση του Η/Υ και λειτουργεί στο παρασκήνιο (background), ελέγχοντας τη μνήμη του συστήματος, καθώς και τα αρχεία και τις εφαρμογές που εκτελούνται ή εισέρχονται στο σύστημα για την ύπαρξη κακόβουλου λογισμικού.

Αυτόματη ενημέρωση: Σε αντίθεση με το παρελθόν, όπου τη διαδικασία ενημέρωσης την εκκινούσε ο χρήστης χειρωνακτικά, σήμερα τα προγράμματα antivirus ενημερώνουν αυτόματα τη βάση δεδομένων τους με τις πρόσφατες υπογραφές των ιών (virus definitions). Η ενημέρωση θα πρέπει να είναι τακτική (ο αποδεκτός σήμερα ρυθμός ενημέρωσης είναι της τάξης των λίγων ημερών), με δεδομένο ότι καθημερινά εμφανίζονται καινούριοι ιοί.

Προστασία ηλεκτρονικής αλληλογραφίας: Το antivirus ελέγχει τα εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικής αλληλογραφίας για την ύπαρξη ιών (στα συνημμένα έγγραφα). Για να συμβεί αυτό, το πρόγραμμα θα πρέπει να συνεργάζεται με τα πλέον δημοφιλή προγράμματα ηλεκτρονικής αλληλογραφίας.

Προγραμματισμένος έλεγχος: Το antivirus επιτρέπει τον καθορισμό (scheduling) προγραμματισμένων ελέγχων στους δίσκους του συστήματος, σε συγκεκριμένη ημερομηνία ή ανά τακτά χρονικά διαστήματα.

Δισκέτα εκκίνησης: Για την αντιμετώπιση των ιών τύπου boot sector, ή για την αντιμετώπιση περιπτώσεων όπου η εκκίνηση του λειτουργικού συστήματος. είναι αδύνατη, συνήθως τα προγράμματα antivirus προσφέρουν τη δυνατότητα δημιουργίας μιας δισκέτας εκκίνησης. Η δισκέτα αυτή ενσωματώνει εφαρμογές διάγνωσης και καθαρισμού του boot sector ή / και (κρίσιμων) αρχείων συστήματος, σε περίπτωση που αυτά έχουν επικαλυφθεί (overwrite) από κακόβουλο λογισμικό.

Καταγραφή συμβάντων (event logging): Τα αρχεία καταγραφής συμβάντων είναι ειδικά αρχεία που καταγράφουν σημαντικά συμβάντα στον υπολογιστή, όπως όταν ένας χρήστης συνδέεται στον υπολογιστή ή όταν κάποιο πρόγραμμα παρουσιάζει σφάλμα. Οποτεδήποτε εμφανίζονται αυτοί οι τύποι συμβάντων, το antivirus καταγράφει τα συμβάντα σε ένα αρχείο καταγραφής που μπορεί να

διαβαστεί χρησιμοποιώντας το πρόγραμμα προβολής συμβάντων. Οι προχωρημένοι χρήστες μπορεί να βρουν χρήσιμες τις λεπτομέρειες που περιέχονται στα αρχεία καταγραφής συμβάντων κατά την αντιμετώπιση προβλημάτων.

5.2 Τείχος προστασίας[100]

Στην επιστήμη των υπολογιστών ο όρος τείχος προστασίας (firewall) χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Το τείχος προστασίας είναι από τα σπουδαιότερα και πιο διαδεδομένα μέσα δικτυακής προστασίας για την ασφαλή λειτουργία του υπολογιστή. Αποτελούν τα πλέον αναγκαία αλλά και αποτελεσματικά μέτρα για την προστασία μεμονωμένων υπολογιστών και ολόκληρων δικτύων απέναντι στους κινδύνους που παραμονεύουν στο Διαδίκτυο.

Ένα τείχος προστασίας μπορεί να ελέγξει την κίνηση των πακέτων του Διαδικτύου από και προς τον υπολογιστή. Μπορεί να εντοπίσει τις πιθανές επιθέσεις στον υπολογιστή, να αναλύσει την κίνηση και τα αρχεία που ανταλλάσσονται, να διακρίνει τις ύποπτες δραστηριότητες και να εμποδίσει την ολοκλήρωσή τους. Προστατεύει ένα δίκτυο από κάποιο άλλο δίκτυο, υποβάλλοντας τα διερχόμενα πακέτα πληροφοριών (εισερχόμενα και εξερχόμενα) σε μια σειρά από ελέγχους και λαμβάνει την απόφαση να τα αφήσει να διέλθουν ή να τα εμποδίσει, ανάλογα με το αν περνούν κάποια τεστ ή όχι. Στην ουσία πρόκειται για έναν ελεγκτή κυκλοφορίας δεδομένων στο Διαδίκτυο.

Ένα τείχος προστασίας μπορεί επίσης να ελέγξει τα προγράμματα που είναι εγκατεστημένα στον ίδιο τον υπολογιστή και συνδέονται στο Διαδίκτυο και τα οποία στέλνουν προς τα έξω ευαίσθητα προσωπικά δεδομένα ή αφήνουν

[100] http://el.wikipedia.org/wiki/Firewall
http://pcex.gr/pc/index.php?option=com_content&task=view&id=30&Itemid=43

ανοικτή μια κερκόπορτα (backdoor) για να μπορούν οι πιθανοί hackers να ελέγξουν τον υπολογιστή. Το τείχος προστασίας μπορεί να κρατήσει κλειστές αυτές τις πόρτες και να ενημερώνει για κάθε ύποπτη κίνηση.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

Πέρα από τους ιούς και τα συναφή προγράμματα, ένας υπολογιστής που συνδέεται στο Διαδίκτυο χωρίς τείχος προστασίας είναι εκτεθειμένος σε ένα σωρό απειλές. Ένας καλός γνώστης δικτύων και σε συνδυασμό με τα κατάλληλα προγράμματα – εργαλεία, μπορεί πολύ εύκολα να εξαπολύσει διάφορες επιθέσεις σε έναν υπολογιστή που δεν έχει τείχος προστασίας.

Η εύρεση ενός καλού και αξιόπιστου τείχους προστασίας δεν είναι δύσκολη υπόθεση, αφού κυκλοφορούν πολλές διαφορετικές εκδόσεις που μπορούν να εξυπηρετήσουν από τον «ανυποψίαστο» μέχρι τον επαγγελματία χρήστη. Μπορεί κανείς να βρει στο Διαδίκτυο πιο «ελαφριά» firewall τα οποία διανέμονται δωρεάν, ενώ τα Windows από την έκδοση XP και μετά, διαθέτουν δικό τους τείχος προστασίας.

5.2.1 Κατηγορίες τειχών προστασίας

Οι δύο μεγάλες κατηγορίες των τειχών προστασίας είναι:

- τα hardware firewalls

- τα software firewalls

Στην πρώτη κατηγορία ανήκουν είτε συσκευές που είναι αυτόνομες (stand alone) και συνδέονται αμέσως με το δίκτυο είτε υπολογιστές που η μόνη τους δουλειά είναι ο ρόλος του τείχους προστασίας σε ένα δίκτυο και που έχουν εγκατεστημένα τα απαραίτητα προς τον σκοπό αυτό προγράμματα.

Επίσης τα τείχη προστασίας χωρίζονται σε δυο μεγάλες κατηγορίες:

- αυτά που παρέχονται σε μορφή προγραμμάτων, τα οποία αναφέρονται ως personal firewall
- αυτά που παρέχονται σε μορφή υλικού, τα οποία καλούνται hardware firewall.

Τα τελευταία κυκλοφορούν είτε ως αυτόνομες συσκευές δικτύου όπως είναι τα μόντεμ ADSL. Σε γενικές γραμμές τα τείχη προστασίας που κυκλοφορούν ως αυτόνομες συσκευές αποτελούν λύσεις κυρίως σε εταιρικά δίκτυα.
Οι διαφορές που υπάρχουν ανάμεσα στα τείχη προστασίας είναι αρκετές. Κάθε μια έχει τα δικά της πλεονεκτήματα και μειονεκτήματα. Σε άλλες περιπτώσεις είναι πιο εύχρηστη και αποτελεσματική η χρήση των software firewall και σε άλλες η χρήση των hardware firewall.

5.3 Φίλτρα προστασίας[101]

Ένα φίλτρο προστασίας είναι ένα πακέτο λογισμικού το οποίο ελέγχει και ρυθμίζει την πρόσβαση σε πληροφορίες ή υπηρεσίες του Διαδικτύου σύμφωνα με καθορισμένα κριτήρια.
Τα φίλτρα προστασίας μπορούν να εγκατασταθούν είτε στον υπολογιστή ενός απλού χρήστη, είτε σε έναν κεντρικό υπολογιστή που ανήκει σε κάποιο φορέα ή σε έναν υπολογιστή ενός παροχέα υπηρεσιών Διαδικτύου και μπορούν να δράσουν ποικιλοτρόπως, όπως να προειδοποιήσουν για προβληματικές

[101] http://www.saferinternet.gr/

ιστοσελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο Διαδίκτυο, να απαγορεύσουν την πρόσβαση σε ύποπτους ιστοχώρους ακόμα και να κλείσουν τελείως τον υπολογιστή.

Ο βασικός στόχος των φίλτρων για την προστασία των ανηλίκων είναι η παροχή ενός αξιόπιστου φράγματος που αποτρέπει την πρόσβαση σε μη αποδεκτό περιεχόμενο, σε περιεχόμενο που θεωρείται επικίνδυνο ή σε περιεχόμενο που μπορεί να προκαλέσει ηθικές βλάβες στην ανάπτυξη των παιδιών. Ταυτόχρονα, το κατάλληλο για παιδιά και για νέους περιεχόμενο δεν θα πρέπει να περιορίζεται.

Σε ότι αφορά τον γονικό έλεγχο, τα φίλτρα ασχολούνται και με τα δεδομένα που εξέρχονται από τον υπολογιστή, π.χ. για την αποφυγή δημοσίευσης προσωπικών στοιχείων από τα παιδιά, όπως ονόματα, διευθύνσεις σπιτιού ή σχολείου, στοιχεία πιστωτικών καρτών, κ.λπ.

Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από τη συχνότητα ανανέωσης των οι λιστών με τις απαγορευμένες τοποθεσίες. Υπάρχουν διαφορετικοί τύποι φίλτρων και το καθένα είναι σχεδιασμένο και λειτουργεί πιο αποτελεσματικά στο είδος της προστασίας που παρέχει. Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να ελέγχει και να ρυθμίζει την πρόσβαση σε τοποθεσίες με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε ιστοχώρους με περιεχόμενο την βία ή τον ρατσισμό.

Τα φίλτρα μπορούν να αποδειχτούν πολύτιμα εργαλεία στην προστασία των ανηλίκων από επιβλαβές περιεχόμενο. Παρόλα αυτά, θα πρέπει να γίνει κατανοητό ότι τα εργαλεία φιλτραρίσματος είναι χρήσιμα για να συμπληρώνουν και όχι να αντικαθιστούν τη γονική επίβλεψη και πιθανώς μόνο σε μικρότερες ηλικίες. Η εκπαιδευτική επίβλεψη στο σπίτι, σε αντιστοιχία με αυτή που γίνεται στα σχολεία, μαζί με την επικοινωνία μέσα στην οικογένεια και την γνώση των κινδύνων, είναι προτιμότερη από τα τεχνολογικά φράγματα καθώς συμβάλλει στη σωστή εκπαίδευση των ανηλίκων, στην κατανόηση των προβλημάτων και

στην ανάπτυξη κριτικής σκέψης για την αντιμετώπιση αυτών. Ενώ τα φίλτρα είναι χρήσιμα όσο τα παιδιά είναι μικρά, καθώς μεγαλώνουν, θα πρέπει να αναπτύξουν ασφαλή και υπεύθυνη συμπεριφορά στο Διαδίκτυο.

5.3.1 Τρόποι λειτουργίας Φίλτρων[102]

Τα φίλτρα προστασίας λειτουργούν με τους εξής τρόπους:

Περιφραγμένες τοποθεσίες: Οι λεγόμενες «περιφραγμένες τοποθεσίες» (walled gardens) ή «λευκές λίστες» (white lists) είναι λίστες από ιστοσελίδες που είναι κατάλληλες για ανηλίκους και επιτρέπουν στον χρήστη να έχει πρόσβαση αποκλειστικά σε αυτές.

Λίστες «Όχι» : Συντάσσεται μία λίστα «Όχι» από ιστοσελίδες που πρέπει να αποφευχθούν (π.χ. με προσβλητικό, βίαιο ή ρατσιστικό περιεχόμενο) και αν το παιδί σας προσπαθήσει να μπει σε κάποια από αυτές, τότε μπλοκάρεται η πρόσβασή του/της. Ορισμένα προγράμματα λειτουργούν και με λίστες απαγορευμένων λέξεων. Μόλις βρεθεί κάποια από αυτές τις λέξεις σε κάποια ηλεκτρονική διεύθυνση ή στην ίδια την ιστοσελίδα, τότε μπλοκάρεται η πρόσβαση. Το πρόβλημα με αυτές τις λίστες τύπου «Όχι» είναι ότι πρέπει να αναβαθμίζονται συνέχεια.

Μπλοκάρισμα ιστοσελίδων με απαγορευμένες λέξεις: Τα πιο απλά φίλτρα της αγοράς μπλοκάρουν περιεχόμενο στο Διαδίκτυο, χρησιμοποιώντας λίστα με απαγορευμένες λέξεις. Αυτές οι λέξεις - κλειδιά δημιουργούνται και μπορούν να ανανεώνονται εύκολα και γρήγορα.

Φιλτράρισμα βάσει αυτόματης ταξινόμησης του περιεχομένου: Τα συστήματα αυτόματης ταξινόμησης αξιολογούν ολόκληρο το κείμενο που υπάρχει σε μια ιστοσελίδα. Χρησιμοποιούν για αυτό γνωστές στατιστικές μεθόδους, όπως αυτές που εφαρμόζουν τα φίλτρα ανεπιθύμητης αλληλογραφίας.

[102] http://www.saferinternet.gr

Αυτοαξιολόγηση ιστοσελίδων: Οι πάροχοι της διαδικτυακής πληροφορίας τοποθετούν εθελοντικά στον αντίστοιχο ιστοχώρο μια ετικέτα, η οποία δείχνει αν και σε ποιο βαθμό η ιστοσελίδα αυτή περιέχει συγκεκριμένο υλικό (π.χ. βία, γυμνό, τυχερά παιχνίδια, περιεχόμενο για ενηλίκους, κ.λ.π.). Οι ετικέτες και οι κατηγορίες έχουν δημιουργηθεί από την Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου I.C.R.A.. Το φίλτρο διαβάζει αυτές τις ετικέτες και αποφασίζει αν θα επιτρέψει την πρόσβαση, σύμφωνα με αυτά που οι γονείς επέλεξαν να επιτρέψουν στα παιδιά τους να δουν. Το πρόβλημα με αυτό το σύστημα είναι ότι εξαρτάται από το αν οι ιδιοκτήτες των ιστοσελίδων θα αξιολογήσουν εθελοντικά τις ιστοσελίδες τους και μέχρι στιγμής, δεν είναι πολλοί αυτοί που το κάνουν.

Συνδυασμός μεθόδων φιλτραρίσματος: Οι βασικές προσεγγίσεις στο φιλτράρισμα συνδυάζονται σήμερα με πολλούς τρόπους με σκοπό να αυξηθεί η αποτελεσματικότητα, αλλά και για να διαφοροποιείται η προσβασιμότητα ανάλογα με την ηλικία.

5.3.2 Σύστημα I.C.R.A.[103]

Το σύστημα I.C.R.A. είναι μια μέθοδος χαρακτηρισμού του περιεχομένου ιστοσελίδων έτσι ώστε να μπορούν τα προγράμματα φιλτραρίσματος να εντοπίζουν το ακατάλληλο περιεχόμενο ευκολότερα. Υπάγεται στο Ινστιτούτο για την Οικογενειακή Ασφάλεια στο Διαδίκτυο, ένα διεθνή μη κερδοσκοπικό οργανισμό και λειτουργεί ως εξής:

Οι δημιουργοί μιας ιστοσελίδας που χρησιμοποιούν το σύστημα I.C.R.A., απαντούν σε ένα ερωτηματολόγιο που ζητά αναλυτικές πληροφορίες για το περιεχόμενο της ιστοσελίδας αυτής. Δημιουργείται έτσι μια συγκεκριμένη ετικέτα περιγραφής του περιεχομένου της ιστοσελίδας. Τα φίλτρα εντοπίζουν την ετικέτα αυτή και ανάλογα με τη ρύθμιση τους σε σχέση με ποιες

[103] http://www.saferinternet.gr

ιστοσελίδες να μπλοκάρουν, επιτρέπουν ή απαγορεύουν την πρόσβαση στην συγκεκριμένη ιστοσελίδα από τον χρήστη.

5.3.3 Σύγκριση φίλτρων

Πίνακας 6: Σύγκριση φίλτρων[104]

■■■■ Άριστα ■■■□ Πολύ Καλά ■■□□ Καλά ■□□□ Ικανοποιητικά □□□□ Φτωχά	Net Nanny	Safe Eyes	CYBER sitter	Cyber Patrol	MaxProtect	McAfee Parental Controls	Filter Pak	imView	Norton Parental Controls	Parental Controls
Γενική Βαθμολογία	■■■■	■■■▮	■■■▮	■■■□	■■■□	■■□□	■■▮□	■■□□	■■□□	■■□□
Ευκολία Χρήσης	■■■■	■■■□	■■■▮	■■■□	■■■▮	■□□□	■■□□	■■■□	■■□□	■■■□
Ευκολία Εγκατάστασης	■■■■	■■■■	■■■▮	■■■■	■▮□□	■□□□	■■■■	■■□□	■□□□	■▮□□
Αποτελεσματικότητα Φιλτραρίσματος	■■■▮	■■■▮	■■■▮	■■■□	■■■□	■■■□	■■■□	■■□□	■■□□	■▮□□
Τιμή*	$28.99	$49.95	$34.95	$39.95	$49.95	$49.99	$49.95/έτος	$59.99/έτος	$59.99	$39.95

***Οι τιμές καταγράφηκαν τον Απρίλιο του 2009**

[104] http://internet-filter-review.toptenreviews.com/

5.4 Οικογενειακές ρυθμίσεις XBOX 360[105]

Το Xbox 360, η δημοφιλή κονσόλα βιντεοπαιχνιδιών της Microsoft, παρέχει στους γονείς μια ειδική κατηγορία στο μενού του, από την οποία έχουν τη δυνατότητα να ρυθμίσουν την πρόσβαση σε παιχνίδια, με βάση το σύστημα διαβάθμισης P.E.G.I.

Κάθε παιχνίδι που κυκλοφορεί διαθέτει τόσο στο εξώφυλλο, όσο και κωδικοποιημένη στον δίσκο, την ηλικιακή αποτίμηση της γεωγραφικής περιοχής στην οποία διατίθεται. Έτσι, το Xbox 360 έχει τη δυνατότητα να μπλοκάρει την πρόσβαση σε παιχνίδια που υπερβαίνουν τα όρια ηλικίας του παιδιού, όπως αυτά έχουν οριστεί από τους γονείς του.

Επιπλέον, ο γονέας μπορεί να ορίσει και έναν κωδικό πρόσβασης στις «Οικογενειακές Ρυθμίσεις», προκειμένου να «κλειδώσει» το μενού αυτό και να βεβαιωθεί πως το παιδί δεν θα μπορέσει να αλλάξει τις ρυθμίσεις. Με αυτές τις δυνατότητες, οι γονείς μπορούν να διασφαλίσουν ότι έχουν τον έλεγχο του περιεχομένου των παιχνιδιών με τα οποία ασχολούνται τα παιδιά τους, χωρίς να χρειάζονται να βρίσκονται συνέχεια μαζί τους και να εποπτεύουν συνεχώς τι παίζουν.

[105] http://www.xbox.com/el-GR/support/xbox360/familysettings/consolefamilysettings.htm
http://infocafe.eu/?p=21

6. ΔΡΑΣΕΙΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΠΡΟΣΤΑΣΙΑΣ

Η επιτακτική ανάγκη για έλεγχο και περιορισμό της ροής παράνομου περιεχομένου, όπως επίσης οι κίνδυνοι και οι απειλές που ελλοχεύουν στο Διαδίκτυο, έχουν οδηγήσει στην δημιουργία διαφόρων ομάδων, δράσεων και υπηρεσιών, που σκοπό έχουν να ενημερώσουν και κυρίως να προστατεύσουν τους χρήστες του Διαδικτύου.

Φορείς ιδιωτικού και δημοσίου δικαίου, σε κρατικό και ευρωπαϊκό επίπεδο, έχουν λάβει δράση για την εξοικείωση των πολιτών με τις σύγχρονες ψηφιακές τεχνολογίες, μέσω της συνεχούς ενημέρωσης και της διαμόρφωσης ενός ασφαλούς περιβάλλοντος πλοήγησης. Σε αυτά τα πλαίσια δράσης, εκστρατείες επαγρύπνησης και προστασίας, πανεκπαιδευτικά δίκτυα, ημερίδες ενημέρωσης και υπηρεσίες δίωξης και καταγγελίας του ηλεκτρονικού εγκλήματος, οργανώνονται με αυξανόμενη συχνότητα.

Στο παρόν κεφάλαιο, αναφέρονται οι σημαντικότερες δράσεις και υπηρεσίες προστασίας που αφορούν την Ελληνική πραγματικότητα. Σκοπός του κεφαλαίου είναι να γνωστοποιήσει σε μαθητές, γονείς, εκπαιδευτικούς ή απλούς χρήστες τις επιλογές που διατίθενται, ώστε να ενημερωθούν για τις παρούσες δυνατότητες ασφαλέστερης πλοήγησης στο Διαδίκτυο από τους διάφορους φορείς και να λάβουν τις κατάλληλες ενέργειες για την αντιμετώπιση των κινδύνων.

6.1 Ομάδα Δράσης για την Ψηφιακή Ασφάλεια[106]

Η Ομάδα Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness and Response to Threats - D.A.R.T.) της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού είναι μια πρωτοβουλία του Υπουργείου Οικονομίας και Οικονομικών στο πλαίσιο της Ψηφιακής Στρατηγικής 2006-2013.

[106] http://www.dart.gov.gr/NewsInner.aspx?new_id=173&nwc_id=20
http://www.okosmosgyromas.gr/node/131

Άμεσος στόχος της ομάδας είναι η ενημέρωση των πολιτών, η πρόληψη καθώς και η ανταλλαγή τεχνογνωσίας για την αντιμετώπιση κινδύνων που σχετίζονται με τις νέες τεχνολογίες πληροφορικής και ηλεκτρονικών επικοινωνιών. Επιπρόσθετα, σκοπεύει στην συνένωση των πολιτών μέσω ενός σημείου αναφοράς για πληροφόρηση, πρόληψη και ενημέρωση για να μην βρεθούν αντιμέτωποι με τους ψηφιακούς κινδύνους και να κατευθυνθούν σωστά και γρήγορα στις πλέον αρμόδιες κάθε φορά αρχές ώστε να αντιμετωπίσουν ενδεχόμενα προβλήματα.

Η προσπάθεια φιλοδοξεί να ενώσει τις δυνάμεις των αρμόδιων φορέων καθώς και να ενδυναμώσει την εμπιστοσύνη των πολιτών στο αναπτυσσόμενο Διαδίκτυο. Η εξοικείωση των πολιτών με τις νέες τεχνολογίες και η ενίσχυση της εμπιστοσύνης στις δυνατότητές τους, θα απελευθερώσει τις υγιείς δυνάμεις και θα δώσει ώθηση στην ψηφιακή Ελλάδα.

Η ομάδα δράσης D.A.R.T. στελεχώνεται με ήδη δοκιμασμένα στελέχη και απαρτίζεται από:

- Ειδικό Γραμματέα Ψηφιακού Σχεδιασμού του Υπουργείου Οικονομίας και Οικονομικών, με ρόλο Συντονιστή.
- Προϊστάμενο του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος του Υπουργείου Δημοσίας Τάξεως.
- Εκπρόσωπο της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων.
- Εκπρόσωπο της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών.
- Δύο ειδικούς εμπειρογνώμονες της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού.

Παράλληλα η ομάδα D.A.R.T. αξιοποιεί κάθε διαθέσιμο κανάλι επικοινωνίας με τους πολίτες για την συνεχή ενημέρωση και εξοικείωση τους σε θέματα ψηφιακής ασφάλειας:

- Διοργάνωση ημερίδων σε όλη την Ελλάδα, εστιασμένων σε θέματα που ενδιαφέρουν το διαφορετικό κάθε φορά κοινό.
- Δημιουργία και παραγωγή 2 φυλλαδίων ανά θεματική κατηγορία (γονείς και παιδιά, καταναλωτής και επιχείρηση κ.α.) με τίτλους «Συμβουλές για ασφαλή πλοήγηση» και «Συμβουλές για ασφαλείς συναλλαγές» αντίστοιχα.
- Δημιουργία 2 cd rom για γονείς και παιδιά με τίτλους «Συμβουλές ασφαλούς πλοήγησης για γονείς» και «Συμβουλές ασφαλούς πλοήγησης για παιδιά».
- Πανελλήνιος online οικογενειακός διαγωνισμός με τίτλο «Οι DARTανιάν του Διαδικτύου».

Η Ομάδα Δράσης για την Ψηφιακή Ασφάλεια δεν είναι μια «κλειστή ομάδα». Επιθυμεί να υποστηρίξει οποιαδήποτε προσπάθεια για την ψηφιακή ασφάλεια που έχει διενεργηθεί από άλλους φορείς. Ήδη έχει αναπτύξει συνεργασία με ένα μεγάλο αριθμό φορέων από διαφορετικούς κλάδους οι οποίοι έχουν εκδηλώσει ενδιαφέρον να υποστηρίξουν τους στόχους της. Επιπρόσθετα είναι ανοιχτή σε προσκλήσεις τόσο για συνεργασίες όσο για την ενημέρωση του ευρύ κοινού σχετικά με την ασφαλή χρήση του Διαδικτύου.

Ο πολίτης και κάθε φορέας μπορεί να ενημερωθεί για σχετικά θέματα αλλά και να απευθυνθεί για αναζήτηση συμβουλής αποστέλλοντας ένα ηλεκτρονικό μήνυμα στην ομάδα μέσα από την ιστοσελίδα www.dart.gov.gr ή και να πάρει τηλέφωνο στο 1020.

6.2 Πανελλήνιο Σχολικό Δίκτυο και Κέντρα Πληροφορικής και Νέων Τεχνολογιών[107]

Το Πανελλήνιο Σχολικό Δίκτυο (www.sch.gr) είναι το προηγμένο Εκπαιδευτικό Ενδοδίκτυο του Υπουργείου Παιδείας, Διά Βίου Μάθησης και Θρησκευμάτων (ΥΠΔΒΜΘ), που διασυνδέει όλα τα σχολεία, τους εκπαιδευτικούς και πλήθος διοικητικών υπηρεσιών και εποπτευόμενων φορέων του ΥΠΔΒΜΘ. Πρόκειται για το μεγαλύτερο δημόσιο δίκτυο στη χώρα σε αριθμό χρηστών και έχει αναγνωριστεί διεθνώς ως ένα αξιόλογο εκπαιδευτικό δίκτυο που προάγει την αξιοποίηση των Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (Τ.Π.Ε.) στην Ελληνική εκπαίδευση.

Η ανάπτυξη του Πανελλήνιου Σχολικού Δικτύου έγινε με τη συγχρηματοδότηση του Ελληνικού Δημοσίου και της Ευρωπαϊκής Ένωσης (Ε.Π. «Κοινωνία της Πληροφορίας» www.infosoc.gr) και με τη σταθερή συνεργασία του ΥΠΔΒΜΘ με δώδεκα εποπτευόμενους ακαδημαϊκούς και ερευνητικούς φορείς του με υψηλή εξειδίκευση και εμπειρία σε θέματα σχεδιασμού, ανάπτυξης και λειτουργίας δικτυακών υποδομών και υπηρεσιών. Σήμερα, η λειτουργία του Πανελλήνιου Σχολικού Δικτύου καλύπτεται πλέον από εθνικούς πόρους.

Το Πανελλήνιο Σχολικό Δίκτυο έχει συμπληρώσει δέκα χρόνια από την έναρξη της λειτουργίας του και με την επιτυχημένη υλοποίησή του έχει δημιουργήσει μία νέα γενιά καινοτόμων εκπαιδευτικών κοινοτήτων που χρησιμοποιούν καθημερινά τις Τ.Π.Ε. στο έργο τους.

Το σχολικό δίκτυο υποστηρίζει επίσης και το διοικητικό έργο της εκπαίδευσης, καθώς το ΥΠΔΒΜΘ είναι από τους πρώτους φορείς του δημοσίου στη Ελλάδα που χρησιμοποιούν εφαρμογές ηλεκτρονικής διακυβέρνησης για τη διαχείριση

[107] http://dide.ilei.sch.gr/keplinet/articles/psd.php#web_filtering
http://www.sch.gr/sch-portlets/aboutSch/docs/AnaforaXrisis-PSD.pdf
Κατερέλος Ι., Παπαδόπουλος Π. (2009). Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη. σελ.235-236
http://www.sch.gr/tieinaitoschmenu/2009-10-04-08-50-34

της εκπαίδευσης, όπως π.χ. για τη συλλογή στοιχείων των μαθητικού και εκπαιδευτικού δυναμικού, για τον προγραμματισμό και την υλοποίηση των προσλήψεων των εκπαιδευτικών και τη μισθοδοσία τους, για τη διανομή των βιβλίων, κ.λπ.

Το Π.Σ.Δ. παρέχει επίσης τη δυνατότητα της δωρεάν σύνδεσης με το Διαδίκτυο προς όλους τους εκπαιδευτικούς της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης από το γραφείο και το σπίτι τους.

Τα Κέντρα Πληροφορικής και Νέων Τεχνολογιών, που συνδέονται με το Π.Σ.Δ., έχουν ιδρυθεί σταδιακά από τα τέλη του ’90 επίσης με πρωτοβουλίες του ΥΠΕΠΘ, στα πλαίσια των προσπαθειών για την αξιοποίηση των δυνατοτήτων των ΤΠΕ και την ένταξή τους στην καθημερινή εκπαιδευτική διαδικασία.

Υπάρχουν 58 τέτοια κέντρα στις εκπαιδευτικές περιφέρειες της χώρας, τα οποία ασχολούνται με:

- Την ανάπτυξη και υποστήριξη του δικτυακού και υπολογιστικού εξοπλισμού των σχολείων.
- Την ανάπτυξη λογισμικού και ψηφιακού περιεχομένου για εκπαιδευτικούς και διοικητικούς σκοπούς.
- Την επιμόρφωση των εκπαιδευτικών στις νέες τεχνολογίες με την ενσωμάτωση των ΤΠΕ στην εκπαιδευτική διαδικασία.
- Την υποστήριξη των μαθημάτων Πληροφορικής των Γυμνασίων, Ενιαίων Λυκείων και ΤΕΕ.

Το Π.Σ.Δ. παρέχει τις κάτωθι υπηρεσίες στα σχολεία και τις διοικητικές μονάδες της εκπαίδευσης:

- Τη φυσική δικτύωση των σχολικών και διοικητικών μονάδων, μέσω του πυκνού του δικτύου διανομής και των γραμμών υψηλής ταχύτητας στο δίκτυο κορμού.

- Τις διατιθέμενες βασικές και προηγμένες τηλεματικές υπηρεσίες προς τους χρήστες της εκπαιδευτικής κοινότητας (π.χ. Ηλεκτρονικό Ταχυδρομείο).
- Την αδιάλειπτη υποστήριξη των χρηστών του Π.Σ.Δ., μέσω ενός δυναμικού μηχανισμού HelpDesk.
- Τη συνεχή και αποτελεσματική ενημέρωση των εκπαιδευτικών, μαθητών και πολιτών για τις δυνατότητες και τις παρεχόμενες υπηρεσίες του Π.Σ.Δ.

Μερικά από τα στοιχεία (Ιούνιος 2010) που τεκμηριώνουν την ευρύτατη χρήση και αξιοποίηση του Π.Σ.Δ. είναι :

- Συνδεδεμένα σχολεία: 15.301
- Συνδεδεμένες διοικητικές υπηρεσίες: 3.181
- Δείκτης ευρυζωνικότητας: 86%
- Εκπαιδευτικοί με προσωπικό λογαριασμό: 75.153
- Μαθητές Γυμνασίου με προσωπικό λογαριασμό: 27.586
- Μεταβολή της συνολικής δικτυακής κίνησης την τελευταία πενταετία: +80% ετησίως.
- Πλήθος ενεργών γραμματοκιβωτίων: 129.805
- Πλήθος φιλοξενούμενων εκπαιδευτικών ιστοσελίδων: 8.407
- Πλήθος ψηφιακών μαθημάτων: 2.432 από 698 σχολεία (σχολικό έτος 2009-10)
- Πλήθος εκπαιδευτικών ιστολογίων: 5.050 τα οποία διαβάζονται από περισσότερους από 135.000 μοναδικούς επισκέπτες ανά μήνα.
- Επισκεψιμότητα δικτυακής πύλης www.sch.gr: 200.000 μοναδικοί επισκέπτες ανά μήνα.
- Ιδιαίτερα υψηλή χρήση του ηλεκτρονικού ταχυδρομείου και των λιστών επικοινωνίας των υπηρεσιών του ΥΠΔΒΜΘ με τα σχολεία.

Ο σχεδιασμός και η μέχρι σήμερα υλοποίηση του Π.Σ.Δ. έχει γίνει με στόχο να παρέχει χρήσιμες υπηρεσίες στο σύνολο της σχολικής κοινότητας, καλύπτοντας μεταξύ άλλων τους παρακάτω εκπαιδευτικούς στόχους:

- Πρόσβαση σε υπηρεσίες τηλεματικής.
- Πρόσβαση σε εκπαιδευτικό ψηφιακό υλικό.
- Εκπαίδευση από απόσταση, τηλεκπαίδευση.
- Αναζήτηση πιστοποιημένα χρήσιμων πληροφοριών.
- Ενθάρρυνση της συνεργασίας.
- Ανταλλαγή πληροφοριών και απόψεων.
- Διεξαγωγή θεματικών συζητήσεων, σεμιναρίων, διαλέξεων, κ.λπ, μέσω Διαδικτύου.
- Συνεργασία και επικοινωνία όλων των βαθμίδων της εκπαίδευσης.
- Επικοινωνία με ευρωπαϊκά εκπαιδευτικά δίκτυα.
- Εξυπηρέτηση προγραμμάτων συμπληρωματικής εκπαίδευσης.
- Δυνατότητα παροχής εκπαίδευσης σε άτομα με ειδικές ανάγκες.
- Ενημέρωση, πληροφόρηση, ψυχαγωγία

6.2.1 Υπηρεσία ελέγχου περιεχομένου στο Διαδίκτυο

Το Π.Σ.Δ. για να προστατεύσει τους μαθητές από το παράνομο και ακατάλληλο περιεχόμενο παρέχει την υπηρεσία ελεγχόμενης πρόσβασης (web-filtering) στον παγκόσμιο ιστό. Με τον τρόπο αυτό αποκόβεται αυτόματα η πρόσβαση σε ιστοσελίδες:

- που προπαγανδίζουν την επιθετική συμπεριφορά, το μίσος και τη βία
- που προωθούν τα ναρκωτικά
- με τυχερά παιχνίδια
- με πορνογραφικό περιεχόμενο
- που προωθούν το ρατσισμό

Σε περίπτωση που οι μαθητές ή οι εκπαιδευτικοί συναντήσουν κάποια σελίδα με ακατάλληλο περιεχόμενο, η οποία δεν φιλτράρεται αυτόματα από την υπηρεσία ελέγχου περιεχομένου, θα πρέπει να στείλουν ηλεκτρονικό μήνυμα στο διαχειριστή της υπηρεσίας στη διεύθυνση cachemaster@sch.gr για να ζητήσουν την απαγόρευση της συγκεκριμένης σελίδας.

6.2.2 Δικτυακή πύλη για το ελεύθερο λογισμικό και λογισμικό ανοιχτού κώδικα για την εκπαίδευση

Απευθύνεται στους χρήστες του Πανελλήνιου Σχολικού Δικτύου μέσω της ιστοσελίδας http://opensoft.sch.gr και αποβλέπει στην ενημέρωση της εκπαιδευτικής κοινότητας για το Ελεύθερο Λογισμικό/Λογισμικό Ανοικτού Κώδικα (ΕΛ/ΛΑΚ) και στην παρουσίαση εφαρμογών ανοικτού κώδικα που θα μπορούσαν να αξιοποιηθούν στην εκπαίδευση.

Ως ΕΛ/ΛΑΚ χαρακτηρίζεται το λογισμικό εκείνο, το οποίο διανέμεται μαζί με τον πηγαίο κώδικά του. Έτσι καθένας μπορεί να το χρησιμοποιήσει για οποιοδήποτε σκοπό, ενώ παράλληλα μπορεί να μελετήσει ή να τροποποιήσει τον πηγαίο κώδικα του προγράμματος και να αναδιανείμει ελεύθερα την αρχική ή την τροποποιημένη έκδοση του προγράμματος.

Η υλοποίηση της πύλης έγινε στα πλαίσια του έργου «Προηγμένες Τηλεματικές Υπηρεσίες για τη Δευτεροβάθμια Εκπαίδευση», το οποίο εντάσσεται στο ΕΠ Κοινωνία της Πληροφορίας, συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση και υλοποιείται από το Πανεπιστήμιο Μακεδονίας - Τμήμα Εφαρμοσμένης Πληροφορικής.

Οι στόχοι της δικτυακής πύλης είναι:

- Ενημέρωση της εκπαιδευτικής κοινότητας για το ΕΛ/ΛΑΚ στην εκπαίδευση και τη δυνατότητα αξιοποίησής του.
- Παρουσίαση ανάλογων δράσεων σε διεθνές επίπεδο.
- Παροχή βήματος ανταλλαγής ιδεών και προτάσεων από τους ενδιαφερόμενους χρήστες του Π.Σ.Δ..

Στην πύλη περιέχονται: Βιβλιοθήκη λογισμικού, Νέα, Σχετικοί σύνδεσμοι, Forum, Στατιστικά, Ανακοινώσεις εκδηλώσεων, Newsletter – RSS, κ.ά.

Στη βιβλιοθήκη γίνεται καταγραφή, ταξινόμηση και παρουσίαση περισσότερων από 400 λογισμικών:

- Προγράμματα και εφαρμογές με δυνατότητα αξιοποίησης στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση.
- Συστήματα ασύγχρονης τηλεκπαίδευσης και ηλεκτρονικής μάθησης.
- Προγράμματα για την υποστήριξη διοικητικών και διαχειριστικών διαδικασιών της σχολικής μονάδας.
- Εφαρμογές γραφείου, επικοινωνίας και Διαδικτύου.

Ενδεικτικές θεματικές ενότητες που περιλαμβάνονται:

- Πληροφορική
- Μαθηματικά
- Χημεία
- Φυσική
- Γεωγραφία
- Μουσική
- Εφαρμογές διαχείρισης της σχολικής τάξης
- Συστήματα τηλεκπαίδευσης

Αποτίμηση χρήσης ΕΛ/ΛΑΚ στο Π.Σ.Δ.:

- Σημαντική οικονομία στην απόκτηση και συντήρηση λογισμικών.
- Υψηλή εγχώρια προστιθέμενη αξία.
    - Απόκτηση τεχνογνωσίας μέσω της συνεισφοράς σε εργασίες: **α)** εξελληνισμού και προσαρμογής, π.χ. Horde, Moodle, Free Radius.

β) ανάπτυξης λογισμικού και την διάθεσή του στην κοινότητα του ΕΛ/ΛΑΚ, π.χ. Dialup_admin.

- Μείωση χρόνου ανάπτυξης υπηρεσιών και εφαρμογών.
- Δυνατότητα προσαρμογής στις ανάγκες.
- Χρήση λογισμικών εξαιρετικής ποιότητας, αξιοπιστίας, απόδοσης και ασφάλειας
- Ασφαλέστερες υλοποιήσεις σε σχέση με αντίστοιχα εμπορικά λογισμικά.

6.2.3 Ασύγχρονη τηλεκπαίδευση

Η υπηρεσία ασύγχρονης τηλεκπαίδευσης του Πανελλήνιου Σχολικού Δικτύου υλοποιεί μια διαδικασία ανταλλαγής μάθησης μεταξύ εκπαιδευτή και εκπαιδευομένων, η οποία πραγματοποιείται ανεξάρτητα του χρόνου και του τόπου.

Η υπηρεσία βασίζεται στο λογισμικό ανοικτού κώδικα Moodle, το οποίο είναι ένα πακέτο λογισμικού για την παραγωγή διαδικτυακών μαθημάτων. Οι χρήστες για να εισέλθουν στο Moodle, χρησιμοποιούν το όνομα χρήστη και τον κωδικό πρόσβασης που διαθέτουν στο Π.Σ.Δ. Οι χρήστες του Π.Σ.Δ. μπορούν να δημιουργήσουν ένα μάθημα στο Moodle, κατόπιν υποβολής αίτησης για απόδοση δικαιωμάτων εκπαιδευτή.

Μερικά από τα πλεονεκτήματα από τη χρήση της ασύγχρονης τηλεκπαίδευσης είναι:

- Το γεγονός πως οι εκπαιδευόμενοι μπορούν να εξετάσουν το περιεχόμενο σύμφωνα με το πρόγραμμά τους.
- Οι εκπαιδευόμενοι μπορούν να ιεραρχήσουν τα θέματα του εκπαιδευτικού υλικού.

- Το ασύγχρονο περιβάλλον είναι πολύ χρήσιμο για όσους μαθαίνουν καλύτερα σκεφτόμενοι για το περιεχόμενο και γι' αυτούς που μπορούν να δουλέψουν στο δικό τους χρόνο και να ακολουθήσουν οδηγίες.
- Υποστηρίζει διάφορες μορφές μάθησης με δυνατότητα επιλογής της πιο κατάλληλης λύσης ως προς το περιεχόμενο και τον αρχάριο.
- Μπορούν να επιλέξουν το μαθησιακό στυλ που προτιμούν κι έτσι μπορούν να αφομοιώσουν και να εφαρμόσουν τη γνώση.
- Η αυτο-έκφραση και ενεργός μάθηση ενθαρρύνουν τη συμμετοχή των εκπαιδευομένων στη διαδικασία της μάθησης.
- Βελτιώνει την κριτική σκέψη των εκπαιδευομένων.
- Διευκολύνει τις συνεργατικές δεξιότητες μάθησης και επικοινωνίας μέσω της διάδρασης και της αλληλεπίδρασης.
- Εξατομίκευση: Οι εκπαιδευόμενοι μπορούν να μάθουν στο δικό τους χρόνο σε ένα ασφαλές περιβάλλον.
- Παρώθηση: Η τεχνολογία μπορεί να κάνει τη μάθηση ευχάριστη και σχετική με τα ενδιαφέροντα των εκπαιδευτικών.

Η πλατφόρμα ασύγχρονης τηλεκπαίδευσης (http://e-learning.sch.gr) του Π.Σ.Δ. είναι προσβάσιμη μέσω ενός απλού φυλλομετρητή (web browser) και η εμφάνιση του περιβάλλοντος τηλεκπαίδευσης είναι εύκολα προσαρμόσιμη. Το λογισμικό που χρησιμοποιείται για την υλοποίηση της υπηρεσίας είναι το Moodle (http://www.moodle.org).

6.2.4 Τηλεδιάσκεψη και σύγχρονη τηλεκπαίδευση

Με τον όρο σύγχρονη τηλεδιάσκεψη εννοείται η αμφίδρομη επικοινωνία με ανταλλαγή εικόνας (video), ήχου (audio) και κειμένου (chat) σε πραγματικό χρόνο μεταξύ δύο ή και περισσότερων ατόμων. Σαν επιπλέον στοιχεία σε μια τηλεδιάσκεψη μπορούμε να αναφέρουμε τη δυνατότητα της παρουσίασης υλικού (π.χ. μέσω του powerpoint) από έναν χρήστη που συμμετέχει στην

τηλεδιάσκεψη προς τους άλλους καθώς και τη δυνατότητα να μοιράζονται οι χρήστες μια εφαρμογή.

Διακρίνονται δύο μεγάλες κατηγορίες στις υπηρεσίες τηλεδιάσκεψης σε σχέση με το πόσα άτομα συμμετέχουν στην τηλεδιάσκεψη και με το πώς γίνεται η διασύνδεση μεταξύ τους. Οι κατηγορίες αυτές είναι:

- Τηλεδιάσκεψη μεταξύ δύο χρηστών με απευθείας σύνδεση (point to point).
- Τηλεδιάσκεψη μεταξύ δύο ή περισσοτέρων χρηστών με τη βοήθεια ενός κεντρικού εξυπηρετητή τηλεδιασκέψεων (point to multipoint).

Οι υπηρεσίες αυτές χρησιμοποιούν ως μέσο το IP δίκτυο του Πανελλήνιου Σχολικού Δικτύου (Π.Σ.Δ.).

Σαν βασικό λογισμικό από τη μεριά ενός χρήστη χρησιμοποιούν: α) τα λογισμικά Netmeeting και ILS της εταιρείας Microsoft (για τηλεδιασκέψεις point to point) και β) το λογισμικό Netmeeting της εταιρίας Microsoft, το Conference Server 6 της εταιρείας FVC και τα προγράμματα Java VC-Client και VC-Moderator που έχουν αναπτυχθεί από το Π.Σ.Δ.

Επιπλέον, το Π.Σ.Δ. προσφέρει την υπηρεσία της τηλεδιάσκεψης μεταξύ δύο ή περισσοτέρων χρηστών μέσω της ιστοσελίδας http://conf.sch.gr, κάνοντας χρήση της εφαρμογής Click to Meet, που είναι πιο εύχρηστη και με περισσότερες δυνατότητες από το Netmeeting..

6.2.5 Βίντεο κατ' απαίτηση

Η υπηρεσία Βίντεο κατ' Απαίτηση του Π.Σ.Δ. έχει σαν σκοπό της τη διάθεση μέσω του Διαδικτύου, πολυμεσικού εκπαιδευτικού περιεχομένου, του οποίου επιμελείται της επεξεργασίας και κωδικοποίησής του και στη συνέχεια ταξινομεί και διαθέτει.

Η συγκεκριμένη υπηρεσία παρέχει τη δυνατότητα στους χρήστες του Π.Σ.Δ. να παρακολουθήσουν το διαθέσιμο αποθηκευμένο υλικό, που μπορεί να αποτελείται από βίντεο, ήχο, πολυμεσικές παρουσιάσεις κ.λπ., χωρίς χρονικούς

περιορισμούς. Παρέχει επίσης δυνατότητες αλληλεπίδρασης, ώστε ο χρήστης να ελέγχει τη ροή του υλικού που παρακολουθεί (Fast Forward, Rewind, Pause, Random Access). Επίσης, η υπηρεσία αφορά και στη διαχείριση των εξυπηρετητών βίντεο, με σκοπό την αποδοτική λειτουργία τους καθώς και τη ρύθμιση των δικτυακών προσβάσεων με τρόπο που να υποστηρίζονται όλα τα απαραίτητα πρωτόκολλα (unicast, multicast).

Η υπηρεσία ωφελεί σημαντικά στην εκπαιδευτική κοινότητα. Συγκεκριμένα:

- Ο εκπαιδευτικός έχει στη διάθεσή του εκπαιδευτικό υλικό (βίντεο, ήχο), το οποίο μπορεί να χρησιμοποιήσει ενισχυτικά στην εκπαιδευτική διαδικασία.
- Ο μαθητής επωφελείται από τη διάθεση ενημερωτικού και εκπαιδευτικού υλικού στο μάθημα, στο σχολικό εργαστήριο, αλλά και εκτός σχολείου.
- Εκπαιδευτικοί, φορείς της εκπαίδευσης και άλλοι, μπορούν να διαθέσουν το πολυμεσικό υλικό τους (βίντεο, ήχο) μέσα από την υπηρεσία σύμφωνα με τον κανονισμό λειτουργίας και τις διαδικασίες που ισχύουν.
- Άλλες υπηρεσίες του Π.Σ.Δ., όπως η ασύγχρονη και σύγχρονη τηλεκπαίδευση επωφελούνται από τις δυνατότητες που παρέχει η υπηρεσία.
- Το σύνολο της εκπαιδευτικής κοινότητας και οι φορείς της εκπαίδευσης επωφελούνται από την υποστήριξη ζωντανών αναμεταδόσεων διαφόρων εκδηλώσεων φορέων της εκπαίδευσης, π.χ. συνέδρια, ημερίδες, κ.λπ.

Η υπηρεσία προσφέρει τις ακόλουθες δυνατότητες:

- Διάθεση πολυμεσικού υλικού σε μορφή βίντεο και ήχου για την υποστήριξη όλων των δικτυακών συνδέσεων (τηλεφωνική σύνδεση, ISDN, ADSL, κ.λπ.).

- Ψηφιοποίηση βίντεο, ήχου και κωδικοποίηση για τη μετάδοση μέσω δικτύου.
- Ταξινόμηση υλικού ανά κατηγορία.
- Αναζήτηση υλικού ανά κατηγορία.
- Ανάρτηση υλικού σύμφωνα με τους όρους της υπηρεσίας.
- Πιστοποίηση χρηστών μέσω της υπηρεσίας καταλόγου.
- Ζωντανές αναμεταδόσεις από οποιαδήποτε σημείο του Π.Σ.Δ..

Η πρόσβαση στην υπηρεσία γίνεται είτε μέσω της δικτυακής πύλης του Π.Σ.Δ. (http://www.sch.gr) είτε απευθείας στη διεύθυνση http://vod.sch.gr. Ο χρήστης μπορεί να πληροφορηθεί για την υπηρεσία (κανονισμό λειτουργίας, διαδικασίες, στατιστικά, οδηγίες χρήσης) και να δει το διαθέσιμο υλικό. Όλοι οι χρήστες απολαμβάνουν την υπηρεσία μέσα από διαδικασίες που ορίζουν τις απαιτούμενες ενέργειες για την ολοκλήρωση της κάθε εργασίας τους.
Για την υποστήριξη των ζωντανών μεταδόσεων ορίζονται οι απαιτήσεις και οι διαδικασίες για την επιτυχή σύνδεση του απομακρυσμένου σημείου με τον βίντεο εξυπηρετητή ώστε να γίνει η μετάδοση με την επιθυμητή ποιότητα.
Η σύνδεση με τις άλλες υπηρεσίες του Π.Σ.Δ. ορίζεται από διαδικασίες που εκδίδονται κατόπιν επεξεργασίας των τεχνικών προδιαγραφών και απαιτήσεων της σύνδεσης. Οι χρήστες πιστοποιούνται μέσω τις υπηρεσίας καταλόγου (LDAP) για την πρόσβαση σε περιεχόμενο για το οποίο απαιτείται έλεγχος.
Η ανάρτηση περιεχομένου ακολουθεί την διαδικασία έγκρισης που προβλέπει ο Κανονισμός Λειτουργίας του Π.Σ.Δ. και στη συνέχεια κωδικοποιείται, ταξινομείται και αναρτάται.

6.2.6 Ηλεκτρονική διαχείριση τάξης

Το Πανελλήνιο Σχολικό Δίκτυο στην προσπάθειά του να καλύπτει τις διαρκείς και ιδιαίτερες ανάγκες της κοινότητας των χρηστών του, σχεδίασε, οργάνωσε και προετοίμασε την υπηρεσία «Ηλεκτρονική Διαχείριση Τάξης (η-τ@ξη)».

Η υπηρεσία που προσφέρεται μέσω της ηλεκτρονικής διεύθυνσης http://eclass.sch.gr απευθύνεται σε εκπαιδευτικούς και μαθητές της Δευτεροβάθμιας Εκπαίδευσης, με στόχο την υποστήριξη της κλασσικής διδασκαλίας και την ενίσχυση της διαδικασίας μάθησης που πραγματοποιείται καθημερινά μέσα στη σχολική τάξη. Οι εκπαιδευτικοί θα ανακαλύψουν ένα χρήσιμο εργαλείο που θα τους βοηθήσει να οργανώσουν καλύτερα τις διδασκαλίες τους στο σχολείο. Οι μαθητές από την πλευρά τους θα αποκτήσουν ένα εναλλακτικό μέσο πρόσβασης στην ύλη των μαθημάτων που διδάσκονται.
Η είσοδος στην υπηρεσία «η-τ@ξη» γίνεται μέσω του Διαδικτύου με τους κωδικούς που διαθέτουν οι εκπαιδευτικοί στο Π.Σ.Δ.. Εκεί οι χρήστες μπορούν να δημιουργήσουν και να εξερευνήσουν τα μαθήματα του σχολείου τους ή να αναζητήσουν περιεχόμενο σε μαθήματα άλλων σχολείων.

6.2.7 Υπηρεσίες για τους μαθητές

Το Πανελλήνιο Σχολικό Δίκτυο έχει ξεκινήσει την παροχή υπηρεσιών στους μαθητές της δευτεροβάθμιας εκπαίδευσης. Οι υπηρεσίες για κάθε μαθητή είναι προσωπικές και τον συνοδεύουν όλα τα χρόνια που βρίσκεται στο σχολείο. Η πρόσβαση στις υπηρεσίες του Π.Σ.Δ. είναι εύκολη είτε από στο σχολικό εργαστήριο πληροφορικής είτε από το σπίτι με ένα ενιαίο όνομα χρήστη και έναν αντίστοιχο κωδικό πρόσβασης.

Το Π.Σ.Δ. προσφέρει μια δικτυακή πύλη (http://students.sch.gr) αφιερωμένη στους μαθητές όπου μπορούν να βρουν νέα, εκπαιδευτικές εφαρμογές, ψυχαγωγικές εφαρμογές αλλά και ενοποιημένη πρόσβαση στις υπηρεσίες που προσφέρει το Π.Σ.Δ. στους μαθητές.
Το Π.Σ.Δ. παρέχει προσωπικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου και οι βασικοί στόχοι της παροχής των λογαριασμών αυτών είναι:

- Η εξοικείωση των μαθητών με τις Τεχνολογίες Πληροφορίας και Επικοινωνιών (ΤΠΕ) στα πλαίσια των αντικειμένων που διδάσκονται στα σχολεία.

- Η επικοινωνία μεταξύ μαθητών και εκπαιδευτικών στα πλαίσια της εκπαιδευτικής διαδικασίας και η ανανέωση των εκπαιδευτικών μεθόδων.
- Η υποστήριξη της διαδικασίας μάθησης μέσα από δικτυακό περιβάλλον και τις ΤΠΕ.
- Η συνεργασία ομάδων ή σχολείων γεωγραφικά διασκορπισμένων, στα πλαίσια Ελληνικών ή ευρωπαϊκών προγραμμάτων.
- Η ανταλλαγή πληροφοριών και απόψεων (π.χ. ερωτήσεις-απαντήσεις από ειδικούς, ασκήσεις και λύσεις, κ.λπ.) και η διεξαγωγή θεματικών συζητήσεων.

Τα μηνύματα που ανταλλάσσονται από το λογαριασμό του μαθητή (είτε στέλνονται είτε λαμβάνονται) αποθηκεύονται μόνιμα σε κατάλληλους φακέλους εντός του γραμματοκιβωτίου (mailbox) του μαθητή. Το ιστορικό των μηνυμάτων είναι μόνο για ανάγνωση από τον μαθητή και δεν είναι δυνατή η διαγραφή του. Υπάρχει η δυνατότητα, αν ο κηδεμόνας του μαθητή το επιθυμεί, να ζητήσει να του γνωστοποιηθεί ο κωδικός του λογαριασμού ηλεκτρονικού ταχυδρομείου του μαθητή. Η αίτηση υποβάλλεται γραπτώς προς το σχολείο.
Ανάλογα με τον τύπο του λογαριασμού θα καθορίζεται το εύρος της επικοινωνίας που θα παρέχεται στον κάτοχό του.

Έτσι παρέχονται δύο τύποι:
Εκπαιδευτικός λογαριασμός: Ο κάτοχός του θα μπορεί να επικοινωνεί με όλους τους μαθητές, καθηγητές και σχολεία που διαθέτουν λογαριασμό εντός του Π.Σ.Δ., δηλαδή με διευθύνσεις της μορφής «username@sch.gr». Ένας τέτοιος λογαριασμός μπορεί να χρησιμοποιείται για την εξοικείωση του μαθητή με την αποστολή και λήψη e-mail στο εργαστήριο πληροφορικής και για ηλεκτρονική επικοινωνία με τους συμμαθητές του. Επίσης, είναι δυνατή η χρήση του για την αποστολή ασκήσεων με ηλεκτρονικό τρόπο στους καθηγητές του σχολείου. Αυτός ο τύπος λογαριασμού υποστηρίζει επικοινωνία μόνο εντός

του εκπαιδευτικού ενδοδικτύου και δεν εκθέτει τους μαθητές σε δυνητικούς κινδύνους του Διαδικτύου.

Πλήρης λογαριασμός: Ο κάτοχός του θα μπορεί να επικοινωνεί με χρήστες του Διαδικτύου γενικότερα, δηλαδή και εκτός του Π.Σ.Δ. αλλά με την εφαρμογή φίλτρων ασφαλείας. Ένας τέτοιος λογαριασμός μπορεί να χρησιμοποιείται για την επικοινωνία του μαθητή με άλλα σχολεία της Ευρώπης ή του κόσμου στα πλαίσια συνεργασιών μεταξύ σχολείων. Για την απόδοση τέτοιου λογαριασμού απαιτείται η έγγραφη συγκατάθεση του κηδεμόνα του μαθητή με τη συμπλήρωση κατάλληλου εντύπου. Στον πλήρη τύπο ο διαχειριστής χρηστών (π.χ. ο καθηγητής Πληροφορικής) μπορεί να ορίζει για τη σχολική μονάδα του τη λίστα απαγορευμένων και επιτρεπόμενων διευθύνσεων επικοινωνίας. Υπάρχουν δύο επίπεδα απαγορευμένων διευθύνσεων επικοινωνίας, σε καθολικό επίπεδο και σε επίπεδο σχολείου:

1. Σε καθολικό επίπεδο, υπάρχει γενική απαγόρευση όλων των διευθύνσεων εκτός του sch.gr και εκτός αυτών που καθορίζονται στις επιτρεπτές διευθύνσεις (domains) επικοινωνίας. Για λόγους προστασίας των μαθητών θα επιτρέπεται η επικοινωνία από και προς δίκτυα τα οποία μπορούν να αποδεικνύουν την ταυτότητα των χρηστών τους, π.χ. ypepth.gr, otenet.gr, forthnet.gr, κ.λπ.
2. Σε επίπεδο σχολείου, για τη διευκόλυνση της επικοινωνίας με σχολεία του εξωτερικού με τα οποία αναπτύσσονται κοινές εκπαιδευτικές δραστηριότητες, θα είναι δυνατός ο ορισμός επιτρεπόμενων διευθύνσεων επικοινωνίας (λευκές λίστες) από τον διαχειριστή της κάθε σχολικής μονάδας.

6.3 Ασφαλέστερο Διαδίκτυο[108]

Από 1η Ιανουαρίου 2009 η Ευρωπαϊκή Επιτροπή διαθέτει ένα πρόγραμμα για ασφαλέστερη χρήση του Διαδικτύου. Μετά την υπερψήφιση, με μεγάλη

[108] IP/08/1899 Βρυξέλλες, 09/12/2008

πλειοψηφία, στο Ευρωπαϊκό Κοινοβούλιο στις 23 Οκτωβρίου 2008, του νέου προγράμματος για ασφαλέστερη χρήση του Διαδικτύου (IP/08/1571), το Συμβούλιο των Υπουργών ενέκρινε το νέο πρόγραμμα.

Το νέο πρόγραμμα για ασφαλέστερη χρήση του Διαδικτύου, που καλύπτει την περίοδο 2009-2013, αποβλέπει τόσο στην προστασία των παιδιών σε ένα όλο και πιο περίπλοκο ηλεκτρονικό επιγραμμικό κόσμο, όσο και στην ενδυνάμωση των καταναλωτών γύρω από την ασφαλή χρήση των υπηρεσιών του Παγκόσμιου Ιστού, όπως η κοινωνική δικτύωση, τα ιστολόγια και τα άμεσα μηνύματα. Ενώ το 75% των παιδιών (ηλικίας μεταξύ 6 και 17 ετών) έχουν ήδη αποκαταστήσει σύνδεση με το Διαδίκτυο και το 50% των 10χρονων διαθέτουν κινητό τηλέφωνο - όπως προκύπτει από μια νέα έρευνα του Ευρωβαρόμετρου- ποσοστό 60% των ευρωπαίων γονέων ανησυχούν ότι τα παιδιά τους μπορεί να πέσουν θύματα σεξουαλικής κακοποίησης και 54% ότι τα παιδιά τους θα μπορούσαν να υποστούν παρενόχληση ή εκφοβισμό.

Το πρόγραμμα για ασφαλέστερη χρήση του Διαδικτύου θα καταπολεμήσει τις επαφές με βλέψεις σεξουαλικής κακοποίησης, την παρενόχληση και τον εκφοβισμό, καθιστώντας το λογισμικό και τις τεχνολογίες κινητών επικοινωνιών περισσότερο εξελιγμένα και ασφαλή.

Στο διάστημα μεταξύ 2009 και 2013 η Ε.Ε. θα διαθέσει 55 εκατ. ευρώ ώστε το Διαδίκτυο να καταστεί ασφαλέστερο και τα οποία θα κατανεμηθούν ως εξής:

- 48% προορίζεται για την ευαισθητοποίηση του κοινού
- 34% για την καταπολέμηση παράνομου περιεχομένου και την αντιμετώπιση επιβλαβούς επιγραμμικής συμπεριφοράς,
- 10% για ασφαλέστερο επιγραμμικό περιβάλλον και 8% για τη σύσταση μιας βάσης γνώσεων.

Το πρόγραμμα για ασφαλέστερη χρήση του Διαδικτύου, για τη χρονική περίοδο 2009-2013, εγκρίθηκε από το Συμβούλιο των Υπουργών και βασίζεται στα επιτεύγματα του προηγουμένου από αυτό, που κάλυψε την περίοδο 2005-2008.

Με το προτεινόμενο νέο πρόγραμμα θα συγχρηματοδοτηθούν έργα για:

- Αύξηση της ευαισθητοποίησης του κοινού: ενδυνάμωση της νεολαίας, των γονέων και των καθηγητών ώστε να πραγματοποιούν υπεύθυνες επιλογές, συμβουλεύοντάς τους για τις σχετικές προφυλάξεις που πρέπει να λαμβάνουν.
- Διάθεση στο κοινό ενός δικτύου από σημεία επαφής, προσβάσιμα είτε μέσω ενός ιστότοπου ή ενός τηλεφωνικού αριθμού, για την αναφορά παράνομου και επιβλαβούς περιεχομένου και συμπεριφοράς, ιδίως σχετικά με υλικό σεξουαλικής κακοποίησης παιδιών, επαφών με βλέψεις σεξουαλικής κακοποίησης και παρενόχλησης ή εκφοβισμού στον κυβερνοχώρο.
- Ενθάρρυνση των πρωτοβουλιών αυτορρύθμισης στο πεδίο αυτό και συμμετοχή των παιδιών στη δημιουργία ασφαλέστερου περιβάλλοντος.
- Δημιουργία μιας βάσης γνώσεων σχετικά με τις νέες τάσεις στη χρήση των επιγραμμικών τεχνολογιών και με τις συνέπειές τους στη ζωή των παιδιών μέσω συνένωσης, σε ευρωπαϊκή κλίμακα, τεχνικής, ψυχολογικής και κοινωνιολογικής εμπειρογνωσίας.

6.4 Ελληνικός κόμβος ασφαλούς Διαδικτύου[109]

Η δράση ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου και η εκστρατεία ενημέρωσης και επαγρύπνησης που διεξάγεται στην Ελλάδα από το 2004, υλοποιούνται υπό την αιγίδα της Ευρωπαϊκής Επιτροπής στο πλαίσιο του προγράμματος Safer Internet.

Οι κύριοι στόχοι της δράσης Saferinternet.gr είναι:

[109] http://www.saferinternet.gr/index.php?parentobjId=Page74
http://dide.ilei.sch.gr/keplinet/articles/saferinternet.php#pres_saferinternet
http://www.0-18.gr/downloads/saferinternet_gr_eisigisi_synigoros.pdf

- Η προστασία των ανήλικων χρηστών του Διαδικτύου από ακατάλληλο ή επιβλαβές για αυτούς περιεχόμενο, ή από ακατάλληλη ή επιβλαβή συμπεριφορά.
- Η ενημέρωση των γονέων για τους τρόπους με τους οποίους μπορούν να προστατευθούν αλλά και να προστατεύσουν αποτελεσματικά τα παιδιά τους από τους κινδύνους που εγκυμονούν από τη μη ορθή χρήση των διαδραστικών τεχνολογιών, όπως είναι το Διαδίκτυο ή το κινητό τηλέφωνο.
- Η προώθηση των θετικών πλευρών των διαδραστικών τεχνολογιών, ως εργαλεία της καθημερινής ζωής.
- Η εκπαίδευση των εκπαιδευτικών για την ασφαλή χρήση του Διαδικτύου και του κινητού τηλεφώνου, ενημερώνοντας τόσο για τα πολλαπλά οφέλη όσο και για τους πιθανούς κινδύνους, με στόχο τη δημιουργία πολλαπλασιαστικής δράσης μέσα στην τάξη.
- Η ενθάρρυνση του διαλόγου μεταξύ ανηλίκων και γονέων σχετικά με τη χρήση του Διαδικτύου, η προώθηση του ψηφιακού αλφαβητισμού και της κριτικής σκέψης.
- Η υποστήριξη, γονέων, εκπαιδευτικών, αλλά και ανήλικων χρηστών με κατάλληλο ενημερωτικό υλικό.

Για την επίτευξη των παραπάνω στόχων, το Saferinternet.gr υλοποιεί σειρά δραστηριοτήτων όπως διοργάνωση ενημερωτικών εκδηλώσεων για το κοινό, σεμινάρια προς εκπαιδευτικούς, προώθηση θεμάτων που σχετίζονται με την ασφάλεια στο Διαδίκτυο στα ΜΜΕ, δημιουργία πολυμορφικού online και έντυπου ενημερωτικού υλικού, καθώς και τηλεοπτικές και ραδιοφωνικές καμπάνιες. Το Saferinternet.gr συνεργάζεται με εκπροσώπους του κράτους, της βιομηχανίας των νέων τεχνολογιών καθώς και με μη Κυβερνητικές Οργανώσεις στην Ελλάδα και το εξωτερικό με πρωταρχικό σκοπό την εξασφάλιση ενός ασφαλέστερου διαδικτυακού περιβάλλοντος.

Η δράση Saferinternet.gr αποτελεί τον εθνικό εκπρόσωπο του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης Insafe, με 27 μέλη στην Ευρώπη. Στα πλαίσια του Insafe το Saferinternet.gr ανταλλάσει απόψεις, εμπειρίες, βέλτιστες πρακτικές και πληροφοριακό υλικό με τα άλλα Ευρωπαϊκά Κέντρα.
Το Saferinternet.gr αποτελεί μια από τις τρεις δράσεις του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, δίπλα στην γραμμή καταγγελιών Safeline και τη γραμμή βοηθείας «ΥποΣΤΗΡΙΖΩ».

Η εκστρατεία SaferInternet πιστεύει ότι η απάντηση στους πιθανούς κινδύνους του Διαδικτύου βρίσκεται τόσο στην εκπαίδευση, όσο και στην πρόληψη:

- Εκπαίδευση που συνεισφέρει στην απαραίτητη αλλαγή του τρόπου συμπεριφοράς, και που δημιουργεί μια υπεύθυνη στάση απέναντι στο Διαδίκτυο.
- Πρόληψη, έτσι ώστε να προωθηθούν οι θετικές πλευρές και τα οφέλη της χρήσης των διαδραστικών τεχνολογιών.

Ο Ελληνικός κόμβος ασφαλούς Διαδικτύου, μέσα από την εμπειρία του και την καθημερινή του επαφή με το κοινό, θεωρεί ότι στην επίτευξη της ασφάλειας των διαδραστικών μέσων μπορούν να συμβάλουν οι παρακάτω δράσεις:

- Δράσεις που αφορούν στα (ποινικά και άλλα) αδικήματα που τελούνται μέσω των μέσων.
- Δράσεις για την διασφάλιση της υγείας και ευημερίας ανηλίκων και ενηλίκων.
- Δράσεις που στοχεύουν στην ανάπτυξη της «ικανότητας στην χρήση των μέσων».

Ο Ελληνικός κόμβος ασφαλούς Διαδικτύου αναλαμβάνει δράσεις που στοχεύουν στην ενημέρωση και αφύπνιση του Ελληνικού κοινού για τη σημασία της «ικανότητας στη χρήσης των μέσων». Έχει όμως ως στόχο του,

από το 2009 και μετά, και με τη στενή συνεργασία της Μονάδας Εφηβικής Υγείας της β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών, να ασχοληθεί πολύ στενά με το θέμα της υγείας των νέων σε σχέση με τη χρήση του Διαδικτύου.

Η εκστρατεία SaferInternet πιστεύει, επίσης, ότι είναι ευθύνη όλων των κοινωνικών φορέων να λάβουν τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των παιδιών στο Διαδίκτυο και τη διασφάλιση των δικαιωμάτων τους στον κόσμο των νέων διαδραστικών τεχνολογιών και της κοινωνίας της πληροφορίας.

Ο Ελληνικός κόμβος ασφαλούς Διαδικτύου απευθύνεται σε διάφορες ομάδες στόχους: εκπαιδευτικά ιδρύματα, γονείς, κοινωνικούς λειτουργούς, βιβλιοθηκάριους, καταναλωτικές οργανώσεις και παιδιά, καθώς και στη βιομηχανία, τις κυβερνήσεις και τα μέσα μαζικής ενημέρωσης.

Συντονιστής του Ελληνικού κόμβου ασφαλούς Διαδικτύου και της εκστρατείας είναι η Extreme Media Solutions, ενώ εταίρος για δράσεις τηλεοπτικής και ραδιοφωνικής προβολής, από το 2007, είναι η ΕΡΤ.

6.5 Safe Internet από την CYTANET[110]

Η υπηρεσία Safe Internet που προσφέρει η CYTANET, είναι μια υπηρεσία φιλτραρίσματος διαδικτυακού περιεχομένου με στόχο να βοηθήσει τους χρήστες να προστατευτούν από το παράνομο, ανεπιθύμητο και επιβλαβές περιεχόμενο του Διαδικτύου. Η υπηρεσία προσφέρεται σαν δωρεάν διευκόλυνση στους συνδρομητές της CYTANET. Με έναν εύκολο και πρακτικό τρόπο, οι χρήστες μπορούν να επιλέξουν κατηγορίες διαδικτυακού περιεχομένου, συγκεκριμένες ιστοσελίδες ή και εφαρμογές Διαδικτύου, στις οποίες δεν θέλουν να επιτρέψουν την πρόσβαση. Μπορούν, επίσης, να καθορίσουν το χρόνο επιτρεπόμενης πρόσβασης στο Διαδίκτυο για κάθε χρήστη του ηλεκτρονικού τους υπολογιστή.

[110] http://www.cytanet.com.cy/Services/safe-internet/GR/faq/

Η υπηρεσία διατίθεται σε τρεις διαφορετικές κατηγορίες ανάλογα το περιβάλλον που θα χρησιμοποιηθεί:

1. Οικογενειακό περιβάλλον
2. Εκπαιδευτικό περιβάλλον
3. Επιχειρηματικό περιβάλλον

Μερικά από τα σημαντικότερα πλεονεκτήματα της υπηρεσίας Safe Internet είναι:

- Δυνατότητα εγκατάστασης του λογισμικού στους υπολογιστές. Ο αριθμός των υπολογιστών στους οποίους μπορεί να εγκατασταθεί το λογισμικό εξαρτάται από το πακέτο υπηρεσίας που έχει επιλεχθεί.
- Δυνατότητα δημιουργίας διαφορετικών προφίλ χρηστών καθορίζοντας τις κατηγορίες περιεχομένου που δεν θα επιτρέπεται η πρόσβαση και τις εφαρμογές Η/Υ που δεν θα μπορούν να χρησιμοποιηθούν κ.λπ.
- Δυνατότητα επιλογής ανάμεσα σε περισσότερες από 30 διαφορετικές κατηγοριών για φιλτράρισμα όπως Ναρκωτικά, Κυβεία, Βία, Περιεχόμενο για ενηλίκους κ.λπ. Σε αυτές περιλαμβάνονται επίσης και υποκατηγορίες όπως Παιχνίδια, Πολιτική, Αθλητικά, Διαδικτυακές Αγορές, Προγράμματα Υποκλοπής προσωπικών δεδομένων κ.λπ.
- Δυνατότητα για μπλοκάρισμα εφαρμογών Η/Υ όπως εφαρμογές ηλεκτρονικού ταχυδρομείου, άμεσης αποστολής μηνυμάτων (Instant Messaging), P2P, FTP κ.λπ.
- Δυνατότητα δημιουργίας καταλόγου με διαδικτυακές διευθύνσεις στις οποίες δεν επιθυμείτε ο χρήστης να έχει ή/και να μην έχει πρόσβαση (Λευκή και Μαύρη λίστα - White and Black list).
- Δυνατότητα καθορισμού ημερών και ωρών πρόσβασης του Διαδικτύου.
- Στατιστικά αποτελέσματα χρήσης της υπηρεσίας και γραφική απεικόνιση των αποτελεσμάτων φιλτραρίσματος.

- Εξ' αποστάσεως διαχείριση της υπηρεσίας. Ο Διαχειριστής της υπηρεσίας μπορεί από οποιονδήποτε υπολογιστή να διαχειριστεί τα προφίλ των χρηστών της υπηρεσίας του. Το μόνο που χρειάζεται είναι μια ενεργή σύνδεση στο Διαδίκτυο, χωρίς η εγκατάσταση του λογισμικού να είναι αναγκαία.

6.6 Μνημόνιο για την ασφαλή χρήση του Διαδικτύου από μαθητές[111]

Μνημόνιο συνεργασίας για την υλοποίηση δράσεων σε θέματα ασφαλούς χρήσης και κατάχρησης του Διαδικτύου από τους μαθητές, υπέγραψαν στις 4/6/2010, στο Υπουργείο Παιδείας, η Υπουργός Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων, Άννα Διαμαντοπούλου, ο καθηγητής Παιδιατρικής και Διευθυντής της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) της Β΄ Πανεπιστημιακής Παιδιατρικής Κλινικής του Νοσοκομείου Π. & Α. Κυριακού, Δημήτριος Καφετζής και η Επιστημονική Υπεύθυνη της Μ.Ε.Υ. και Λέκτορας Παιδιατρικής – Εφηβικής Παιδιατρικής του Πανεπιστημίου Αθηνών, Άρτεμις Τσίτσικα.

Συγκεκριμένα, προβλέπονται οι κάτωθι δράσεις:

1. Διοργάνωση εκπαιδευτικών σεμιναρίων απευθυνόμενων σε εκπαιδευτικούς, με τη θεσμική στήριξη του Υπουργείου Παιδείας και θέμα την ασφαλή χρήση και την κατάχρηση του Διαδικτύου για τον παιδί και τον έφηβο, σε κομβικά σημεία της χώρας (προτεινόμενος αριθμός 3-6). Στόχος των σεμιναρίων είναι η εκπαίδευση σχολικών συμβούλων / διευθυντών σχολείων, έτσι ώστε με το πέρας του σεμιναρίου τα άτομα αυτά να μεταφέρουν την αποκτηθείσα γνώση στους εκπαιδευτικούς της περιφέρειας / του σχολείου τους.
2. Δημιουργία ολιγοσέλιδου ηλεκτρονικού υλικού με χρήσιμες συμβουλές για την ασφαλή χρήση του Διαδικτύου και πρόλογο από την ηγεσία του

[111] http://www.minedu.gov.gr/publications/docs/keimeno_mnhmonioy_100604.pdf
http://www.minedu.gov.gr/publications/docs/dt_ypografh_mnhmonioy_dhlwseis__100604.pdf

Υπουργείου Παιδείας,. Το δημιουργικό και το περιεχόμενο του φυλλαδίου θα επιμεληθούν η Μ.Ε.Υ. και το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου. Το Υπουργείο θα αναλάβει την ανάρτηση του υλικού στο Διαδίκτυο και την προώθησή του σε όλα τα σχολεία της χώρας προς ενημέρωση των εκπαιδευτικών και των μαθητών.

3. Δημοσιοποίηση με την συνεργασία των δύο φορέων των δράσεων για τον ετήσιο εορτασμό της Ημέρας Ασφαλούς Διαδικτύου, ο οποίος πραγματοποιείται σε περισσότερες από 60 χώρες σε όλον τον κόσμο τη δεύτερη Τρίτη του μήνα Φεβρουαρίου και συντονίζεται σε εθνικό επίπεδο από το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου.
4. Παραχώρηση από τη Δράση Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου σε ηλεκτρονική μορφή (pdf) των δύο εκπαιδευτικών του εγχειριδίων «Μαθαίνω να σερφάρω δημιουργικά και με ασφάλεια – τα πρώτα βήματα» και «Μαθαίνω να σερφάρω δημιουργικά και με ασφάλεια – για προχωρημένους», με σκοπό τη δημοσίευσή τους στην ιστοσελίδα του Πανελλήνιου Σχολικού Δικτύου, στον ελεγχόμενο χώρο για εκπαιδευτικούς, με την επισήμανση στους τελικούς δικαιούχους για τον κοινωφελή σκοπό του υλικού που δημιουργήθηκε με την συγχρηματοδότηση της Ευρωπαϊκής Επιτροπής και για τη χρήση του υλικού αποκλειστικά μέσα στις σχολικές τάξεις.
5. Διοργάνωση ενημερωτικής εκστρατείας από τη Μ.Ε.Υ. σε σχολεία της χώρας με θέμα το ασφαλές Διαδίκτυο σε συνεργασία με το Υπουργείο.
6. Ενημέρωση των καθηγητών και μαθητών πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης για τις δράσεις της Μ.Ε.Υ. και του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου με ευθύνη του Υπουργείου.
7. Υλοποίηση επιμορφωτικών προγραμμάτων με στόχο την δια βίου εκπαίδευση των εκπαιδευτικών σε θέματα ασφαλούς χρήσης και κατάχρησης του Διαδικτύου και απώτερο στόχο την διεύρυνση του προγράμματος αυτού για όλους τους εκπαιδευτικούς.

8. Σύσταση κοινής από τους δύο φορείς επιτροπής που θα ασχολείται με θέματα ασφαλούς χρήσης και κατάχρησης του Διαδικτύου για τους μαθητές των σχολείων και εξειδίκευσης των προβλεπομένων από το παρόν δράσεων.

6.7 SafeLine[112]

Η SafeLine είναι μια Ελληνική ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο η οποία ιδρύθηκε το 2003, με πρωτοβουλία του Ιδρύματος Τεχνολογίας και Έρευνας του Ιδρύματος Μείζονος Ελληνισμού, της Safenet και της Forthnet. Υποστηρίζεται από το Safer Internet Programme της Ευρωπαϊκής Ένωσης και υλοποιείται από τους οργανισμούς ΙΤΕ-ΙΠ Ίδρυμα Τεχνολογίας και Έρευνας, Ινστιτούτο Πληροφορικής και SAFENET Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Διαδικτύου.

Επιπλέον, από τον Οκτώβριο του 2005, η SafeLine είναι μέλος του INHOPE, του Ευρωπαϊκού Συνδέσμου Παροχών Ανοικτών Γραμμών για το Διαδίκτυο, γεγονός που επιτρέπει την καλύτερη συνεργασία με αντίστοιχους φορείς άλλων ευρωπαϊκών χωρών και την αποτελεσματικότερη επεξεργασία των καταγγελιών. Προκειμένου να εξασφαλίσει όσο το δυνατόν αποτελεσματικότερη λειτουργία, η SafeLine συνεργάζεται με τους Φορείς Παροχής Υπηρεσιών Διαδικτύου (ISP), το Ακαδημαϊκό Δίκτυο "ΕΔΕΤ", το Σχολικό Δίκτυο, την Αρχή Διατήρησης Απορρήτου των Επικοινωνιών, Ενώσεις Καταναλωτών, την Δίωξη Ηλεκτρονικού Εγκλήματος της Αθήνας και της Θεσσαλονίκης και την Αρχή Προστασίας Προσωπικών Δεδομένων.

Πρωταρχικό της μέλημα είναι η εξάλειψη της παιδικής πορνογραφίας, η καταπολέμηση κάθε είδους παράνομου περιεχομένου στο Διαδίκτυο, καθώς και θέματα ρατσισμού, ηλεκτρονικής χαρτοπαιξίας και προστασίας πνευματικής ιδιοκτησίας και καταναλωτών. Η SafeLine δέχεται καταγγελίες για ιστοσελίδες ή υπηρεσίες νέων (newsgroups) στο Διαδίκτυο οι οποίες περιέχουν εικόνες

[112] http://www.safeline.gr/
http://www.infosoc.gr/infosoc/el-GR/TodayNews/saferinternet_04-03-2009.htm

κακομεταχείρισης παιδιών, ρατσιστικό και ξενοφοβικό περιεχόμενο που παραβαίνει την Ελληνική νομοθεσία ή άλλο παράνομο περιεχόμενο. Οι καταγγελίες μπορούν να κατατεθούν μέσω ηλεκτρονικής φόρμας, ταχυδρομείου, ηλεκτρονικού ταχυδρομείου και τηλεφωνικά.

Τα μέλη της SafeLine εξετάζουν την καταγγελία και ύστερα την αναφέρουν στις αρχές για περαιτέρω επεξεργασία. Ό χρήστης που καταθέτει μια καταγγελία (http://www.safeline.gr/report), μπορεί να πληροφορηθεί για το αποτέλεσμα της μόλις αυτό είναι επιτρεπτό. Αν κάποιος χρήστης το επιθυμεί μπορεί να κρατήσει την ανωνυμία του. Τα στοιχεία των χρηστών που καταθέτουν καταγγελίες είναι άκρως εμπιστευτικά.

Εκπρόσωποι της ομάδας της SafeLine λαμβάνουν μέρος σε διάφορες δραστηριότητες και συναντήσεις όπως και επισκέπτονται κατά τη διάρκεια του σχολικού έτους ιδρύματα της Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης (Δημοτικά, Γυμνάσια και Λύκεια). Η SafeLine επισκέπτεται σχολεία και παρουσιάζει την ανοιχτή γραμμή σε μαθητές, καθηγητές και εκπαιδευτικούς. Η άδεια για τις επισκέψεις αυτές χορηγείται από το Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων μέσω προγραμμάτων Αγωγής Υγείας. Στις ενημερώσεις αυτές οι εκπρόσωποι της ομάδας παρουσιάζουν την ιστοσελίδα στους μαθητές, τους συμβουλεύουν, τους δίνουν πληροφορίες για τους κινδύνους του Διαδικτύου και συζητούν μαζί τους για θέματα που τους απασχολούν.

6.7.1 Στατιστικά στοιχεία SafeLine[113]

Ο αριθμός των καταγγελιών που έλαβε η SafeLine τους πρώτους 8 μήνες του 2010, έφτασε τις 1.270 (αύξηση 114% σε σχέση με το αντίστοιχο διάστημα του 2009). Οι καταγγελίες αυτές αφορούν σε παράνομο περιεχόμενο, ή παράνομες δραστηριότητες, στο Διαδίκτυο, αντιστοιχούν δε σε περίπου 8 καταγγελίες για κάθε εργάσιμη ημέρα του έτους. Ο αριθμός των καταγγελιών που λαμβάνει

[113] http://saferinternet.gr/index.php?parentobjId=Page75&p=0

ετησίως η SafeLine βρίσκεται σε μια ανοδική τροχιά, σχεδόν από την ίδρυσή της το 2003, όπως φαίνεται και από το διάγραμμα παρακάτω. Τα τελευταία 3 χρόνια οι καταγγελίες αυξάνονται κατά 1.250 ανά έτος.

Οι αιτίες της γοργής αύξησης στον αριθμό των καταγγελιών, που παρατηρείται από το 2008, είναι δύσκολο να προσδιοριστούν με ακρίβεια, σίγουρα όμως οφείλονται και στην αύξηση της ορατότητας της SafeLine, στην αύξηση του αριθμού των χρηστών του Διαδικτύου και στη βελτίωση της συνειδητοποίησής τους: Μια ανοικτή γραμμή, σαν τη SafeLine, αποτελεί στην ουσία το μόνο τρόπο χαρτογράφησης της παράνομης πλευράς του Διαδικτύου και αυτή η χαρτογράφηση βοηθάει στον περιορισμό της κακοποίησης παιδιών, του ρατσισμού, της διαδικτυακής απάτης, κ.λπ. Η SafeLine είναι σε θέση να διαπιστώσει ότι οι χρήστες του Διαδικτύου, που νοιάζονται για την αυτονομία του και συμβάλλουν σε αυτήν την προσπάθεια, αυξάνονται χρόνο με το χρόνο.

Σε σύγκριση, το δίκτυο INHOPE δέχεται περίπου 50.000 καταγγελίες ανά μήνα, ο αριθμός των οποίων αυξάνει σταθερά με αργό ρυθμό (~300 καταγγελίες ανά μήνα).

Οι καταγγελίες που δέχεται η SafeLine, αφού επιβεβαιωθούν, κατηγοριοποιούνται ανάλογα με το είδος του παράνομου περιεχομένου. Τους τελευταίους 20 μήνες οι καταγγελίες αφορούσαν κατά:

- 21% σε κακοποίηση παιδιών, πορνογραφία, κ.λπ.
- 34% σε ρατσισμό, ξενοφοβία, εξύβριση και συκοφαντική δυσφήμηση.
- 19% σε παραβίαση προσωπικών δεδομένων και υποκλοπή ταυτότητας.
- 26% σε οικονομικές απάτες μέσω διαδικτυακών αγορών, θέματα copyright και παράνομο spam.

Σε σύγκριση, το INHOPE εμφανίζει τα παρακάτω ποσοστά για την περίοδο μέχρι και το πρώτο εξάμηνο του 2010:

- 20% σε κακοποίηση παιδιών

- 8% σε πορνογραφία, κ.λπ.
- 0,5% σε ρατσισμό
- 9% σε spam

Κατά τη διάρκεια των τριών τελευταίων εξαμήνων, οι καταγγελίες για ρατσισμό, ξενοφοβία, εξύβριση και συκοφαντική δυσφήμηση έχουν αυξηθεί δραματικά, ενώ οι υπόλοιπες κατηγορίες αυξήθηκαν με αργό ρυθμό.

Ανοδικό ήταν και το ποσοστό των αναφορών για τα συστήματα κοινωνικής δικτύωσης (social networks) καθώς αντιστοιχεί στο 38% των καταγγελιών και αφορά κυρίως την υποκλοπή ταυτότητας, ηλεκτρονικό εκφοβισμό (cyber bullying), αποπλάνηση ανηλίκων (grooming), ρατσισμό και υποκλοπή κωδικών πρόσβασης.

Οι καταγγελίες που αφορούν σε κακοποίηση παιδιών καταχωρούνται και στην κοινή βάση δεδομένων του INHOPE. Τόσο από τη σύγκριση των στατιστικών στοιχείων της SafeLine, όσο και των ανάλογων παγκόσμιων στατιστικών στοιχείων του INHOPE, διαφαίνεται ότι λίγες είναι οι διαφορές μεταξύ του τι καταγγέλλουν οι Έλληνες και τι οι αλλοδαποί χρήστες του Διαδικτύου. Αυτό προφανώς οφείλεται στην παγκόσμια φύση του Διαδικτύου.

6.8 Γραμμή βοηθείας «ΥποΣΤΗΡΙΖΩ»[114]

Η Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) της Β΄ Παιδιατρικής Κλινικής του πανεπιστημίου Αθηνών, που εδρεύει στο νοσοκομείο Παίδων «Π & Α Κυριακού», διαχειρίζεται τη γραμμή βοηθείας «ΥποΣΤΗΡΙΖΩ» του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου.

Η γραμμή αυτή, απευθύνεται σε παιδιά και εφήβους και τις οικογένειές τους, παρέχοντας υποστήριξη και συμβουλές για θέματα που σχετίζονται με τη χρήση του Διαδικτύου, του κινητού τηλεφώνου και των ηλεκτρονικών παιχνιδιών

[114] http://www.saferinternet.gr/index.php?parentobjId=Page187
http://www.ant1online.gr/Ereuna/Pages/20102/55cb7ef3-cfcf-4bb4-a0bb-057d3eeefc7e.aspx
http://www.tanea.gr/default.asp?pid=96&ct=1&artid=4559795&nid=0&rid=#

(παρενόχληση, εξάρτηση, επιβλαβές περιεχόμενο, παιδοφιλία, κ.α.). Η γραμμή βοηθείας «ΥποΣΤΗΡΙΖΩ» είναι χωρίς χρέωση για αστικές και υπεραστικές κλήσεις (με την υποστήριξη του ΟΤΕ). Στελεχώνεται από εξειδικευμένους παιδοψυχολόγους σε θέματα χρήσης – κατάχρησης Διαδικτύου για τα παιδιά και τους εφήβους. Το προσωπικό της γραμμής προσφέρει συμβουλές, παρέχει ψυχολογική υποστήριξη, παραπέμπει στη γραμμή καταγγελιών Safeline.gr και στη Δίωξη Ηλεκτρονικού Εγκλήματος για περιπτώσεις ηλεκτρονικού εγκλήματος. Λειτουργεί στη Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.), στο Παράρτημα του Νοσοκομείου Παίδων «Π. & Α. Κυριακού».

Μπορεί κανείς να επικοινωνήσει με το προσωπικό της γραμμής είτε καλώντας στον αριθμό χωρίς χρέωση για αστικές και υπεραστικές κλήσεις 800 11 800 15 από Δευτέρα έως Παρασκευή και ώρες 09:00 - 15:00, είτε αποστέλλοντας ηλεκτρονικό μήνυμα στο help@saferinternet.gr.

6.8.1 Στατιστικά στοιχεία γραμμής βοηθείας «ΥποΣΤΗΡΙΖΩ»[115]

Η γραμμή βοηθείας «ΥποΣΤΗΡΙΖΩ» δέχτηκε κατά το πρώτο διάστημα λειτουργίας της (Αύγουστος 2009 - Μάιος 2010) 982 αιτήματα, είτε μέσω τηλεφώνου είτε μέσω ηλεκτρονικού ταχυδρομείου, σχετικά με προβλήματα που προέκυψαν κατά τη χρήση του Διαδικτύου.

Το περιεχόμενο των αιτημάτων που υποβλήθηκαν στη γραμμή έχει ως εξής:

- Αναζήτηση πληροφοριών / συμβουλών: 404 (41,14%)
- Εξάρτηση: 301 (35,8%)
- Οικονομικές απάτες: 75 (7,64%)
- Επικίνδυνο περιεχόμενο: 62 (6,31%)
- Βία, εκφοβισμός: 56 (5,7%)
- Κλοπή προσωπικών δεδομένων: 54 (5,54%)
- Ανορεξία: 13 (1,32%)

[115] http://saferinternet.gr/index.php?parentobjId=Page75&p=0

- Αποπλάνηση ανηλίκων: 10 (1,02%)
- Πρόθεση για αυτοκτονία: 3 (0,03%)
- Εκβιασμός: 2 (0,02%)
- Άλλο: 2 (0,02%)

Το προσωπικό της γραμμής βοηθείας έδινε συμβουλές και πληροφορίες και παρείχε ψυχολογική υποστήριξη (608 αναφορές), παρέπεμπε στη γραμμή καταγγελιών Safeline.gr και στη Δίωξη Ηλεκτρονικού Εγκλήματος για περιπτώσεις ηλεκτρονικού εγκλήματος (152 αναφορές) ή σε άλλους αρμόδιους φορείς αντίστοιχα με τη φύση της αναφοράς (π.χ. καταναλωτικές οργανώσεις κ.λπ.) (118 αναφορές). Τέλος, 107 περιπτώσεις παραπέμφθηκαν στα ιατρεία της Μονάδας Εφηβικής Υγείας για να ενταχθούν στο πρόγραμμα της Μ.Ε.Υ. για τους εφήβους με υπερβολική ενασχόληση με το Διαδίκτυο.
Το 85,5% των ατόμων που κάλεσαν τη γραμμή ήταν ενήλικες (ως επί το πλείστον γονείς), το 10,5% επαγγελματίες (π.χ. εκπαιδευτικοί) και το 4% ανήλικοι.

6.9 Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος[116]

Το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας ερευνά υποθέσεις που έχουν σχέση με το διαδικτυακό έγκλημα. Οι πολίτες μπορούν να απευθύνονται στο Τμήμα δίωξης Ηλεκτρονικού Εγκλήματος για εγκληματικές πράξεις που γίνονται μέσω Διαδικτύου και τιμωρούνται από τη νομοθεσία.

Οι εγκληματικές πράξεις που συνήθως καταγγέλλονται είναι:

- Παιδική πορνογραφία (Ιστοσελίδες –chatroom με σκοπό την διακίνηση υλικού παιδικής πορνογραφίας – αποπλάνηση ανηλίκων).

[116] http://www.dart.gov.gr/NewsInner.aspx?new_id=130&nwc_id=22
http://www.minpress.gr/minpress/index/currevents/draseis_paidia_mme_safe_internet.htm

- Απάτες μέσω Διαδικτύου (Ισπανικό Λόττο - Νιγηριανές επιστολές - Εικονικές Δημοπρασίες κ.ά.)
- Cracking (ψηφιακοί βανδαλισμοί-Deface και άλλα)
- Διακίνηση ή Πειρατεία Λογισμικού (online πώληση Mp3 και κινηματογραφικών ταινιών, αλλά και λογισμικού)
- Απάτες με πιστωτικές κάρτες μέσω Διαδικτύου (Ηλεκτρονικές Αγορές on line μέσω ιστοσελίδων απατηλών-χρέωση πιστωτικών καρτών εν αγνοία του κατόχου)
- Διακίνηση ναρκωτικών. (Online αγορά και πώληση ναρκωτικών ουσιών)
- Συκοφαντική δυσφήμηση και παραβίαση προσωπικών δεδομένων μέσω Διαδικτύου (Δημοσίευση ερωτικών φωτογραφιών και προσωπικών στοιχείων εν αγνοία των θυμάτων)
- Εκβίαση – Απειλές μέσω Διαδικτύου

Το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στελεχώνεται από εξειδικευμένους αστυνομικούς οι οποίοι περιηγούνται στο Διαδίκτυο, με σκοπό την πρόληψη του διαδικτυακού εγκλήματος, ενώ παράλληλα διερευνά καταγγελίες πολιτών και διενεργεί σχετικές προανακρίσεις.

Η έρευνα του Διαδικτύου σχετικά με την πρόληψη πραγματοποιείται σε διαδικτυακούς τόπους (chat rooms, news groops, blogs και ιστοσελίδες) των οποίων το περιεχόμενο είναι σε κοινή θέα και στα οποία έχουν πρόσβαση όλοι οι χρήστες του Διαδικτύου.

Σε περίπτωση που προκύψει εκμετάλλευση ανηλίκου ή διακίνηση υλικού παιδικής πορνογραφίας ή οποιαδήποτε άλλη εγκληματική συμπεριφορά, εφαρμόζονται οι προβλεπόμενες διαδικασίες εντοπισμού, σύμφωνα με τις ισχύουσες διατάξεις. Ταυτόχρονα, εφόσον συντρέχουν οι προϋποθέσεις αυτοφώρου εγκλήματος, η Ελληνική Αστυνομία προβαίνει στη σύλληψη των δραστών και την προσαγωγή τους ενώπιον της δικαιοσύνης.

Τρόποι επικοινωνίας:

Για Αθήνα:

- Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος
  Λ. Αλεξάνδρας 173 Τ.Κ. 115 22 Αθήνα
  Fax: 210 6476462
  Τηλέφωνα: 210 6476464, 210 6476000
  E-mail: ccu@ath.forthnet.gr

Για Θεσσαλονίκη:

- Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος
  Μοναστηρίου 241 Τ.Κ. 546 28 Θεσσαλονίκη
  Fax: 2310-559929
  Τηλέφωνα: 2310 388370-5, 2310 388000
  E-mail: info@cybercrime.gr

6.10 Ελληνική Καταναλωτική Οργάνωση[117]

Η Ε.ΚΑΤ.Ο, είναι μια Πανελλήνια Καταναλωτική Οργάνωση, η οποία ιδρύθηκε στην Ελλάδα με Δικαστική Επικύρωση στις 26 Μαρτίου 1999. Έδρα της Οργάνωσης ορίζεται η Θεσσαλονίκη και μπορεί να ιδρύει γραφεία, υποκαταστήματα, επιτροπές, κ.λπ., σε όλη την Ελληνική επικράτεια, μετά από απόφαση του Διοικητικού Συμβουλίου. Η Ελληνική Καταναλωτική Οργάνωση είναι μη κερδοσκοπικού χαρακτήρα. Κύριος στόχος της είναι η προστασία των καταναλωτών, η επιμόρφωση, η εκπαίδευσή τους και ειδικότερα η διακήρυξη των θεμελιωδών δικαιωμάτων των καταναλωτών. Στην ιστοσελίδα της οργάνωσης μπορεί ο καταναλωτής να ενημερωθεί για τα δικαιώματα του, για έρευνες, προγράμματα και να υποβάλει μία καταγγελία.

Τρόποι επικοινωνίας:

- Τηλέφωνο: 2310 226426

[117] http://www.ekato.org/index.html

- Fax: 2310 908519
- E-mail: info@ekato.org

6.11 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών[118]

Η Α.Δ.Α.Ε. είναι μία ανεξάρτητη Αρχή που έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Οι πολίτες μπορούν να απευθύνονται στην Α.Δ.Α.Ε για τα παρακάτω αδικήματα:

- Υποκλοπή της τηλεφωνικής τους συνομιλίας είτε γίνεται από σταθερό είτε κινητό τηλέφωνο
- Υποκλοπή SMS- MMS στην κινητή τηλεφωνία
- Γνώση δεδομένων θέσης και κίνησης από μη εξουσιοδοτημένα άτομα και κτήσης τους με παράνομο τρόπο (πχ. εξερχόμενες κλήσεις, εισερχόμενες κλήσεις, γνώση απόρρητου αριθμού)
- Υποκλοπή e-mail
- Γνώση της IP κίνησης συνδρομητή Διαδικτύου από μη εξουσιοδοτημένα άτομα και κτήσης τους με παράνομο τρόπο
- Παράνομη πρόσβαση σε mail server για υποκλοπή e-mails.

6.12 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[119]

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) είναι μια συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή. Ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο Ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία

[118] http://www.dart.gov.gr
[119] http://www.dpa.gr/

95/46/ΕΚ. Η Οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης.

Επίσης, όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η Α.Π.Δ.Π.Χ. εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002.

Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006.

Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ).

Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της Ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Στην περίπτωση που θεωρεί κάποιος, ότι θίγεται κατά οποιονδήποτε τρόπο η προστασία των προσωπικών του δεδομένων, μπορεί να προσφύγει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και να υποβάλει καταγγελία στην ηλεκτρονική διεύθυνση http://www.dpa.gr/

6.13 Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου[120]

Τον Ιανουάριο του 2002 γεννήθηκε η ιδέα για την καθιέρωση του εορτασμού της Παγκόσμιας Ημέρας Ασφαλούς Διαδικτύου «Safer Internet Day». Η ιδέα γίνεται πράξη από το 2004 κάθε δεύτερη Τρίτη του Φεβρουαρίου και αποτελεί κορύφωση των δράσεων όλων των Εθνικών Κόμβων Ασφαλούς Διαδικτύου. Στις 9 Φεβρουαρίου 2010 εορτάστηκε για έβδομη συνεχή χρονιά σε περισσότερες από 60 χώρες. Η ημέρα αυτή οργανώνεται από το Πανευρωπαϊκό Δίκτυο Εθνικών Κόμβων INSAFE, την Ευρωπαϊκή Επιτροπή και αποτελεί εφαλτήριο ευαισθητοποίησης μικρών και μεγάλων στα θέματα που αφορούν την ασφαλή και ηθικά σωστή χρήση του Διαδικτύου, του κινητού τηλεφώνου και όλων των διαδραστικών τεχνολογιών που είναι πια κομμάτι της καθημερινότητάς των πολιτών.

Η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου αποτελεί σταθμό προβληματισμού για τους τρόπους με τους οποίους μπορούν οι ενήλικες να προστατεύσουν τα παιδιά και τους νέους από παράνομο και επιβλαβές υλικό που βρίσκεται στο Διαδίκτυο, αλλά και απολογισμού των πεπραγμένων για να επιτευχθεί ο συγκεκριμένος στόχος. Ως μέρος μιας συνεκτικής προσέγγισης από την Ευρωπαϊκή Ένωση, το Πρόγραμμα Ασφαλούς Διαδικτύου αποσκοπεί στην προώθηση της ασφαλέστερης χρήσης του Διαδικτύου και των νέων διαδικτυακών τεχνολογιών, ιδίως για τα παιδιά, καθώς επίσης και στην καταπολέμηση του παράνομου περιεχομένου στο Διαδίκτυο και του περιεχομένου που είναι ανεπιθύμητο από τον τελικό χρήστη.

Η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου εορτάζεται με την διοργάνωση ημερίδων, σεμιναρίων, συνέδριων, παρουσιάσεων, παιδικών διαγωνισμών και άλλων εκδηλώσεων.

[120] http://dide.ilei.sch.gr/keplinet/education/sid.php#sid2009
http://www.cyberethics.info/cyethics2/UserFiles/file/Safer_Internet_Day_2009Greek.pdf
http://www.ant1online.gr/Ereuna/Pages/20102/55cb7ef3-cfcf-4bb4-a0bb-057d3eeefc7e.aspx

6.14 SimSafety[121]

Το έργο «SimSafety: Flight Simulator for Internet Safety» με συγχρηματοδότηση από την Ευρωπαϊκή, απευθύνεται σε γονείς, μαθητές κι εκπαιδευτικούς και προσεγγίζει ζητήματα ασφαλούς χρήσης του Διαδικτύου υπό το πρίσμα της συνεργασίας και της αλληλεγγύης μεταξύ των νεότερων και των μεγαλύτερων 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.

Στο πλαίσιο του έργου αναπτύσσεται σε Διαδικτυακό Εικονικό Περιβάλλον το σενάριο ενός παιχνιδιού που ως στόχο έχει την εξοικείωση των παιχτών με πιθανούς κινδύνους, εκθέτοντάς τους σε αυτούς με ασφαλή τρόπο και με τη συνοδεία ενηλίκων. Οι παίχτες καλούνται να καλλιεργήσουν την κριτική τους σκέψη και να αποκαλύψουν / αντιμετωπίσουν τους πιθανούς κινδύνους, αναπτύσσοντας δεξιότητες, αποκτώντας γνώσεις κι εν γένει καλλιεργώντας μια νέα νοοτροπία, εκείνη της ασφαλούς χρήσης του Διαδικτύου.

Στο έργο συμμετέχουν εταίροι από διαφορετικές χώρες (Ελλάδα, Κύπρο, Φιλανδία, Πορτογαλία, Ρουμανία, Αγγλία) οι οποίοι, με επικεφαλής το Ελληνικό Ανοιχτό Πανεπιστήμιο, εξειδικεύονται σε συμπληρωματικούς επιστημονικούς τομείς (π.χ. εκπαίδευση ανηλίκων, εκπαίδευση ενηλίκων, ανάπτυξη εκπαιδευτικού λογισμικού κ.α.) και συνεργάζονται στενά ως προς το θεωρητικό σχεδιασμό και την υλοποίηση του παιχνιδιού. Ικανός αριθμός χωρών (9) αναμένεται να εμπλακεί στις εκπαιδευτικές δραστηριότητες με παιγνιώδη τρόπο, ανταλλάσσοντας εμπειρίες κι επιτυχημένα παραδείγματα και εξασφαλίζοντας τη διάδοση των αποτελεσμάτων στο ευρύτερο κοινό.

Το έργο στοχεύει στην αντίληψη συγκεκριμένων ζητημάτων που αφορούν στην ασφάλεια του Διαδικτύου στην πραγματική τους διάσταση και προσκαλεί τους γονείς και τους εκπαιδευτικούς να αναλάβουν το ρόλο του «συνοδού» σε αυτή

[121] http://dide.ilei.sch.gr/keplinet/articles/saferinternet.php

την απόπειρα και με τον τρόπο αυτό να έλθουν πιο κοντά στα ζητήματα που απασχολούν τα παιδιά ή/και τους μαθητές τους.

Το έργο απευθύνεται σε μαθητές ηλικίας 9 με 11 ετών (αν και τα ηλικιακά όρια είναι ελαστικά) ενώ αυτό που θα προσκληθούν να κάνουν οι γονείς, οι μαθητές και οι εκπαιδευτικοί είναι, παίζοντας το συγκεκριμένο παιχνίδι είτε μέσα από το σχολείο είτε μέσα από το σπίτι σε χρόνο που θα συναποφασιστεί μεταξύ των συμμετεχόντων και των εταίρων του έργου, να προσφέρουν μέσα από συστηματική και μεθοδευμένη λήψη ανατροφοδότησης, τη δική τους άποψη για τη προστιθέμενη αξία (added value) του «εξομοιωτή πτήσης για την ασφαλή χρήση του Διαδικτύου» τόσο από εκπαιδευτικής άποψης όσο και σε σχέση με τις δυνατότητες που παρέχει στην αντιμετώπιση του συγκεκριμένου προβλήματος.

Το έργο προσβλέπει στην άντληση εμπειριών και κέρδους από όλους τους εμπλεκόμενους φορείς και συμμετέχοντες σε ατομικό και συλλογικό επίπεδο. Ακόμη πιο ουσιαστικό κέρδος προσδοκάται να αποκομίσουν τα ίδια τα παιδιά, τα οποία μέσα από μια ενδεδειγμένη εκπαιδευτική μεθοδολογία, εκείνη της εκπαίδευσης και της προσωπικής εξέλιξης μέσα από το παιχνίδι, θα κληθούν με ευχάριστο τρόπο να καλλιεργήσουν σημαντικές δεξιότητες, όπως είναι η κριτική και συνδυαστική σκέψη, η φαντασία, η αναζήτηση, ο προβληματισμός.

7. ΕΠΙΛΟΓΟΣ

7.1 Συμπεράσματα

Το Διαδίκτυο αναμφισβήτητα αποτελεί ένα σημαντικό και πολύτιμο εργαλείο στην εποχή μας. Σε πολλές περιπτώσεις η συμβολή του είναι αναγκαία και παίζει καθοριστικό ρόλο στην επίτευξη διαφόρων σκοπών. Τομείς όπως το εμπόριο, η εκπαίδευση, η ιατρική, η ενημέρωση και η ψυχαγωγία, επωφελούνται και κάνουν το έργο τους ευκολότερο και πιο ποιοτικό χρησιμοποιώντας τα προνόμια του Διαδικτύου.

Όπως κάθε εργαλείο όμως, η απερίσκεπτη και λανθασμένη χρήση του μπορεί να αποβεί μοιραία. Η πλοήγηση στο Διαδίκτυο και η επίδραση που ασκεί στον χρήστη, ο οποίος δεν είναι ενημερωμένος, κρύβει κινδύνους αλλά και παγίδες που μπορούν να οδηγήσουν σε προβληματικές καταστάσεις ή συμπεριφορές.

Πολλοί είναι οι επιτήδειοι που χρησιμοποιούν το Διαδίκτυο ως μέσο για να πετύχουν τους κακοπροαίρετους στόχους τους, όπως παραπλάνηση των χρηστών με απώτερο σκοπό την κερδοσκοπία, την κλοπή προσωπικών δεδομένων, την διάδοση κακόβουλου λογισμικού ενάντια στην «υγεία» του ηλεκτρονικού υπολογιστή, την δημιουργία και την διάδοση παραπληροφόρησης και προπαγάνδας.

Ιδιαίτερη προσοχή πρέπει να δοθεί για την σωστή και ασφαλή πλοήγηση των ανήλικων χρηστών, λαμβάνοντας υπόψη το ευαίσθητο της ηλικίας τους, την ελλιπή κριτική τους σκέψη και ικανότητα και την μεταβατική φάση της ζωής τους, στην οποία μπορεί να δημιουργηθούν λάθος πρότυπα. Η ελεύθερη φύση του Διαδικτύου μπορεί να αποβεί καταστροφική όταν η πλοήγηση σε αυτό είναι ανεξέλεγκτη και καταχρηστική. Μερικά από τα σοβαρότερα προβλήματα που αντιμετωπίζουν οι ανήλικοι χρήστες στο Διαδίκτυο είναι: ο εθισμός, η παιδική πορνογραφία, η αποπλάνηση / παρενόχληση τους και η διέρρευση των προσωπικών τους δεδομένων.

Οι έρευνες που έχουν πραγματοποιηθεί μαρτυρούν ότι στην πλειονότητα τους οι Έλληνες χρήστες δεν διαθέτουν τις απαραίτητες γνώσεις και τα επαρκή εφόδια για να προστατεύσουν τους εαυτούς τους αλλά και τα παιδιά από τις σκοτεινές πτυχές του Διαδικτύου. Η ευθύνη για την ασφαλή πλοήγηση στο Διαδίκτυο ανήκει στον καθένα. Τόσο στο οικογενειακό, εκπαιδευτικό και κοινωνικό περιβάλλον, όσο και στους παροχείς υπηρεσιών Διαδικτύου, Μέσα Μαζικής Ενημέρωσης και Internet café.

Σε επίπεδο λογισμικού κυκλοφορούν προγράμματα προστασίας και ασφάλειας του ηλεκτρονικού υπολογιστή. Επίσης διατίθενται φίλτρα προστασίας και γονικού ελέγχου, των οποίων η χρήση τους θα πρέπει να είναι συμπληρωματική και όχι πρωτίστης σημασίας, προσφέροντας επιπλέον ασφάλεια στην πλοήγηση των παιδιών. Ακόμα, για την ασφαλή πλοήγηση των παιδιών στο Διαδίκτυο συμβάλλουν όλο και περισσότερο τα λειτουργικά συστήματα.

Η ασφάλεια και η προστασία των πολιτών ενισχύεται με τις διάφορες ομάδες και υπηρεσίες που έχουν δημιουργηθεί, όπως γραμμές καταγγελιών (παράνομου περιεχομένου, ηλεκτρονικής παρενόχλησης, διαρροής προσωπικών δεδομένων, κ.λπ.), ομάδες δράσης επαγρύπνησης και ενημέρωσης σχετικά με το Διαδίκτυο, τους κινδύνους του και τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.), αρχές προστασίας και διασφάλισης προσωπικών και απόρρητων δεδομένων και τέλος, διαδικτυακές υπηρεσίες προς τους μαθητές.

Παρόλα αυτά, η ενοχοποίηση και δαιμονοποίηση του Διαδικτύου μπορεί να επισκιάσει και συνεπώς να στερήσει τα πάμπολλα πλεονεκτήματα που διαθέτει. Χαρακτηριστικά το Διαδίκτυο προσφέρει: ψυχαγωγία, διασκέδαση, ενημέρωση, αναζήτηση πληροφοριών, παροχή υπηρεσιών, κοινωνική επαφή και μηδενισμό αποστάσεων, εξάλειψη χρονικών περιορισμών και δημιουργία θέσεων εργασίας. Ιδιαίτερα σημαντικός είναι ο ρόλος του στην εκπαίδευση, καθώς έχει επιφέρει αλλαγές στον τρόπο διδασκαλίας και στην μετάδοση γνώσεων.

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας, το γενικότερο συμπέρασμα που απορρέει είναι ότι το Διαδίκτυο δεν είναι αθώο ή ένοχο. Ως τέτοιες μπορούν να χαρακτηριστούν μονάχα οι πράξεις των ανθρώπων.

7.2 Προτάσεις για μελλοντική έρευνα

Όπως διαπιστώθηκε από την αναζήτηση πληροφοριών που έλαβε χώρα κατά τη διάρκεια εκπόνησης της πτυχιακής εργασίας, η βιβλιογραφία για το σχετικό θέμα είναι περιορισμένη. Για τον λόγο αυτό, οι περισσότερες πηγές που χρησιμοποιήθηκαν, προήλθαν από το Διαδίκτυο.

Τα τελευταία χρόνια πραγματοποιούνται αρκετές μελέτες σχετικές με την ανάπτυξη και την χρήση του Διαδικτύου, όπως επίσης και με τις συνήθειες των Ελλήνων χρηστών. Παρόλα αυτά, οι έρευνες αυτές θα πρέπει να προωθηθούν και να γνωστοποιηθούν περισσότερο στο Ελληνικό κοινό, ενδυναμώνοντας την ενημέρωση του.

Ενδιαφέρον θα αποτελούσε η διεξαγωγή μιας πανελλήνιας μελέτης, η οποία θα εξέταζε τις θετικές επιδράσεις που έχει επιφέρει η χρήση του Διαδικτύου στους διάφορους τομείς της ζωής των χρηστών, αλλά και τις αρνητικές αντίστοιχα.

Τέλος, τα Μέσα Μαζική Ενημέρωσης, χρησιμοποιώντας την δύναμη της επίδρασης που ασκούν στους πολίτες και εκμεταλλευόμενα το μεγάλο εύρος των αποδεκτών, θα μπορούσαν να διεξάγουν καμπάνιες ενημέρωσης σχετικές με την ασφαλή πλοήγηση των ανήλικων χρηστών στο Διαδίκτυο, μιας και η προσπάθεια που έχει πραγματοποιηθεί ως τώρα δεν φαίνεται να είναι αρκετή.

7.3 Διαχείριση Πτυχιακής Εργασίας

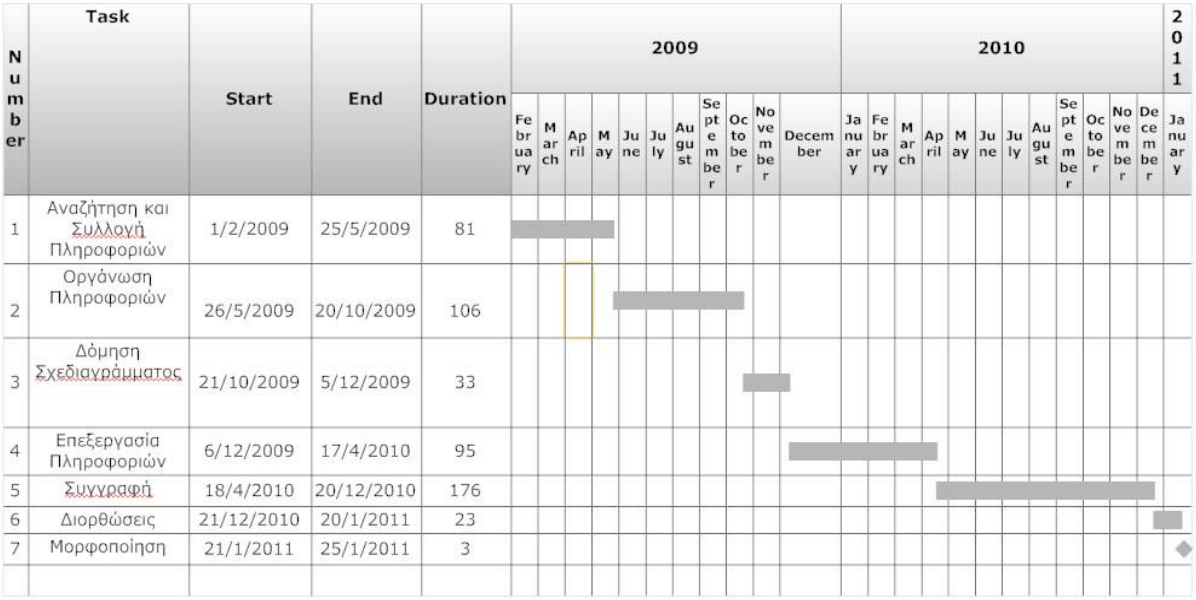
Αξίζει να σημειωθεί, ότι το στάδιο της αναζήτησης πληροφοριών συνεχίστηκε μέχρι την ολοκλήρωση της πτυχιακής εργασίας, διότι σε θέματα που αφορούν το Διαδίκτυο, οι μεταβολές είναι ταχύτατες, συνεχείς, προκύπτοντας νέα στοιχεία και δεδομένα. Το στάδιο της συγγραφής διήρκησε αρκετά μεγάλο διάστημα, λόγω στρατιωτικών υποχρεώσεων.

Στον ακόλουθο πίνακα φαίνονται οι τα διάφορα στάδια της εκπόνησης της παρούσας πτυχιακής εργασίας.

Πίνακας 7: Στάδια ανάπτυξης πτυχιακής εργασίας

Α/Α	**Διεργασία**	**Διάρκεια σε εβδομάδες**	**Έναρξη**
1	Αναζήτηση και Συλλογή Πληροφοριών	11	01/02/2009
2	Οργάνωση Πληροφοριών	15	26/05/2009
3	Δόμηση Σχεδιαγράμματος	5	21/10/2009
4	Επεξεργασία Πληροφοριών	13	06/12/2009
5	Συγγραφή	25	18/04/2010
6	Διορθώσεις	3	21/12/2010
7	Μορφοποίηση	1	21/01/2011

Στο ακόλουθο σχήμα παρουσιάζεται το διάγραμμα Gantt που απεικονίζει τις προγραμματισμένες διάρκειες.



Σχήμα 45 – Διάγραμμα Gantt

8. ΑΝΑΦΟΡΕΣ

8.1 Ελληνική Βιβλιογραφία

[1] **Κατερέλος Ι., Παπαδόπουλος Π.** (2009). *Οι έφηβοι και το Internet, ασφαλής και δημιουργική χρήση*. Ινστιτούτο Οπτικοακουστικών Μέσων. Αθήνα: Καστανιώτη.

[2] **Χρυσοστομίδου Β.** (11/05/2008). *Παιδιά στο ίντερνετ*. περιοδικό «Κ». τεύχος 258.

[3] **Καλμαντή Μ., Μαρκάκη Ε.Α.** (2010). *Ο εθισμός στο Διαδίκτυο*. περιοδικό «Γιατρεύω». τεύχος 15.

[4] **Τσιμιτάκης Μ.** (25/05/2008). *Χαμένοι στα παιχνίδια του Ίντερνετ*. εφημερίδα «Καθημερινή».

[5] *Παιδί και Internet*. (09/09/2007). ειδική έκδοση της εφημερίδας «Έθνος»

8.2 Διαδίκτυο

[1] Εργαστήρια Ελευθέρων Σπουδών Πληροφορικής. (09/02/2009). *10 Φεβρουαρίου 2009: Ημέρα Ασφαλούς Διαδικτύου*. Ανακτήθηκε 26/08/2010 από http://ediadiktio.blogspot.com/2009/02/10-2009.html

[2] **Αντωνίου Α., Πασπαράκη Μ.** *Ασφάλεια στο Διαδίκτυο*. Δικτυακή Εκπαιδευτική Πύλη του Υπουργείου Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων. Ανακτήθηκε 19/05/2010 από http://www.e-yliko.gr/htmls/pc_use/safety.aspx

[3] **Παπάνης Ε., Παπάνη Ε.Μ.** (26/03/2009). *Διαδίκτυο και γονείς*. Ανακτήθηκε 18/01/2010 από http://epapanis.blogspot.com/2009_03_01_archive.html

[4] Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας. (2005). *Πλάνο δράσης για την ανάπτυξη του Internet στην Ελλάδα*. Ανακτήθηκε 20/01/2010 από http://www.sepe.gr/files/news/SEPE_Meleti_Internet.pdf

[5] **Αντωνίου Θ., Μελίδου Θ., Νικόπουλος Χ.** (2009). *Το Internet στην Ελλάδα*. Ανακτήθηκε 30/9/2010 από http://www.politonsymaxia.gr/?p=511

[6] Παρατηρητήριο για την Κοινωνίας της Πληροφορίας. (2010). *Ταυτότητα χρηστών Internet στην Ελλάδα*. Ανακτήθηκε 14/12/2010 από http://www.observatory.gr/files/meletes/

[7] Ελληνική ιστοσελίδα της Microsoft. *Προστατεύστε την οικογένεια σας: Πέρα από τα βασικά*. Ανακτήθηκε 12/09/2010 από http://www.microsoft.com/hellas/protect/family/default.mspx

[8] Τμήμα Πληροφορικής Ιόνιο Πανεπιστήμιο. (2008). *Προστασία από Κακόβουλο Λογισμικό*. Ανακτήθηκε 02/10/2010 από http://di.ionio.gr/~emagos/Security/Simeioseis-asfaleia%20Part%20B.pdf

[9] Ελεύθερη ηλεκτρονική εγκυκλοπαίδεια Βικιπαίδεια. *Ιός (υπολογιστές)*. Ανακτήθηκε 25/11/2010 από http://el.wikipedia.org/wiki/Ιός_(υπολογιστές)

[10] Ομάδα Δράσης για την Ψηφιακή Ασφάλεια. *Γονείς και Διαδίκτυο*. Ανακτήθηκε 10/10/2009 από http://www.dart.gov.gr/NewsInner.aspx?

[11] Πανελλήνιο Σχολικό Δίκτυο. *Πρόσβαση στο διαδίκτυο από το σπίτι συμβουλές προς τους γονείς*. Ανακτήθηκε 11/12/2009 από http://www.sch.gr/2010-04-07-09-22-34/2010-04-07-10-31-40/Σελίδα-4#content

[12] Γραφείο Τηλεπικοινωνιών & Δικτύων Η/Υ, ΤΕΙ Κρήτης - Παράρτημα Χανιών. *Θέματα Ασφάλειας Προσωπικού Υπολογιστή & Δικτύων Η/Υ*. Ανακτήθηκε 16/06/2010 από http://noc.chania.teicrete.gr/docs/security.pdf

[13] Forthnet. *Dialers & Υψηλές Χρεώσεις*. Ανακτήθηκε 26/06/2010 από http://www.forthnet.gr/templates/viewcontentTmArt.aspx?p=102396

[14] Ο.Τ.Ε. *Προστατευθείτε από διογκωμένους λογαριασμούς*. Ανακτήθηκε 23/06/2010 από http://www.otenet.gr/hd/abuse/abuse_xrewseis.htm

[15] Hellas On Line (HOL). *Dialers*. Ανακτήθηκε 24/06/2010 από http://support.hol.gr/uploads/pdf/dialers_info.pdf

[16] Πανελλήνιο Σχολικό Δίκτυο. *Τι είναι το Spam*. Ανακτήθηκε 28/06/2010 από http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?

[17] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *Spam, ενημερωθείτε για την αζήτητη ηλεκτρονική επικοινωνία*. Ανακτήθηκε 02/07/2010 από http://www.dpa.gr/pls/portal/docs/.../ENTYPO_EKDILOSIS_LOW_1.PDF

[18]Forthnet. *Οδηγός αποφυγής ανεπιθύμητων e-mail (spam).* Ανακτήθηκε 29/06/2010 από http://www.forthnet.gr/templates/viewcontentTmCh.aspx?

[19] Ομάδα Δράσης για την Ψηφιακή Ασφάλεια. *Ηλεκτρονικό ταχυδρομείο: spam / phising*. Ανακτήθηκε 04/07/2010 από http://www.dart.gov.gr/

[20] Forthnet. *Τι είναι το Phishing και πώς λειτουργεί*. Ανακτήθηκε 06/07/2010 από http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043

[21] Κέντρο Πληροφορικής & Νέων Τεχνολογιών Ηλείας. *Ημέρα Για Ασφαλέστερο Διαδίκτυο*. Ανακτήθηκε 06/07/2010 από http://dide.ilei.sch.gr/keplinet/education/sid.php

[22] **Ντελέζος Κ.** (28/10/2010). *Στα 11 γνωρίζουν το ίντερνετ τα Ελληνόπουλα*. τα Νέα online. Ανακτήθηκε 25/11/2010 από http://www.tanea.gr/default.asp?pid=2&ct=1&artid=4601360

[23] madata.gr. (21/09/2010). *Το Internet κάνει τους νέους ανήθικους*. Ανακτήθηκε 29/11/2010 από http://www.madata.gr/diafora/science/76851.html

[24] **Αθανάσαινας Π.** (21/01/2008). *Εθισμός στο Διαδίκτυο, μια νέα μορφή εξάρτησης*. Ανακτήθηκε 03/02/2009 από http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_21_21/01/2008_219134

[25] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. *Υπερβολική ενασχόληση*. Ανακτήθηκε 05/03/2009 από http://www.saferinternet.gr/index.php?objId=Category35&parentobjId=Page2

[26] Ελεύθερη Ηλεκτρονική Εγκυκλοπαίδεια Βικιπαίδεια. *Εθισμός των νέων στο Διαδίκτυο*. Ανακτήθηκε 06/03/2009 από http://el.wikipedia.org/wiki/Εθισμός_των_νέων_στο_Διαδίκτυο

[27] internetandkids.com (07/05/2009). *Πείραμα για τον εθισμό στο Διαδίκτυο και τα ηλεκτρονικά μέσα στην Καλιφόρνια*. Ανακτήθηκε 01/10/2010 από http://www.internetandkids.com/2009/05/blog-post.html

[28] Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) Β΄ Παιδιατρική Κλινική Πανεπιστημίου Αθηνών Νοσοκομείο Παίδων "Παν. & Αγλ. Κυριακού". *Χρήση και κατάχρηση του Διαδικτύου (Internet): Συσχετίσεις με ψυχοκοινωνικούς παράγοντες που αφορούν τους χρήστες*. Ανακτήθηκε 15/03/2009 από http://www.youth-health.gr/gr/index.php?I=5&J=2&K=7

[29] Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια. *Τι είναι οι διαβαθμίσεις;*. Ανακτήθηκε 02/04/2009 από http://www.pegi.info/gr/index/id/212

[30] **Κρητικός Γ.** (07/02/2009). *Ηλεκτρονικές επιθέσεις σε παιδιά*. Ανακτήθηκε 20/05/2009 από http://www.ethnos.gr/article.asp?catid=11424&subid=2&pubid=2394807

[31] Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρώπινων Δικαιωμάτων. (08/01/2008). *Δημοσίευση νόμου για την καταπολέμηση της σεξουαλικής εκμετάλλευσης*. Ανακτήθηκε 13/05/2009 από http://www.ministryofjustice.gr/site/el/Ενημέρωση/Ανακοινώσεις/tabid/220/itemid/1018/amid/569/Default.aspx

[32] **Σιάφακας Β.** (24/08/2008). *Για την κοινωνική δικτύωση*. Ανακτήθηκε 19/07/2010 από http://archive.enet.gr/online/online_text/c=110,dt=24.08.2008,id=74017000

[33] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *Υπηρεσίες κοινωνικής δικτύωσης*. Ανακτήθηκε 29/06/2010 από http://www.dpa.gr/portal/page?_pageid=33,32920&_dad=portal&_schema=PORTAL

[34] Ενδελεχής blog. (28/01/2010). *Σελίδες κοινωνικής δικτύωσης και νέοι*. Ανακτήθηκε 29/06/2010 από http://endelexis.blogspot.com/2010/01/blog-post_28.html

[35] **Μπράτιτσης Θ., Καρασπύρου Ι., Κυρίδης Α**. *Ιστοχώροι κοινωνικής δικτύωσης: Απόψεις εφήβων για ζητήματα ασφάλειας και ενημέρωσης*. Ανακτήθηκε 29/09/2010 από http://www.etpe.gr/files/proceedings/26/1286267686_85.pdf

[36] ditiki.gr. (25/03/2010). *Διαδίκτυο και νέοι*. Ανακτήθηκε 29/06/2010 από http://www.ditiki.gr/index.php/Απόψεις/Διαδίκτυο-Νέοι.html

[37] **Δρακάκης Φ.** (19/08/2010). *Facebook places*. Ανακτήθηκε 30/09/2010 από http://www.deasy.gr/fresh-fish/1094,Facebook+places.html

[38] imerisia.gr (20/8/2010). *Διάτρητο το «Facebook Places;»*. Ανακτήθηκε 30/09/2010 από http://www.imerisia.gr/article.asp?catid=14049&subid=2&pubid=52281147

[39] **Δεληγιάννης Κ.** (29/08/2010). *Ουδέν κρυπτόν από το Facebook*. Ανακτήθηκε 30/09/2010 από http://news.kathimerini.gr/4dcgi/_w_articles_world_1_29/08/2010_413088

[40] Chatdanger.com. *Mobiles*. Ανακτήθηκε 11/11/2009 από http://www.chatdanger.com/mobiles/

[41] microsoft.com (22/09/2006). *Αποφύγετε τις ασύρματες επιθέσεις μέσω του κινητού σας τηλεφώνου Bluetooth*. Ανακτήθηκε 12/11/2009 από https://www.microsoft.com/hellas/protect/yourself/mobile/bluetooth.mspx

[42] Ελληνικός Κόμβος Επαγρύπνησης για ένα Ασφαλέστερο Διαδίκτυο. *Προτάσεις σχετικές με το θέμα «Ηλεκτρονικό παιχνίδι και Internet café» όπως κατατέθηκαν στην Ειδική Μόνιμη Επιτροπή Έρευνας και Τεχνολογίας της Βουλής των Ελλήνων, στις 19 Μαρτίου 2008*. Ανακτήθηκε 15/12/2009 από http://www.0-18.gr/downloads/saferinternet_gr_eisigisi_synigoros.pdf

[43] Ελληνικός Κόμβος Επαγρύπνησης για ένα Ασφαλέστερο Διαδίκτυο. (10/02/2009). *Αποτελέσματα Ευρωβαρόμετρου Safer Internet 2009 για την Ελλάδα*. Ανακτήθηκε 20/07/2010 από http://www.saferinternet.gr/index.php?childobjId=Text509&parentobjId=Category23&objId=Category119

[44] Ελληνική Ανοικτή Γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο-SafeLine.gr. *Ασφαλής χρήση του Διαδικτύου: Συμβουλές για γονείς*. Ανακτήθηκε 20/07/2010 από http://www.safeline.gr/Διαδίκτυο-και-γονείς

[45] Κέντρο Πληροφορικής & Νέων Τεχνολογιών Ηλείας. *Ασφάλεια στο Διαδίκτυο*. Ανακτήθηκε 20/07/2010 από http://dide.ilei.sch.gr/keplinet/articles/saferinternet.php

[46] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. (15/09/2009). *Προώθηση της ασφαλούς χρήση του Διαδικτύου στο σχολείο - η άποψη των εκπαιδευτικών*. Ανακτήθηκε 08/10/2010 από http://saferinternet.gr/index.php?action=download&objId=File342

[47] **Λύτρα Α.** (20/08/2010). *Ζητά 'ασπίδες' στα ίντερνετ καφέ*. Ανακτήθηκε 05/12/2010 από http://www.ethnos.gr/article.asp?catid=11424&subid=2&pubid=25694949

[48] microsoft.com. (14/12/2004). *Τα παιδιά και το Διαδίκτυο: Συνήθεις απορίες*. Ανακτήθηκε 08/10/2010 από http://www.microsoft.com/hellas/athome/security/children/kidsafetyfaq.mspx

[49] Δικτυακή Εκπαιδευτική Πύλη του Υπουργείου Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων. *Υπηρεσίες παρόχου σύνδεσης*. Ανακτήθηκε 13/10/2010 από http://www.e-yliko.gr/htmls/pc_use/snav2.aspx

[50] Ελεύθερη ηλεκτρονική εγκυκλοπαίδεια Wikipedia. *Antivirus software*. Ανακτήθηκε 03/08/2010 από http://en.wikipedia.org/wiki/Antivirus_software

[51] Ελεύθερη ηλεκτρονική εγκυκλοπαίδεια Wikipedia. *Firewall*. Ανακτήθηκε 05/08/2010 από http://el.wikipedia.org/wiki/Firewall

[52] PC Expert. *Firewall*. Ανακτήθηκε 05/08/2010 από http://pcex.gr/pc/index.php?option=com_content&task=view&id=30&Itemid=43

[53] ant1online.gr. (09/02/2010). *Ασφαλής χρήση του Διαδικτύου για τα παιδιά*. Ανακτήθηκε 17/06/2010 από http://www.ant1online.gr/Ereuna/Pages/20102/55cb7ef3-cfcf-4bb4-a0bb-057d3eeefc7e.aspx

[54] Σύγκριση φίλτρων γονικού έλεγχου. Ανακτήθηκε 22/09/2009 από http://internet-filter-review.toptenreviews.com/

[55] micosoft.com. (14/08/2007). *Windows Live OneCare Family Safety*. Ανακτήθηκε 23/10/2009 από http://www.microsoft.com/hellas/protect/products/family/onecarefamilysafety.mspx

[56] Ομάδα Δράσης για την Ψηφιακή Ασφάλεια. *Τί είναι το D.A.R.T.* Ανακτήθηκε 11/05/2009 από http://www.dart.gov.gr/NewsInner.aspx?new_id=173 &nwc_id=20

[57] **Γιαννοπούλου Α.** (2008). *Ομάδα Δράσης για την Ψηφιακή Ασφάλεια*. Ανακτήθηκε 11/05/2009 από http://www.okosmosgyromas.gr/node/131

[58] Κέντρο Πληροφορικής & Νέων Τεχνολογιών Ηλείας. *Εκπαιδευτικές Υπηρεσίες Πανελλήνιου Σχολικού Δικτύου (Π.Σ.Δ.)*. Ανακτήθηκε 26/11/2010 από http://dide.ilei.sch.gr/keplinet/articles/psd.php#web_filtering

[59] **Λυμπέρης Α.** (2005). *Καταγραφή και αποτίμηση της χρήσης του Πανελλήνιου Σχολικού Δικτύου.* Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών - Τομέας Δικτυακών Τεχνολογιών. Πάτρα. Ανακτήθηκε 27/11/2010 από http://www.sch.gr/sch-portlets/aboutSch/docs/AnaforaXrisis-PSD.pdf

[60] Πανελλήνιο Σχολικό Δίκτυο. *Τι είναι το Πανελλήνιο Σχολικό Δίκτυο;* Ανακτήθηκε 23/10/2009 από http://www.sch.gr/tieinaitoschmenu/2009-10-04-08-50-34

[61] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. Ποιοι είμαστε. Ανακτήθηκε 13/04/2009 από http://www.saferinternet.gr/index.php?parentobjId=Page74

[62] Υπηρεσία φιλτραρίσματος περιεχομένου cytanet - safe internet. (2008). *Πληροφορίες*. Ανακτήθηκε 21/04/2009 από http://www.cytanet.com.cy/Services/safe-internet/home/GR/

[63] Υπουργείο Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων. *Μνημόνιο Συνεργασίας*. Ανακτήθηκε 12/11/2010 από http://www.minedu.gov.gr/publications/docs/keimeno_mnhmonioy_100604.pdf

[64] Υπουργείο Παιδείας Δια Βίου Μάθησης και Θρησκευμάτων. (04/06/2010). *Μνημόνιο για την ασφαλή χρήση του Διαδικτύου από μαθητές*. Ανακτήθηκε 12/11/2010 από http://www.minedu.gov.gr/?option=com_content&view=article&id=705%253A04-06-10-...

[65] Ελληνική Ανοικτή Γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο-SafeLine. *Ποιοί Είμαστε - Σκοπός μας.* Ανακτήθηκε 15/07/2010 από http://www.safeline.gr/Σκοπός-μας

[66] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. (06/07/2010). *Στατιστικά στοιχεία γραμμής βοηθείας ΥποΣΤΗΡΙΖΩ Αύγουστος 2009 - Μάιος 2010.* Ανακτήθηκε 17/09/2010 από http://www.saferinternet.gr/index.php?parentobjId=Page75

[67] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. (13/07/2010). *Στατιστικά στοιχεία Ανοιχτής Γραμμής Καταγγελιών Safeline περιόδου 1-6/2010.* Ανακτήθηκε 20/09/2010 από http://www.saferinternet.gr/index.php?parentobjId=Page75

[68] Δράση Ενημέρωσης και Επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. *Γραμμή Βοήθειας Ελληνικού Κέντρου Ασφαλούς Διαδικτύου*. Ανακτήθηκε 20/09/2010 από http://www.saferinternet.gr/index.php?parentobjId=Page187

[69] tanea.gr (9/02/2010). *Αυξήθηκαν 149% οι καταγγελίες για «κατάχρηση» στο Internet.* Ανακτήθηκε 25/05/2010 από http://www.tanea.gr/default.asp?pid=96&ct=1&artid=4559795&nid=0&rid=%23

[70] Ομάδα Δράσης για την Ψηφιακή Ασφάλεια. *Δίωξη Ηλεκτρονικού Εγκλήματος.* Ανακτήθηκε 20/09/2010 από http://www.dart.gov.gr/NewsInner.aspx?new_id=130&nwc_id=22

[71] Γενική Γραμματεία Επικοινωνίας - Γενική Γραμματεία Ενημέρωσης. *Παιδιά και ΜΜΕ: Ασφαλής πρόσβαση στο Διαδίκτυο και προστασία των ανηλίκων*. Ανακτήθηκε 04/12/2010 από http://www.minpress.gr/minpress/index/currevents/draseis_paidia_mme_safe_internet.htm

ΓΛΩΣΣΑΡΙΟ

ADSL (Asymmetric Digital Subscriber Line): Ασύμμετρη Ψηφιακή Συνδρομητική Γραμμή. Τεχνολογία που παρέχει ασύμμετρο εύρος δεδομένων (bandwidth) μέσω ενός ζεύγους καλωδίων, που πρακτικά σημαίνει ότι το εισερχόμενο bandwidth (από το δίκτυο προς το χρήστη) είναι μεγαλύτερο από το εξερχόμενο (από το χρήστη προς το δίκτυο).

Antispam: Όρος που χαρακτηρίζει κάθε ενέργεια, πολιτική ή λογισμικό, κατά της μαζικής αποστολής ανεπιθύμητων μηνυμάτων (spam).

Antivirus: Αντι-ιικό. Λογισμικό που προστατεύει τον υπολογιστή από ιούς (viruses) και τους εξουδετερώνει σε περίπτωση μόλυνσης.

Browser: Φυλλομετρητής. Εφαρμογή λογισμικού η οποία χρησιμοποιείται για την πρόσβαση στις ιστοσελίδες του Διαδικτύου.

Chat: Ζωντανή επικοινωνία / συνομιλία μέσω του Διαδικτύου, με χρήση κειμένου, μικροφώνου ή κάμερας.

Default: Αρχικές ρυθμίσεις. Οι προεγκατεστημένες (εργοστασιακές) ρυθμίσεις ενός υπολογιστή ή μιας εφαρμογής λογισμικού, που συνήθως μπορούν να αλλάξουν από τον ίδιο το χρήστη.

Digital: Ψηφιακός - αυτός που αποτελείται από δυαδικό κώδικα.

Domain Name: Το όνομα με το οποίο αναγνωρίζεται ένας δικτυακός τόπος (web site). π.χ.«www.site.com».

Download: «Κατέβασμα» ή λήψη δεδομένων. Η διαδικασία με την οποία λαμβάνονται δεδομένα και αρχεία από τον υπολογιστή, μέσω του Διαδικτύου.

E-Banking: Οι τραπεζικές συναλλαγές μέσω του Διαδικτύου.

E-government: Ηλεκτρονική διακυβέρνηση. Γενικός όρος που αναφέρεται σε οποιεσδήποτε κυβερνητικές λειτουργίες ή διαδικασίες πραγματοποιούνται σε

ηλεκτρονική μορφή μέσω του Διαδικτύου (συναλλαγές με τους πολίτες, δημόσιες υπηρεσίες που παρέχουν online εξυπηρέτηση ή πληροφόρηση κ.λ.π.).

E-mail : Ηλεκτρονικό ταχυδρομείο / ηλεκτρονική αλληλογραφία. Πρόκειται για την ηλεκτρονική μεταβίβαση αλληλογραφίας μέσω υπολογιστών καθώς επίσης και αρχείων εικόνας και κειμένου.

E-Shop: Ηλεκτρονικό κατάστημα. Ένα κατάστημα πώλησης ειδών το οποίο λειτουργεί μέσω του Διαδικτύου, με ολοκληρωμένη διαδικασία πώλησης και πληρωμής.

Firewall: Τείχος προσασίας. Το σύνολο του τεχνικού εξοπλισμού (υλικού και λογισμικού) που χρησιμοποιείται για να την προστασία του υπολογιστή, ελέγχοντας κάθε εισερχόμενο ή εξερχόμενο δεδομένο, για λόγους ασφάλειας.

FTP (File Transfer Protocol): Πρωτόκολλο Μεταφοράς Δεδομένων. Το FTP είναι το πρωτόκολλο μεταφοράς αρχείων και αποτελεί ένα πρότυπο με το οποίο χρησιμοποιώντας ειδικά προγράμματα (FTP Clients) μπορεί ο χρήστης να κάνει download μέσω του Διαδικτύου αρχεία στον υπολογιστή του.

GUI (Graphical User Interface): Περιβάλλον διεπαφής χρήστη. GUI ονομάζεται το γραφικό περιβάλλον διεπαφής (interface) με το οποίο γίνεται εφικτή η επικοινωνία του χρήστη με μια εφαρμογή, μια ιστοσελίδα κ.λπ. Περιλαμβάνει δηλαδή τα στοιχεία πλοήγησης, τα κουμπιά, τα χρώματα και τη γενικότερη γραφική διάταξη, τα εικαστικά στοιχεία κ.λπ.

Hacker: Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση. Ένας hacker μπορεί να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες.

Hardware: Τεχνικός εξοπλισμός. Ο «ορατός» εξοπλισμός ενός συστήματος (δίσκοι, οδηγοί ανάγνωσης και εγγραφής, οθόνες, πληκτρολόγια, εκτυπωτές, μητρικές πλακέτες, επεξεργαστές κ.λπ.).

Hard disk / hard drive: Σκληρός δίσκος. Μαγνητικός δίσκος στον οποίο ο υπολογιστής αποθηκεύει και από τον οποίο αντλεί δεδομένα. Μπορεί να είναι εσωτερικός ή εξωτερικός.

HTML (Hyper Text Markup language): Γλώσσα προγραμματισμού για το περιβάλλον του παγκόσμιου ιστού, η οποία επιτρέπει την μορφοποίηση και «στήσιμο» των δεδομένων σε αρχεία html τα οποία διαβάζονται και εμφανίζονται από τους φυλλομετρητές (broswers).

HTTP (Hypertext Transfer Protocol): Πρωτόκολλο Μεταφοράς Υπερκειμένου. Το πρωτόκολλο που χρησιμοποιούν οι φυλλομετρητές (broswers) και οι servers για να επικοινωνούν μεταξύ τους.

HTTPS (Secure Hypertext Transfer Protocol): Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου. Ασφαλές πρωτόκολλομεταφοράς και αποθήκευσης ευαίσθητων προσωπικών δεδομένων. Οι δικτυακοί τόποι που υποστηρίζουν το συγκεκριμένο πρωτόκολλο, παρέχουν ασφαλή διαχείριση των προσωπικών δεδομένων των χρηστών και συνήθως αφορούν σε online συναλλαγές, αποστολή στοιχείων πιστωτικής κάρτας κ.λπ.

IP Address: Διεύθυνση IP. Διεύθυνση με τη μορφή ακολουθίας αριθμών που προσδίδεται σε κάθε υπολογιστή ή δίκτυο που είναι συνδεδεμένο στο Διαδίκτυο. Μία διεύθυνση IP έχει 4 μέρη με δεκαδικούς αριθμούς από το 0-255 για το κάθε μέρος. π.χ. 290.54.123.55. Ένας υπολογιστής μπορεί να αποκτά διαφορετική IP διεύθυνση κάθε φορά που συνδέεται ενώ, αντίστροφα, μία IP διεύθυνση μπορεί να αντιστοιχεί σε αρκετούς διαφορετικούς υπολογιστές, για παράδειγμα όταν χρησιμοποιείται τοπικός Web Server (proxy server).

IRC (Internet Relay Chat): Η ζωντανή αναμετάδοση μίας συνομιλίας στο Διαδίκτυο, που επιτρέπει την online επικοινωνία με άλλους συνομιλητές σε πραγματικό χρόνο. Εν συντομία έχει επικρατήσει ως Chat.

ISDN (Integrated Services Digital Network): Είδος τηλεφωνικής γραμμής που επιτρέπει μεγάλες ταχύτητες μετάδοσης δεδομένων κάθε μορφής, data, ήχο, video, κτλ. Η σύνδεση στο Διαδίκτυο μέσω μίας ISDN γραμμής επιτρέπει μετάδοση δεδομένων μέχρι και 128Kbps σε αντίθεση με τις συνδέσεις με απλές ψηφιακές γραμμές που επιτρέπουν συνδέσεις μέχρι 41Kbps.

ISP (Internet Service Provider): Πάροχος Υπηρεσιών Διαδικτύου. Φορέας που παρέχει υπηρεσίες πρόσβασης στο Διαδίκτυο. Συχνά ονομάζεται απλά Internet Provider ή Internet Access Provider.

Junk e-mail: Ανεπιθύμητη Αλληλογραφία. Έτσι χαρακτηρίζονται από τους χρήστες τα άχρηστα e-mail, π.χ. διαφημιστικού περιεχομένου.

LAN (Local Area Network): Τοπικό δίκτυο υπολογιστών που εκτείνεται στα όρια ενός κτιρίου ή περιοχής μικρών αποστάσεων.

Link: Ηλεκτρονικός σύνδεσμος. Οποιαδήποτε παραπομπή ή εφαρμογή μέσα σε μία ιστοσελίδα η οποία κατόπιν επιλογής (click) με το ποντίκι, μεταφέρει τον χρήστη σε κάποιο άλλο σημείο εσωτερικά ή εξωτερικά. Link μπορεί να είναι ένα κείμενο ή μία εικόνα.

Malware: Κακόβουλο λογισμικό. Σύνθεση των όρων malicious και software. Λογισμικό το οποίο σχεδιάζεται σκόπιμα προκειμένου να βλάψει ή να καταστρέψει εξ ολοκλήρου ένα σύστημα.

Modem: Είναι η συσκευή που συνδέει τον υπολογιστή στο Διαδίκτυο μέσα από μια απλή τηλεφωνική γραμμή, με σκοπό την μεταφορά δεδομένων. Το modem διαμορφώνει (modulate) και αναδιαμορφώνει (demodulate) το αναλογικό σήμα της τηλεφωνικής γραμμής ώστε να μεταδώσει ψηφιακές πληροφορίες.

Newsgroups: Ομάδες συζήτησης. Χώρος στον οποίο πραγματοποιούνται ανοιχτές ή κλειστές συζητήσεις.

Newsletter: Ενημερωτικό δελτίο που αποστέλλεται σε ηλεκτρονική μορφή από μια εταιρία ή οργανισμό σε τακτά χρονικά διαστήματα, συνήθως μέσω

ηλεκτρονικού ταχυδρομείου, σε όλους τους ενδιαφερόμενους (πελάτες, επισκέπτες μιας ιστοσελίδας, μέλη κ.λπ.) με σκοπό την πληροφόρησή τους για νέα προϊόντα / υπηρεσίες, προσφορές, εταιρικά νέα κ.λπ.

Offline: Εκτός σύνδεσης. Έλλειψη σύνδεσης υπολογιστή με άλλους υπολογιστές ή τράπεζες δεδομένων ή επαφής με το Διαδίκτυο.

Online: Σε σύνδεση. Άμεση ηλεκτρονική σύνδεση με άλλους υπολογιστές ή τράπεζες δεδομένων ή επαφής με το Διαδίκτυο.

P2P (peer-to-peer): Τεχνολογία που συνδέει απευθείας υπολογιστές χρηστών. Επιτρέπει την ανταλλαγή πληροφοριών, αρχείων κ.λπ. χωρίς τη διαμεσολάβηση server.

Password: Κωδικός πρόσβασης. Μοναδική και απόρρητη λέξη κλειδί με την οποία ο χρήστης, σε συνδυασμό με το username, αποδεικνύει την ταυτότητά του όταν εισέρχεται σε περιορισμένης πρόσβασης σελίδες ή εφαρμογές.

Phishing: Τεχνική που στοχεύει στην εκμαίευση προσωπικών δεδομένων στο Διαδίκτυο με σκοπό την απάτη (συνήθως οικονομική).

Pop-up Window (Ad): Αναδυόμενο παράθυρο. Μορφή διαφήμισης η οποία αναδύεται και φορτώνει σε ένα νέο μικρότερο παράθυρο μπροστά ή πίσω από τον φυλλομετρητή (browser) την ώρα που ο χρήστης μπαίνει σε μια ιστοσελίδα. Μέσα στο pop window μπορεί να υπάρχει μία απλή εικόνα ή μία ολόκληρη σελίδα με κάθε μορφής πληροφορία και τεχνολογία συνήθως για διαφημιστικούς λόγους.

Privacy Policy: Πολιτική Προστασίας Απορρήτου Προσωπικών Στοιχείων. Δήλωση Εμπιστευτικότητας. Η πολιτική μιας επιχείρησης που διαθέτει ιστοσελίδα ως προς τη συλλογή και χρήση των προσωπικών δεδομένων των επισκεπτών / πελατών της.

Proxy Server: Ένας server στον οποίο πραγματοποιείται ενδιάμεση αποθήκευση πληροφοριών του Διαδικτύου με σκοπό την εύκολη ανάκλησή τους.

Software: Με τον όρο λογισμικό υπολογιστών, ή λογισμικό (software) ορίζεται η συλλογή από προγράμματα υπολογιστών, διαδικασίες και οδηγίες χρήσης που εκτελούν ορισμένες εργασίες σε ένα υπολογιστικό σύστημα.

Spam: Μη ζητηθείσα ηλεκτρονική αλληλογραφία για την απευθείας εμπορική ή άλλη προώθηση προϊόντων ή υπηρεσιών.

Spyware: Λογισμικό παρακολούθησης ενός υπολογιστικού συστήματος. Το spyware αποτελεί λογισμικό που συγκεντρώνει πληροφορίες, παρακολουθεί τις κινήσεις του χρήστη στο Διαδίκτυο και αποστέλλει τις πληροφορίες σε τρίτους.

TCP/IP (Transmission Control Protocol / Internet Protocol): Πρωτόκολλο Ελέγχου Μετάδοσης / Πρωτόκολλο Διαδικτύου). Το πρωτόκολλο με το οποίο οι υπολογιστές επικοινωνούν μεταξύ τους στο Διαδίκτυο.

Trojan (horse): Δούρειος Ίππος. Πρόγραμμα που ενώ εμφανίζεται απόλυτα ακίνδυνο για το χρήστη, έχει έμμεσες ή άμεσες καταστρεπτικές συνέπειες για τον υπολογιστή, επιτρέποντας σε έναν ή περισσότερους hackers να έχουν πρόσβαση σε αυτόν.

Update: Νεότερη έκδοση ενός προγράμματος υπολογιστή που περιλαμβάνει νέες ή βελτιωμένες λειτουργίες.

Upload: «Ανέβασμα». Είναι η αποστολή αρχείων σε έναν υπολογιστή από έναν άλλο. Είναι το αντίθετο του download.

URL (Uniform Resource Locator): Παγκόσμιος Εντοπιστής Πόρων. Η διεύθυνση που συνολικά καθορίζει ένα Web Site. Όπως σε μια ατζέντα διευθύνσεων προσδιορίζεται ακριβώς η θέση του κωδικού πόλης και του αριθμού, έτσι και στο URL ορίζεται η ακριβής δομή των στοιχείων μιας διεύθυνσης.

Username: Το όνομα χρήστη, που χρησιμοποιείται (συνήθως σε συνδυασμό με έναν κωδικό πρόσβασης (password) για την εισαγωγή σε μια υπηρεσία, εφαρμογή ή σύστημα.

Virus: Επιβλαβής ιός (πρόγραμμα) το οποίο κατόπιν ενέργειας του χρήστη ή εν αγνοία του, εισβάλλει στον σύστημα και μολύνει τον υπολογιστή με σκοπό να του δημιουργήσει ζημιά.

Web Page: Ιστοσελίδα. Μεμονωμένη σελίδα προγραμματισμένη στην γλώσσα HTML η οποία είναι μέρος ενός συνολικού Web Site. Μία Web Page πρέπει να περιέχει κείμενα με links και μπορεί να περιέχει επίσης εικόνες, animation αλλά και ήχο, video κ.λπ.

Web Server: Διακομιστής ιστοσελίδων. Υπολογιστής συνδεμένος με το Διαδίκτυο ο οποίος με τη χρήση κατάλληλου λογισμικού επιτρέπει σε άλλες ηλεκτρονικές συσκευές (Η/Υ, Palmtops, Mobile Phones) να έχουν πρόσβαση στις πληροφορίες ή υπηρεσίες που αυτός παρέχει και με αυτή την έννοια να εξυπηρετεί αυτές τις συσκευές.

Web Site: Δικτυακός τόπος. Χαρακτηρισμός της παρουσίας στο World Wide Web. Ένας δικτυακός τόπος ή ιστοσελίδα όπως πολλοί το αναφέρουν στα ελληνικά. Ένα Web Site περιλαμβάνει εκτός από την αρχική σελίδα, πρόσθετες σελίδες Web, καθώς και άλλα στοιχεία όπως εικόνες, video, ήχο και πρέπει να χαρακτηρίζεται από μία διεύθυνση (URL ή Domain Name) π.χ. www.site.gr

Worm: Σκουλήκι. Πρόγραμμα ή αλγόριθμος που αυτο-πολλαπλασιάζεται και συνήθως προκαλεί βλάβες σε ένα σύστημα ή το τερματίζει. Σε αντίθεση με τους «παραδοσιακούς» ιούς, τα worms δεν απαιτούν την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν από το ένα σύστημα στο άλλο.

WWW (World Wide Web): Παγκόσμιος Ιστός. Χαρακτηρισμός του γραφικού περιβάλλοντος που πλέον διέπει το Διαδίκτυο. Χάρη στις δυνατότητες

πολυμέσων που προσφέρει, συνέβαλε σημαντικά στην ραγδαία εξάπλωση του Διαδικτύου.