ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κίνδυνοι και ασφάλεια στο Διαδίκτυο για τη νεολαία: Μία κριτική επισκόπηση

Αθανάσιος Α. Καμάρης

Επιβλέποντες: **Αφροδίτη Τσαλγατίδου,** Αναπληρωτής Καθηγητής
Βασίλειος Δαγδιλέλης, Καθηγητής Τμήματος Εκπαιδευτικής & Κοινωνικής Πολιτικής Πανεπιστημίου Μακεδονίας

ΑΘΗΝΑ

ΦΕΒΡΟΥΑΡΙΟΣ 2015

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κίνδυνοι και ασφάλεια στο Διαδίκτυο για τη νεολαία: Μία κριτική επισκόπηση

Αθανάσιος Α. Καμάρης

Α.Μ.: 1115200500023

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Αφροδίτη Τσαλγατίδου,** Αναπληρωτής Καθηγητής
Βασίλειος Δαγδιλέλης, Καθηγητής Τμήματος Εκπαιδευτικής & Κοινωνικής Πολιτικής Πανεπιστημίου Μακεδονίας

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποσκοπεί στη διερεύνηση των κινδύνων και της ασφάλειας στο Διαδίκτυο για τη νεολαία, κλείνοντας συμπερασματικά τόσο με μια κριτική επισκόπηση των ευρημάτων υπό το πρίσμα της υποκειμενικής άποψης του συγγραφέα, όσο και με κάποιες προτάσεις του για την καλύτερη και αποτελεσματικότερη αντιμετώπιση των κινδύνων.

Τα κύρια βήματα που ακολουθήθηκαν για την εκπόνηση της παρούσας εργασίας περιλαμβάνουν την προσέγγιση των εννοιών του Κινδύνου και της Ασφάλειας στο Διαδίκτυο μέσω της καταγραφής, περιγραφής και ανάλυσης διαφόρων κατηγοριών κινδύνων του Διαδικτύου, καθώς και την καταγραφή ερευνών και στατιστικών στοιχείων. Από την ανάλυση αυτή, αφενός μεν διαφαίνεται ο βαθμός επικινδυνότητας των κινδύνων, αφετέρου δε εξάγονται πολλά χρήσιμα συμπεράσματα για αυτούς. Ακολούθως, αναφέρονται και αναπτύσσονται οι βασικές μέθοδοι αντιμετώπισης των κινδύνων του Διαδικτύου καθώς και οι διαθέσιμοι πόροι αντιμετώπισης αυτών, ενώ παρουσιάζονται τρόποι ασφαλούς χρήσης του Διαδικτύου για γονείς, εκπαιδευτικούς και μαθητές αναφορικά με τους κινδύνους που αποτυπώθηκαν στην εργασία.

Εν κατακλείδι, συμπεραίνεται πως παρά τα αδιαμφισβήτητα οφέλη του Διαδικτύου σε ποικίλους τομείς όπως η εκπαίδευση, η μόρφωση, η υγεία, η έρευνα, η ψυχαγωγία, η επικοινωνία στις κοινωνίες των πολιτών, η ανταλλαγή πληροφοριών και απόψεων, κ.ά., που το καθιστούν το σπουδαιότερο μέσο νέων τεχνολογιών της σύγχρονης εποχής, υπάρχουν αρκετοί και ποικιλόμορφοι κίνδυνοι από τους οποίους οι χρήστες και ιδιαίτερα οι νέοι, τόσο σε ηλικία όσο και σε εμπειρία, απειλούνται. Με σκοπό λοιπόν, την πρόληψη και την προστασία των χρηστών από τους κινδύνους αυτούς, ώστε να απολαμβάνουν με ασφάλεια τα οφέλη του Διαδικτύου, έχει αναπτυχθεί ήδη πλήθος μεθόδων και πόρων αντιμετώπισής τους που δίνουν ιδιαίτερη έμφαση στη διαπαιδαγώγηση των χρηστών. Βέβαια, σε κάθε περίπτωση υπάρχουν πολλά περιθώρια βελτίωσης της ασφάλειας κατά τη χρήση του Διαδικτύου, γεγονός το οποίο μεταφράζεται πως θα πρέπει να υπάρξει περαιτέρω ευαισθητοποίηση και συλλογική προσπάθεια όλων μας (σε επίπεδο πολιτείας, κοινωνίας, ατόμου, κ.λπ.).

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Διαδίκτυο

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διαδίκτυο, κίνδυνος, ασφάλεια, προστασία, νεολαία

ABSTRACT

The current study aims on investigating and analyzing the matters of Internet safety and the dangers underlying its use with regard to the youth, concluding with a critical review on the findings in the light of the subjective view of the author, as well as with some proposals for dealing with those pitfalls in a more efficient and optimal manner.

The main steps that were followed in the implementation of the current study involve approaching the concepts of Danger of and Safety on the Internet, through the listing, description and analysis of the categories of dangers inherent of the Internet, as well as gathering relevant studies and statistical data. From this analysis, on the one hand the level of underlying dangers is revealed while on the other hand many useful conclusions can be drawn about them. Subsequently, the basic methods of dealing with the dangers of the Internet as well as the available resources to this end are reported and detailed, while also presented are ways of safely using the Internet for parents, educators and students alike with regard to the dangers that were listed and detailed in this study.

In conclusion, it is deduced that in spite of the indisputable benefits of the Internet in various areas of activities, like schooling and education, learning, health, research, recreation, communication between people, the exchange of information and views, etc., which renders it the most important medium of new technologies of the modern era, there are several and various dangers from which users are threatened and especially those lacking in age or experience. Therefore, with the aims of prevention and the protection of users from the aforementioned dangers, so they can safely enjoy the benefits of the Internet, the necessary resources have been allocated and a number of methods have already been developed, with an emphasis on educating the users. Of course, in every case there is a lot of space for improvement regarding the safety on using the Internet, a fact that translates to the need of raising the level of awareness regarding those issues and that there should be a concentrated effort by everyone (on a personal level as well as on the levels of the state, society, etc.).

SUBJECT AREA: Internet

KEYWORDS: Internet, danger, safety, protection, youth

Στη σύζυγό μου
για την αμέριστη συμπαράσταση και συμβολή της
στην ολοκλήρωση των σπουδών μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας Πτυχιακής Εργασίας, θα ήθελα να ευχαριστήσω τους επιβλέποντες, αναπληρώτρια καθηγήτρια Αφροδίτη Τσαλγατίδου και καθηγητή Βασίλειο Δαγδιλέλη, καθώς και την ομότιμο καθηγήτρια Μαρία Γρηγοριάδου, για τη συνεργασία και την πολύτιμη συμβολή τους στην εκπόνηση και ολοκλήρωσή της.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ 13

1.1 Το Διαδίκτυο και η χρήση του 13

1.2 Δομή της εργασίας 14

2. ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ 16

2.1 Ορισμός του Κινδύνου και της Ασφάλειας στο Διαδίκτυο 16

2.2 Κατηγορίες - Είδη κινδύνων στο Διαδίκτυο 17

2.2.1 Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content) 18

2.2.2 Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages) 18

2.2.3 Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation) 19

2.2.4 Ηλεκτρονική αποπλάνηση χρηστών (Online grooming) 20

2.2.5 Βίαια παιχνίδια (Violent games) 20

2.2.6 Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction) 21

2.2.7 Διαδικτυακός εκφοβισμός (Cyber bullying) 23

2.2.8 Παρώθηση σε επιβλαβείς συμπεριφορές 24

2.2.9 Ηλεκτρονικός τζόγος (Online gambling) 25

2.2.10 Κακόβουλο λογισμικό που μολύνει Ηλεκτρονικούς Υπολογιστές (Η/Υ) (Malware) 26

2.2.11 Παιδική πορνογραφία (Child pornography) 26

2.2.12 Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy) 28

2.2.13 Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation) 28

2.2.14 Υποκλοπή προσωπικών δεδομένων των χρηστών 29

2.2.14.1 «Phishing» 29

2.2.14.2 «Pharming» 30

2.2.15 Φυσικές Παθήσεις που προκαλούνται από παρατεταμένη χρήση του Η/Υ 30

2.3 Οι κίνδυνοι του Διαδικτύου με αριθμούς 31

3. ΜΕΘΟΔΟΙ ΚΑΙ ΠΟΡΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ .33

3.1 Μέθοδοι Αντιμετώπισης των Κινδύνων του Διαδικτύου 33

3.1.1 Τεχνικές Μέθοδοι Αντιμετώπισης 33

3.1.1.1 Φίλτρα 33

3.1.1.1.1 Περιφραγμένες τοποθεσίες (Walled gardens) – Λευκές λίστες (White lists) 34

3.1.1.1.2 Μαύρες λίστες (Black lists) 34

3.1.1.1.3 Ουδέτερες ζώνες (Demilitarized zones – DMZs) 34

3.1.1.1.4 Διαχωρισμός ανεπιθύμητης – ομαδικής αλληλογραφίας (Spam – Bulk mail filtering) 34

3.1.1.1.5 Αξιολόγηση - Βαθμολόγηση ιστοσελίδων (Website rating) ... 35
3.1.1.1.6 Αυτοαξιολόγηση ιστοσελίδων ... 35
3.1.1.1.7 Συνδυασμός μεθόδων φιλτραρίσματος ... 35
3.1.1.2 Γονικός Έλεγχος (Parental control) ... 35
3.1.1.3 Προγράμματα προστασίας και καταπολέμησης κακόβουλου λογισμικού (Antivirus – Antimalware) ... 36
3.1.1.4 Τείχος Προστασίας «Firewall» ... 36
3.1.1.5 PEGI (Pan-European Game Information) ... 37
3.1.1.5.1 PEGI: Κατάταξη του παιχνιδιού σε ηλικιακές ομάδες ... 38
3.1.1.5.2 PEGI: Χαρακτηρισμός του περιεχομένου ... 38
3.1.1.5.3 Η ένδειξη «PEGI OK» ... 39
3.1.1.5.4 PEGI Online ... 40
3.1.2 Μέθοδοι Αντιμετώπισης Παιδαγωγικού Χαρακτήρα ... 40
3.1.2.1 Τηλεδιασκέψεις – Διαδικτυακά σεμινάρια (Webinars) ... 41
3.1.2.2 Συνέδρια – Σεμινάρια – Ημερίδες ... 41
3.1.2.3 Τηλεοπτικές εκπομπές – Ντοκιμαντέρ – Τηλεοπτικά σποτ ... 42
3.1.2.4 Κοινωνικό Σχολείο ... 43

3.2 Πόροι Αντιμετώπισης των Κινδύνων του Διαδικτύου ... 43
3.2.1 Δικτυακοί Πόροι Αντιμετώπισης ... 44
3.2.1.1 Ελληνικό Κέντρο Ασφαλούς Διαδικτύου ... 44
3.2.1.1.1 Δράση Ενημέρωσης «Saferinternet.gr» ... 44
3.2.1.1.2 Γραμμή Καταγγελιών «SafeLine» ... 45
3.2.1.1.3 Γραμμή Βοηθείας «ΥποΣΤΗΡΙΖΩ» ... 45
3.2.1.2 Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου «sch.gr» ... 46
3.2.2 Μη-Δικτυακοί Πόροι Αντιμετώπισης ... 46
3.2.2.1 Ελληνική Εταιρία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο ... 46
3.2.2.2 Μονάδα Εφηβικής Υγείας του Πανεπιστημιακού Νοσοκομείου Παίδων «Π. & Α. Κυριακού» ... 47
3.2.2.3 Ελληνική Αστυνομία: Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ... 47

4. ΟΔΗΓΙΕΣ ΑΣΦΑΛΟΥΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ... 50

4.1 Ασφαλής χρήση του Διαδικτύου από Νεαρά Άτομα: Οδηγίες για Γονείς και Κηδεμόνες ... 50

4.2 Ασφαλής χρήση του Διαδικτύου: Οδηγίες για Νεαρά Άτομα ... 52

4.3 Ασφαλής χρήση του Διαδικτύου από Νεαρά Άτομα: Οδηγίες για Εκπαιδευτικούς ... 55

5. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΠΡΟΤΑΣΕΙΣ ... 57

5.1 Συμπερασματική απόδοση της έρευνας σύμφωνα με την κριτική άποψη του συγγραφέα ... 57

5.2 Προτάσεις βελτιστοποίησης του υφιστάμενου πλαισίου για την αντιμετώπιση των κινδύνων του Διαδικτύου..... 59

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ 61

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ 64

ΑΝΑΦΟΡΕΣ 65

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1: Οι χρήστες του Διαδικτύου ως ποσοστό του πληθυσμού κάθε χώρας (2012) 13

Σχήμα 2: Σταθερές ευρυζωνικές συνδέσεις Διαδικτύου ως ποσοστό του πληθυσμού κάθε χώρας (2012) 14

Σχήμα 3: Στατιστικά στοιχεία ηλεκτρονικού τζόγου (Ελλάδα 2010-2011) 25

Σχήμα 4: Στατιστικά στοιχεία καταγγελιών στη SafeLine.gr ανά έτος (2003-2010) 31

Σχήμα 5: Στατιστικά στοιχεία καταγγελιών στη SafeLine.gr ανά κατηγορία (2013) 31

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Σήμανση ακατάλληλου – προσβλητικού περιεχομένου....18

Εικόνα 2: Διακωμωδώντας την πραγματικότητα των Ανεπιθύμητων μηνυμάτων....19

Εικόνα 3: Μία παραστατική προσέγγιση του Διαδικτυακού εθισμού....22

Εικόνα 4: Διαδικτυακή εξάρτηση – μία εικόνα χίλιες λέξεις....23

Εικόνα 5: Απεικονίζοντας τον Διαδικτυακό εκφοβισμό ως αναπόσπαστο κομμάτι της Διαδικτυακής ζωής του θύτη....24

Εικόνα 6: Αναπαριστώντας την έννοια «Phishing»....29

Εικόνα 7: Λογότυπα δημοφιλέστερων προγραμμάτων «Antivirus» με άδεια ελεύθερης χρήσης....36

Εικόνα 8: Αναπαράσταση της έννοιας του Τείχους προστασίας «firewall»....37

Εικόνα 9: Ετικέτες κατάταξης σε ηλικιακές ομάδες «PEGI»....38

Εικόνα 10: Ετικέτες χαρακτηρισμού περιεχομένου «PEGI»....38

Εικόνα 11: Η ένδειξη «PEGI OK»....39

Εικόνα 12: Τα λογότυπα «PEGI Online»....40

Εικόνα 13: Λογότυπο Μονάδας Εφηβικής Υγείας «ΥποΣΤΗΡΙΖΩ»....45

Εικόνα 14: Ενημερωτικός Κόμβος «sch.gr» – υπηρεσία «Ασφάλεια στο Διαδίκτυο»....46

Εικόνα 15: Λογότυπο Ελληνικής Εταιρείας Μελέτης Διαταραχής Εθισμού Διαδίκτυο....46

Εικόνα 16: Δίωξη Ηλεκτρονικού Εγκλήματος – πρωτοβουλία «Cyberkids»....48

Εικόνα 17: Αφίσα «Keep your kids SAFE on the Internet»....51

Εικόνα 18: Τι σημαίνει να είμαι Ασφαλής;....52

Εικόνα 19: Αφίσα «Συνταγή για Ασφαλή πλοήγηση στο Internet»....54

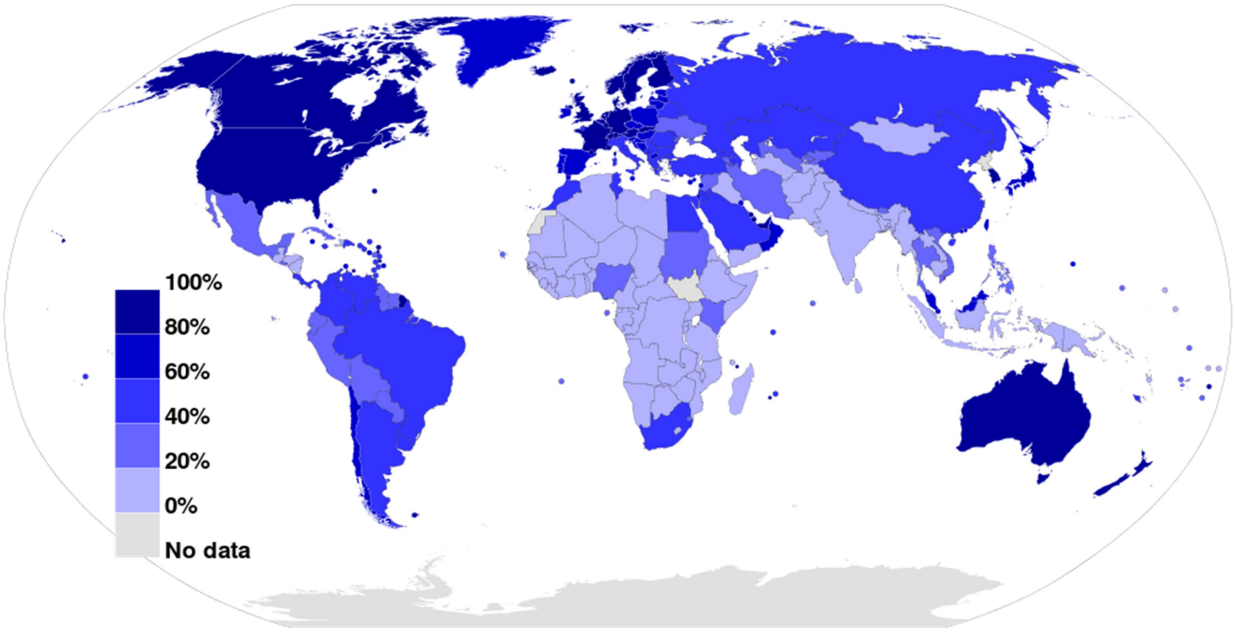
ΠΡΟΛΟΓΟΣ

Η παρούσα βιβλιογραφική και δικτυογραφική έρευνα εκπονήθηκε στα πλαίσια υλοποίησης πτυχιακής εργασίας, απαραίτητης για την ολοκλήρωση των Προπτυχιακών μου Σπουδών στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών της Σχολής Θετικών Επιστημών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

1. ΕΙΣΑΓΩΓΗ

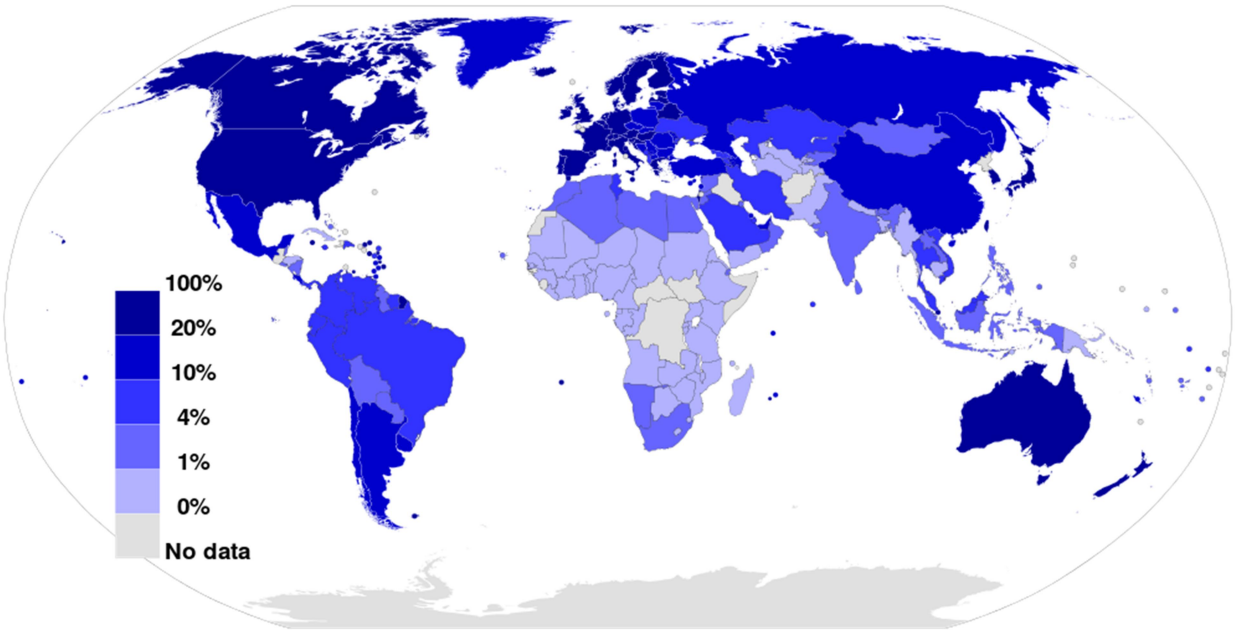
1.1 Το Διαδίκτυο και η χρήση του

Το Διαδίκτυο (Internet), δηλαδή το παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών που ανταλλάσσουν μηνύματα χρησιμοποιώντας τυποποιημένους κανόνες επικοινωνίας (πρωτόκολλα) [1], έκανε για πρώτη φορά την εμφάνιση του σε πρώιμη μορφή το έτος 1969 (το επονομαζόμενο ARPAnet) [2] [3] για να καλύψει τις ανάγκες άμεσης επικοινωνίας μέσω δικτύωσης (networking) ανάμεσα στο Πανεπιστήμιο της Καλιφόρνια (University of California, Los Angeles – UCLA) και το Ινστιτούτο Ερευνών του Στάνφορντ (Stanford Research Institute – SRI) υπό την εποπτεία του Υπουργείου Άμυνας των Η.Π.Α. [4]. Έξι χρόνια αργότερα η διάδοση του Διαδικτύου διευρύνεται και είναι πλέον εμπορικά διαθέσιμο, ενώ το 1991 ο Παγκόσμιος Ιστός (World Wide Web – WWW) διατίθεται στο ευρύ κοινό [5]. Η διάδοση της χρήσης του Διαδικτύου ολοένα και αυξάνεται καλύπτοντας τα μήκη και τα πλάτη του πλανήτη. Το 2003 οι Ευρυζωνικές Συνδέσεις (Broadband Connections) κάνουν την εμφάνιση τους στην Ελλάδα [6] σημαίνοντας την απαρχή της ευρείας χρήσης του Διαδικτύου στη Χώρα μας. Πράγματι, σύμφωνα με έρευνα που διεξήχθη για τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union – ITU) το ποσοστό χρήσης του Διαδικτύου στην Ελλάδα το 2013 ανήλθε στο 59,87% έναντι του 17,8% το 2003 [7].



Σχήμα 1: Οι χρήστες του Διαδικτύου ως ποσοστό του πληθυσμού κάθε χώρας (2012)

Το Διαδίκτυο εδραιώνεται σταδιακά σε απαραίτητο μέσον-εργαλείο της επαγγελματικής, οικονομικής και κοινωνικής ζωής και δεν αργεί να προσελκύσει το ενδιαφέρον των νεαρών ατόμων. Έρευνα που διεξήχθη από το ΚΕ.ΠΛΗ.ΝΕ.Τ. Κυκλάδων [8] τον Ιανουάριο του 2009 σε 627 μαθητές τριών Γυμνασίων και ενός Λυκείου της Σύρου έδειξε πως το 43,16% των μαθητών Γυμνασίου και το 50% των μαθητών Λυκείου χρησιμοποιούν καθημερινά το Διαδίκτυο, ενώ το 29,62% των μαθητών Γυμνασίου και το 19,29% των μαθητών Λυκείου το χρησιμοποιεί τρείς έως πέντε φορές την εβδομάδα. Η συντριπτική πλειοψηφία κάνει χρήση του Διαδικτύου στο σπίτι, κυρίως για την εκπόνηση σχολικών εργασιών, τη συμμετοχή σε σελίδες κοινωνικής δικτύωσης (social networking) και τη ψυχαγωγία.



Σχήμα 2: Σταθερές ευρυζωνικές συνδέσεις Διαδικτύου ως ποσοστό του πληθυσμού κάθε χώρας (2012)

Παρά τα αδιαμφισβήτητα οφέλη του, ιδιαίτερη σημασία κρίνεται σκόπιμο να δοθεί στους κινδύνους που μπορεί κανείς να αντιμετωπίσει στο Διαδίκτυο, κυρίως για τους νέους που βρίσκονται περισσότερο εκτεθειμένοι και απροστάτευτοι, καθώς το γνωστικό και γενικότερα μορφωτικό τους «προφίλ» δεν επαρκεί για την κατανόηση των κινδύνων αυτών και τη λήψη κατάλληλων προστατευτικών μέτρων. Η ίδια έρευνα αναδεικνύει τη σπουδαιότητα του προβλήματος. Αναλυτικότερα, το 59,65% των μαθητών Λυκείου έχει προσεγγιστεί Διαδικτυακά από άγνωστο άτομο με σκοπό την ανάπτυξη ηλεκτρονικής επαφής και το 61,4% έχει δεχτεί ενοχλητικά μηνύματα. Τα αντίστοιχα ποσοστά σε μαθητές Γυμνασίου είναι αισθητά χαμηλότερα, ικανά εντούτοις να αποτυπώσουν τον κίνδυνο που διατρέχουν και αυτοί οι μαθητές.

1.2 Δομή της εργασίας

Η παρούσα εργασία αποσκοπεί στη βιβλιογραφική και δικτυογραφική προσέγγιση των κινδύνων και της ασφάλειας στο Διαδίκτυο για τη νεολαία, κλείνοντας με μια κριτική επισκόπηση των ευρημάτων.

Η εργασία αναπτύσσεται σε πέντε συνολικά κεφάλαια.

Το πρώτο κεφάλαιο είναι το παρόν.

Στο δεύτερο κεφάλαιο προσεγγίζονται οι έννοιες του «Κινδύνου» και της «Ασφάλειας στο Διαδίκτυο» μέσω της καταγραφής και περιγραφής διαφόρων κατηγοριών κινδύνων του Διαδικτύου. Επίσης, καταγράφονται έρευνες και στατιστικά στοιχεία, διαμέσου των οποίων αφενός μεν διαφαίνεται ο βαθμός επικινδυνότητας των κινδύνων, αφετέρου δε εξάγονται πολλά χρήσιμα συμπεράσματα για αυτούς.

Στο τρίτο κεφάλαιο αναφέρονται και αναπτύσσονται οι βασικές μέθοδοι αντιμετώπισης των κινδύνων του Διαδικτύου καθώς και οι διαθέσιμοι πόροι αντιμετώπισης αυτών.

Το τέταρτο κεφάλαιο παρουσιάζει τρόπους ασφαλούς χρήσης του Διαδικτύου για γονείς, εκπαιδευτικούς και μαθητές αναφορικά με τους κινδύνους που ήδη αναπτύχθηκαν.

Τέλος, στο πέμπτο κεφάλαιο διατυπώνονται κάποια συμπεράσματα που προκύπτουν από τα στοιχεία που καταγράφηκαν στην εργασία υπό το πρίσμα της υποκειμενικής άποψης του συγγραφέα και αναφέρονται κάποιες προτάσεις του για την αποτελεσματικότερη αντιμετώπιση των κινδύνων.

2. ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 Ορισμός του Κινδύνου και της Ασφάλειας στο Διαδίκτυο

Το Διαδίκτυο αποτελεί ένα απαραίτητο εργαλείο στη ζωή κάθε σύγχρονου ανθρώπου προκειμένου ολοκληρώσει ευκολότερα και γρηγορότερα τις δραστηριότητες που καλείται να διεκπεραιώσει στα πλαίσια των καθημερινών του υποχρεώσεων και ψυχαγωγίας. Παρέχοντας τεράστιο όγκο πληροφορίας και άμεση ψηφιακή διασύνδεση κάθε γωνιάς του πλανήτη με τον υπόλοιπο κόσμο ανέξοδα και με υψηλές ταχύτητες, συμβάλλει μεταξύ άλλων στην αποτελεσματικότερη και ποικιλότροπη επικοινωνία μεταξύ των χρηστών του, στη βελτίωση των συναλλαγών, στην ανάπτυξη της αγοράς εργασίας εκτός γεωγραφικών συνόρων, στην εξέλιξη της επιστήμης και στη βελτίωση της εκπαιδευτικής διαδικασίας, με την τελευταία να είναι ιδιαίτερα σημαντική δεδομένου πως αφορά σε άτομα νεαρής ηλικίας [9].

Ωστόσο, κάθε χρήστης (user) του Διαδικτύου κρίνεται σκόπιμο να λαμβάνει υπόψη του πως όπως στον πραγματικό κόσμο έτσι και στον ψηφιακό κόσμο του Διαδικτύου, υπάρχουν κίνδυνοι, τους οποίους θα πρέπει να γνωρίζει προκειμένου προστατευτεί ώστε να είναι σε θέση να απολαμβάνει με ασφάλεια τα οφέλη που αυτό προσφέρει.

Οι έννοιες του «Κινδύνου» και της «Ασφάλειας στο Διαδίκτυο» δεν έχουν οριστεί με σαφήνεια από τους επιστήμονες του κλάδου και αυτός είναι ο λόγος απουσίας συγκεκριμένων ορισμών από τη βιβλιογραφία. Ενδεικτικά αναφέρονται ευρύτεροι ορισμοί των Διαδικτυακών Κινδύνων που εντοπίστηκαν έπειτα επιστάμενης αναζήτησης:

- Ο Volkmann, Matthew J. του Πανεπιστημίου της Αϊόβα (University of Iowa) των Η.Π.Α. αναφέρει:

«Οι Διαδικτυακοί κίνδυνοι μπορούν να οριστούν ως κάθε τι που μπορεί να προκαλέσει βλάβη σε ένα χρήστη του Διαδικτύου. Η βλάβη αυτή μπορεί να είναι διαφόρων μορφών όπως φυσική, συναισθηματική, ψυχολογική, οικονομική, κοινωνική ή στην υπόληψη του χρήστη.» (Internet dangers can be defined as anything that may cause harm to an internet user. This harm can come in many forms (e.g. physical, emotional, psychological, financial, social, and reputational).) [10]

- Η Warner-Blankenship, Jennifer M. του Πανεπιστημίου της Αϊόβα (University of Iowa) των Η.Π.Α. αναφέρει:

«Οι Διαδικτυακοί κίνδυνοι είναι κίνδυνοι που σχετίζονται με το να είναι κάποιος χρήστης του Διαδικτύου. Οι κίνδυνοι αυτοί μπορεί επίσης να αφορούν στην πρόσβαση σε ανεπιθύμητες πληροφορίες. Υπάρχει μεγάλη ποικιλία Διαδικτυακών κινδύνων από θέματα ασφάλειας έως διάφορα είδη θυματοποίησης.» (Internet dangers are risks involved with being an online member or internet user. These dangers can also be access to unwanted information. There are a large range of internet risks from security to various kinds of victimization.) [11]

- Η Ιαπωνική εταιρεία παροχής λύσεων ασφάλειας σε θέματα πληροφορικής, Trend Micro, αναφέρει σε φυλλάδιο ενημέρωσης με τίτλο *«The online protection talk»*:

«Ένας από τους πιο ευθείς τρόπους για να σκεφτεί και να μιλήσει κάποιος για τους Διαδικτυακούς κινδύνους είναι οι απειλές που ένα παιδί μπορεί να δεχθεί και αυτές που μπορεί ακόμη και ακούσια να προξενήσει.» (One of the most straightforward ways to think and talk about online dangers is in terms of threats your child may receive, and those he or she may, even inadvertently, send out.) [12]

- Το Wikipedia.org για την παρεμφερή έννοια της «Απειλής στον Ιστό» (Web threat) αναφέρει:

«Απειλή στον Ιστό είναι κάθε απειλή που χρησιμοποιεί το Παγκόσμιο Ιστό για να διευκολύνει το έγκλημα στο Διαδίκτυο.» (A web threat is any threat that uses the World Wide Web to facilitate cybercrime.) [13]

Συνοψίζοντας, το γενικότερο πνεύμα μελέτης του φαινομένου κινείται γύρω από την ευρύτερη διαπίστωση πως ***κίνδυνο*** αποτελεί καθετί που απειλεί τη ζωή, την ασφάλεια ή την ακεραιότητα ενός προσώπου ή ενός πράγματος [14] και αντίστοιχα ***ασφάλεια*** είναι η κατάσταση που χαρακτηρίζεται από την απουσία κινδύνου [15].

Τέλος, κρίνεται σκόπιμο να διευκρινιστεί πως η έννοια του κινδύνου είναι δυναμική καθώς προσδιορίζεται κοινωνικά, ταξικά και ηλικιακά, ενώ δεν είναι σταθερή στο χρόνο και στο χώρο, δεδομένου πως κάτι που αποτελεί κίνδυνο υπό ορισμένες συνθήκες μπορεί να είναι ασφαλές υπό άλλες.

2.2 Κατηγορίες - Είδη κινδύνων στο Διαδίκτυο

Η απουσία συγκεκριμένου επιστημονικού ορισμού των «Κινδύνων στο Διαδίκτυο» αντισταθμίζεται από την εκτενή αναφορά στις ποικίλες κατηγορίες κινδύνων από τις οποίες τεκμαίρεται και προσεγγίζεται ουσιαστικά και η έννοια των Κινδύνων αυτών.

Στο παρόν κεφάλαιο θα εξεταστούν οι συνηθέστερες κατηγορίες κινδύνων όπως αυτές καταγράφονται στην παγκόσμια βιβλιογραφία και δικτυογραφία, οι οποίες έχουν ως ακολούθως:

- Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content)
- Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages)
- Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation)
- Ηλεκτρονική αποπλάνηση χρηστών (Online grooming)
- Βίαια παιχνίδια (Violent games)
- Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction)
- Διαδικτυακός εκφοβισμός (Cyber bullying)
- Παρώθηση σε επιβλαβείς συμπεριφορές
- Ηλεκτρονικός τζόγος (Online gambling)
- Κακόβουλο λογισμικό που μολύνει Ηλεκτρονικούς Υπολογιστές (Η/Υ) (Malware)
- Παιδική πορνογραφία (Child pornography)
- Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy)
- Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation)
- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Phishing»
- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Pharming»
- Φυσικές παθήσεις που προκαλούνται από παρατεταμένη χρήση του Η/Υ

2.2.1 Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content) [16] [17] [18] [19]

Εικόνα 1: Σήμανση ακατάλληλου – προσβλητικού περιεχομένου

Ένα περιεχόμενο λεκτικό, οπτικό ή ακουστικό θεωρείται ακατάλληλο ή προσβλητικό όταν παραβιάζει τα κοινωνικά, θρησκευτικά ή πολιτισμικά πρότυπα ή τις προσωπικές και οικογενειακές αξίες του ατόμου.

Πιο συγκεκριμένα, το ακατάλληλο-προσβλητικό υλικό μπορεί να περιλαμβάνει ρατσιστικά, βίαια ή σεξουαλικώς προκλητικά στοιχεία, υλικό που προστατεύεται από πνευματικά δικαιώματα, απαγορευμένο ή παράνομο υλικό, να προάγει την ξενοφοβία, τη βία, τα ναρκωτικά, τα τυχερά παιχνίδια (τζόγο), επικίνδυνες ή εγκληματικές δραστηριότητες, ακραίες πολιτικές ή φυλετικές απόψεις και άλλες μη ασφαλείς συμπεριφορές όπως λόγου χάρη διατροφικές διαταραχές ή να παρουσιάζει πορνογραφικό υλικό. Αξίζει να σημειωθεί πως η ακαταλληλότητα και ο βαθμός προσβολής σχετίζεται στενά με την ηλικία και την ψυχική κατάσταση του ατόμου στο οποίο εκτίθεται το συγκεκριμένο περιεχόμενο, καθώς υπάρχουν περιπτώσεις που ένα περιεχόμενο θεωρείται ακατάλληλο για τα παιδιά ή/και τους εφήβους διότι ενδεχομένως να τα αναστατώσει, να τα ενοχλήσει, να τα ωθήσει σε ανάρμοστη συμπεριφορά ή να παρέχει εικόνες και αντιλήψεις που δεν είναι ακόμη έτοιμα να εξερευνήσουν· αντίθετα το ίδιο περιεχόμενο μπορεί να θεωρείται κατάλληλο για ενήλικα άτομα.

Το ακατάλληλο-προσβλητικό περιεχόμενο απαντάται συνήθως σε ιστοσελίδες αμφιβόλου προελεύσεως, σε Διαδικτυακά παιχνίδια (online games), στο ηλεκτρονικό ταχυδρομείο (e-mail), ενώ πλέον η πιθανότητα έκθεσης σε αυτό αυξάνεται με τη χρήση των κινητών τηλεφώνων τα οποία πλέον στις περισσότερες περιπτώσεις διαθέτουν διαρκή (24ωρη) πρόσβαση στο Διαδίκτυο.

2.2.2 Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages) [20] [21] [22]

Το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα συχνά κατακλύζονται από μηνύματα που διανέμονται μαζικά σε μεγάλο αριθμό παραληπτών (bulk mails) οι οποίοι υπό άλλες συνθήκες δε θα επέλεγαν να τα δουν (unsolicited material). Το περιεχόμενο αυτών των μηνυμάτων σχετίζεται συνήθως με τη διαφήμιση προϊόντων, την προώθηση ψευδο-τυχερών παιχνιδιών, ψευδο-νομικών υπηρεσιών, πορνογραφικού υλικού κ.ά.. Συχνά οι χρήστες λαμβάνουν αλυσιδωτά μηνύματα ηλεκτρονικού ταχυδρομείου (chain e-mails) στα οποία ο αποστολέας ζητά την προώθηση τους σε άλλους χρήστες. Ο κίνδυνος στην περίπτωση αυτή έγκειται στο γεγονός πως μαζί με το μήνυμα αυτό εμφανίζονται στις περισσότερες περιπτώσεις οι διευθύνσεις ηλεκτρονικού ταχυδρομείου (e-mail addresses) όλων των προηγούμενων ατόμων που προώθησαν το εν λόγω μήνυμα. Με τον τρόπο αυτό δε γνωρίζει κανείς ποιος θα λάβει το μήνυμα και με ποιο

τρόπο θα χρησιμοποιήσει τις ηλεκτρονικές διευθύνσεις που εμφανίζονται σε αυτό. Αξίζει, στο σημείο αυτό, να σημειωθεί ότι μία έρευνα φέρεται να αναφέρει πως η αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ανά έτος υπεύθυνη για την παραγωγή τόσων ρύπων του φαινομένου του θερμοκηπίου, όσων εκπέμπουν αντίστοιχα 3.100.000 αυτοκίνητα, ενώ κάθε χρόνο καταναλώνει 33.000.000.000 κιλοβατώρες (kWh), ενέργεια ικανή για τροφοδοτηθούν 2.400.000 σπίτια! [23]

Εικόνα 2: Διακωμωδώντας την πραγματικότητα των Ανεπιθύμητων μηνυμάτων

2.2.3 Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation) [24]

Η αλόγιστη χρήση του Διαδικτύου κυρίως με τη συμμετοχή σε Διαδικτυακά παιχνίδια, σε σελίδες κοινωνικής δικτύωσης και δωμάτια συνομιλίας (chat-rooms) δημιουργεί συναισθηματική απόσταση μεταξύ των ανθρώπων και αλλοιώνει την ποιότητα επικοινωνίας ανάμεσα τους με αποτέλεσμα την αποξένωση του χρήστη από τον πραγματικό κόσμο. Αρκετοί χρήστες του Διαδικτύου αφιερώνουν αναρίθμητες ώρες στις προαναφερθείσες δραστηριότητες γεγονός που λειτουργεί επιβαρυντικά για τον ελεύθερο χρόνο που θα μπορούσαν να διαθέσουν για τη δια ζώσης συμμετοχή σε κοινές δραστηριότητες με φίλους, γνωστούς και ομάδες ατόμων με ανάλογα ενδιαφέροντα. Είναι γνωστό άλλωστε ότι σήμερα πολλοί χρήστες του Διαδικτύου «ζουν» κατά βάση στην εικονική πραγματικότητα (virtual reality) που προσφέρουν τα σημερινά Διαδικτυακά παιχνίδια και οι λοιπές υπηρεσίες του Διαδικτύου (social networks, forums, chatrooms, instant messagers, κ.λπ.) με πρωταρχικό σκοπό να «χτίσουν» το εικονικό τους εαυτό (avatar) [25] παραμελώντας ακόμη και βασικές βιολογικές τους ανάγκες [26]. Με σκοπό την ενημέρωση και την πρόληψη της αποξένωσης αυτής, χαρακτηριστικό είναι το τηλεοπτικό σποτ [27] της εκστρατείας για την ασφαλή πλοήγηση στο Διαδίκτυο του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου [28] με τίτλο *«Σε ποιον κόσμο ζεις;»* σχετικά με την υπερβολική ενασχόληση με τους εικονικούς κόσμους.

2.2.4 Ηλεκτρονική αποπλάνηση χρηστών (Online grooming) [29] [30] [31]

Αποπλάνηση αποτελεί η κακόβουλη εκμετάλλευση από αγνώστους της ανωνυμίας που προσφέρει το Διαδίκτυο προκειμένου προσεγγίσουν ανήλικα άτομα με σκοπό να τα παρενοχλήσουν σεξουαλικά. Τα δωμάτια συνομιλίας (chat-rooms), οι σελίδες κοινωνικής δικτύωσης και τα Διαδικτυακά παιχνίδια είναι οι χώροι που δρουν συνήθως τέτοια άτομα (groomers) καθώς βρίσκουν πρόσφορο έδαφος δεδομένης της ύπαρξης πολλών υποψήφιων θυμάτων, της ευκολότερης και ταχύτερης προσέγγισης αυτών, της ανάπτυξης σχέσης εμπιστοσύνης σε αντιδιαστολή με την άμεση επαφή (face-to-face contact), καθώς και της δυνατότητας να καταχωρίσουν ψευδή στοιχεία σχετικά με την ταυτότητά τους, την ηλικία και το φύλο τους. Με τον τρόπο αυτό αναζητούν τα υποψήφια ανήλικα θύματα με τα οποία επιδιώκουν αρχικά να αναπτύξουν φιλική σχέση, προσποιούμενοι φιλικά-οικεία σε αυτά πρόσωπα ή υποσχόμενοι διάφορα δώρα ή χρησιμοποιώντας φιλοφρονήσεις και κολακευτικά σχόλια ή ποικιλόμορφες απειλές, ώστε να αποσπάσουν κατά το δυνατό περισσότερες πληροφορίες για αυτά (όπως τόπος διαμονής, ενδιαφέροντα, σεξουαλικές εμπειρίες, κ.λπ.) και να δημιουργήσουν σχέσεις εμπιστοσύνης με απώτερο σκοπό τη σεξουαλική συνεύρεση.

2.2.5 Βίαια παιχνίδια (Violent games) [32]

Τα ηλεκτρονικά παιχνίδια είτε παίζονται Διαδικτυακά (online games), είτε με τη δημιουργία αυτόνομου τοπικού δικτύου από τους παίκτες (multiplayer LAN games), είτε είναι παιχνίδια κονσόλας (video games) προσελκύουν το ενδιαφέρον εκατομμυρίων παιχτών καθημερινά. Τα ηλεκτρονικά παιχνίδια χαρακτηρίζονται από μια ευρεία γκάμα περιεχομένου με δημοφιλέστερα τα παιχνίδια δράσης (action games). Υποκατηγορίες αυτών είναι τα παιχνίδια ξυλοδαρμού και πολεμικών τεχνών (beat 'em up games, hack and slash games), πάλης (fighting games), βολών (shooter games) [33] κ.ά., με τα τελευταία να κατέχουν τα πρωτεία βιαιότητας και να έχουν δεχθεί έντονη κριτική αναφορικά με τα αρνητικά πρότυπα που προβάλλουν και τις αρνητικές επιδράσεις που ασκούν ιδιαίτερα σε άτομα νεαρής ηλικίας, χωρίς όμως να είναι βέβαιο το κατά πόσο τα βίαια ηλεκτρονικά παιχνίδια επηρεάζουν τελικά και τις πτυχές της προσωπικότητας του ατόμου στην καθημερινή του συμπεριφορά [34] [35].

Το γεγονός της μη ύπαρξης σαφών συμπερασμάτων, σχετικά με τη μεταφορά βίαιης συμπεριφοράς από τα παιχνίδια στον πραγματικό κόσμο, προκύπτει από τις διάφορες έρευνες που πραγματοποιήθηκαν κατά καιρούς.

Ενδεικτικά αναφέρονται: *α)* η έρευνα του Πανεπιστημίου του Τέξας (Texas A&M International University) που καταλήγει ότι η ενασχόληση με βίαια παιχνίδια αυξάνει την οπτικοχωρική νόηση (visuospatial cognition)[1] του ατόμου και σε κάποιες περιπτώσεις μπορεί να ενθαρρύνει προϋπάρχουσες βίαιες προτιμήσεις [36] και *β)* η έρευνα του ISFE (Interactive Software Federation of Europe) σύμφωνα με την οποία διαπιστώνεται πως η ενασχόληση με ένα βίαιο παιχνίδι αυξάνει τη διέγερση του ατόμου και την πιθανότητα να εμφανίσει επιθετική συμπεριφορά, μνημονεύοντας παράλληλα ότι η άμεση σύνδεση των παιχνιδιών με την εξωτερίκευση βίαιης συμπεριφοράς προς την κοινωνία παραμένει αναπάντητο ζήτημα [37]. Στον αντίποδα βρίσκεται η έρευνα του

[1] **Οπτικοχωρική νόηση** *[ελεύθερος ορισμός]***:** Μία ιδιαίτερα πολύπλοκη νοητική διεργασία του εγκεφάλου, η οποία απαιτεί τη διερευνητική οπτική σάρωση δια της κίνησης των ματιών, τη γρήγορη και ακριβή καθοδήγηση της προσοχής, την πρόβλεψη των συνεπειών των διαφόρων ενεργειών, την ενσωμάτωση του τρέχοντος οπτικού ερεθίσματος στις αποθηκευμένες αναπαραστάσεις τμημάτων της σκηνής που έχουμε δει σε προγενέστερο χρόνο, καθώς και τη γνώση των αντικειμένων και των σχέσεων μεταξύ τους.

Πανεπιστημίου της Βιλανόβα (Villanova University) και του Πανεπιστημίου Ράτγκερς (Rutgers University) σύμφωνα με την οποία τα βίαια παιχνίδια δεν έχουν άμεση συσχέτιση με τις βίαιες και παραβατικές συμπεριφορές που εμφανίζουν άτομα που ενασχολούνται με αυτά, σημειώνοντας χαρακτηριστικά ότι *«το να θεωρείται πως ένα νεαρό άτομο που διέπραξε ένα βίαιο έγκλημα είχε παίξει και ένα από τα δημοφιλή βίαια παιχνίδια, είναι τόσο άστοχο όσο το να επισημαίνουμε πως ο εγκληματίας φορούσε κάλτσες»* [38].

2.2.6 Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction) [39]

Ο εθισμός ή εξάρτηση στο Διαδίκτυο είναι το αποτέλεσμα της πολύωρης ενασχόλησης του χρήστη με Διαδικτυακές δραστηριότητες όπως ο ηλεκτρονικός τζόγος, η συμμετοχή σε δωμάτια συζητήσεων και η συμμετοχή σε Διαδικτυακά παιχνίδια. Εμφανίστηκε αρχικά σε ενήλικες και σύντομα σημείωσε ραγδαία επέκταση σε νεαρά άτομα.

Σύμφωνα με την Α. Τσίτσικα, Επίκουρη Καθηγήτρια Παιδιατρικής-Εφηβικής Ιατρικής και Επιστημονική Υπεύθυνο της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) της Β΄ Παιδιατρικής Κλινικής Πανεπιστημίου Αθηνών του Νοσοκομείου Παίδων «Π. & Α. Κυριακού» [40], ο όρος «εθισμός» ή «εξάρτηση» χρησιμοποιείται σε εισαγωγικά δεδομένου πως δεν απολαμβάνει της αποδοχής της Αμερικανικής Ψυχιατρικής Εταιρείας ως κατάσταση αληθούς εθισμού ενώ για να χαρακτηριστεί ένα άτομο ως εθισμένο στο Διαδίκτυο θα πρέπει να πληροί τουλάχιστον τρία από τα ακόλουθα χαρακτηριστικά:

i. Χρησιμοποιεί το Διαδίκτυο για μεγαλύτερο χρονικό διάστημα από αυτό που αρχικά είχε πρόθεση,

ii. Καταναλώνει πέραν του δέοντος χρόνο ή/και χρήμα σε Διαδικτυακές δραστηριότητες,

iii. Εμφανίζει Συμπτώματα Συνδρόμου Απόσυρσης, όπως ψυχοκινητική διέγερση, εκούσια ή ακούσια κίνηση δακτυλογράφησης των δακτύλων του χεριού, άγχος, έμμονη σκέψη για το Διαδίκτυο, όνειρα για το Διαδίκτυο,

iv. Χρησιμοποιεί το Διαδίκτυο προκειμένου να αποφύγει τα παραπάνω Συμπτώματα του Συνδρόμου Απόσυρσης,

v. Βιώνει έκπτωση της λειτουργικότητας σε κοινωνικό, οικογενειακό και προσωπικό επίπεδο, παραμελεί την προσωπική φροντίδα και υγιεινή, παρουσιάζει απώλεια ύπνου, προκαλεί ενδοοικογενειακές συγκρούσεις και βιώνει σχολική αποτυχία.

vi. Συνεχίζει τη χρήση του Διαδικτύου παρά τη γνώση της προαναφερθείσας έκπτωσης.

Ο βαθμός επικινδυνότητας του «εθισμού» ή της «εξάρτησης» αναδεικνύεται από τα ευρήματα έρευνας που πραγματοποίησε η Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) του Νοσοκομείου Παίδων «Π. & Α. Κυριακού» σε δείγμα 897 Ελλήνων εφήβων (430 αγοριών και 467 κοριτσιών) σύμφωνα με τα οποία το 1% των εφήβων παρουσίαζε υπερβολική χρήση του Διαδικτύου σε επίπεδο «εθισμού» και το 12,8% παρουσίαζε περιοδικά ή συχνά προβλήματα σχετικά με την κατάχρηση του Διαδικτύου βρισκόμενοι ένα στάδιο πριν τον «εθισμό».

Εικόνα 3: Μία παραστατική προσέγγιση του Διαδικτυακού εθισμού

Ο Κ. Σιώμος, Διδάκτωρ της Ιατρικής Σχολής του Πανεπιστημίου Θεσσαλίας και Ειδικευόμενος Ψυχίατρος Παίδων και Εφήβων στο Ιπποκράτειο Νοσοκομείο Θεσσαλονίκης, ορίζει ως άτομο εθισμένο στο Διαδίκτυο εκείνο που πέραν της πολύωρης ημερήσιας ενασχόλησης του με το Διαδίκτυο θα πρέπει να πληροί τα ακόλουθα επιστημονικά κριτήρια:

- *«Εξιδανίκευση του μέσου: Ο χρήστης θεωρεί τον Η/Υ ή το Διαδίκτυο το σημαντικότερο «κεφάλαιο» της καθημερινότητάς του.*
- *Τροποποίηση της διάθεσης: Σε όσους εθίζονται στα ηλεκτρονικά παιχνίδια παρουσιάζεται αύξηση της παραγωγής του νευροδιαβιβαστή του εγκεφάλου ντοπαμίνη, η οποία συνδέεται με την ευχαρίστηση.*
- *Ανοχή: Το άτομο χρειάζεται σταδιακά όλο και περισσότερες ώρες χρήσης του Η/Υ ώστε να νιώθει ευχαρίστηση.*
- *Σύγκρουση: Ενώ το παιδί αισθάνεται ότι έχει πρόβλημα, δεν μπορεί να κάνει κάτι για να περιορίσει τη χρήση του Η/Υ.*
- *Ενασχόληση αρχικώς με ηπιότερες και όχι τόσο εθιστικές λειτουργίες του Διαδικτύου, όπως είναι η αποστολή ηλεκτρονικών μηνυμάτων, και σταδιακή μετάβαση σε πιο διαδραστικές Διαδικτυακές λειτουργίες όπως τα δωμάτια συνομιλιών, οι ομάδες ειδήσεων ή ακόμη και τα αποκαλούμενα κοινωνικά παιχνίδια, όπως το «Second Life», στο οποίο κάθε χρήστης φτιάχνει μια νέα «εικονική» Διαδικτυακή ζωή με όλες τις εκφάνσεις της.»* [41]

Σχετική μελέτη που διεξήγαγε ο ίδιος σε 2200 μαθητές ηλικίας 12 έως 18 ετών σχολείων του Νομού Θεσσαλίας προέκυψε πως το 70,8% των μαθητών είχε πρόσβαση στο Διαδίκτυο το οποίο χρησιμοποιούσε κυρίως για τη συμμετοχή σε Διαδικτυακά ηλεκτρονικά παιχνίδια (50,9% των χρηστών) και υπηρεσίες πληροφοριών (46,8% των χρηστών), ενώ το 8,2% των χρηστών χαρακτηρίζεται από εθισμό με τα αγόρια να υπερτερούν έναντι των κοριτσιών με αναλογία 3:1 [42].

Εικόνα 4: Διαδικτυακή εξάρτηση – μία εικόνα χίλιες λέξεις

Οι Chakraborty, Basu και Vijaya Kumar, το έτος 2010, σε άρθρο τους με τίτλο *«Internet Addiction: Consensus, Controversies, and the Way Ahead»* [43], αναφέρουν πως ο «Διαδικτυακός εθισμός» είναι ο πιο διαδεδομένος όρος για την περιγραφή της δυσπροσαρμοστικής συμπεριφοράς του ατόμου που παρουσιάζει τα ακόλουθα χαρακτηριστικά:

(1) *Υπερβολική χρήση (excessive use), η οποία σχετίζεται συχνά με την απώλεια της αίσθησης του χρόνου,*

(2) *Απόσυρση (withdrawal), συμπεριλαμβάνοντας συναισθήματα θυμού, έντασης ή/και κατάθλιψης, όταν η πρόσβαση σε Η/Υ είναι αδύνατη,*

(3) *Ανοχή (tolerance), συμπεριλαμβάνοντας την ανάγκη για καλύτερο υπολογιστικό εξοπλισμό (computer equipment), περισσότερο λογισμικό (software) ή περισσότερες ώρες ενασχόλησης,*

(4) *Αρνητικές επιπτώσεις (negative repercussions), συμπεριλαμβάνοντας παράπονα, ψέματα, χαμηλή επίτευξη των στόχων, κοινωνική απομόνωση και κόπωση.*

Τέλος, αξίζει να σημειωθεί ότι σύμφωνα με έρευνα που φέρεται να διενεργήθηκε στη Μεγάλη Βρετανία από τους αναλυτές της εταιρείας *«The Future Laboratory»*, δύο στους τρεις ανθρώπους όταν βρεθούν σε ένα μέρος όπου το κινητό τους τηλέφωνο δεν έχει σήμα ή όταν η σύνδεσή τους στο Διαδίκτυο διακοπεί λόγω βλάβης, σύντομα καταλαμβάνονται από εκνευρισμό και άγχος. [44]

2.2.7 Διαδικτυακός εκφοβισμός (Cyber bullying)

Ο Διαδικτυακός Εκφοβισμός ορίζεται από τους P.K. Smith, J. Madhavi, M. Carvalho, M. Fisher, S. Russell και N. Tippett [45] ως *«μια επιθετική, σκόπιμη και επαναλαμβανόμενη πράξη η οποία πραγματοποιείται από ένα άτομο ή μια ομάδα ατόμων, μέσω της χρήσης ηλεκτρονικών μορφών επικοινωνίας, εναντίον ενός ατόμου που δεν μπορεί εύκολα να υπερασπιστεί τον εαυτό του».*

Η ολοένα αυξανόμενη χρήση των ηλεκτρονικών συσκευών και του Διαδικτύου καθιστά τον Διαδικτυακό Εκφοβισμό ως τη μορφή εκφοβισμού με το μεγαλύτερο ρυθμό αύξησης (Cart, 2010) [46].

Εικόνα 5: Απεικονίζοντας τον Διαδικτυακό εκφοβισμό ως αναπόσπαστο κομμάτι της Διαδικτυακής ζωής του θύτη

Πραγματοποιείται συνήθως μέσα από το ηλεκτρονικό ταχυδρομείο, τα δωμάτια συζητήσεων, τους ιστότοπους κοινωνικής δικτύωσης (social networking sites), τις ιστοσελίδες (web sites), τα ιστολόγια (blogs), τα Διαδικτυακά παιχνίδια και τα κινητά τηλέφωνα [47]. Οι μορφές που μπορεί να έχει είναι [48]:

- Η διακωμώδηση ή/και εξευτελισμός του θύματος
- Η αποστολή προσβλητικών και άσεμνων μηνυμάτων μέσω Διαδικτυακών εφαρμογών
- Το άσεμνο περιεχόμενο κατά τη διάρκεια συνομιλιών
- Ο εξευτελισμός ενός νεαρού ατόμου με τη δημιουργία ενός προφίλ ή ιστολογίου το οποίο περιλαμβάνει σκόπιμα λανθασμένα στοιχεία ή εξευτελιστικό περιεχόμενο
- Η αποστολή απειλητικών μηνυμάτων
- Η δημοσιοποίηση προσωπικών βίντεο ή φωτογραφιών χωρίς τη συγκατάθεση του ατόμου

Η ιδιαιτερότητα του Διαδικτυακού Εκφοβισμού έγκειται στο γεγονός πως επεμβαίνει στον προσωπικό χώρο του θύματος, ενώ είναι δύσκολος ο περιορισμός του εξαιτίας της αδυναμίας ελέγχου του αριθμού και του περιεχομένου των μηνυμάτων που μπορεί να λάβει ένας χρήστης του Διαδικτύου.

2.2.8 Παρώθηση σε επιβλαβείς συμπεριφορές [49]

Ανάμεσα στους κινδύνους του Διαδικτύου ο ιστότοπος *Ασφάλεια στο Διαδίκτυο του Παιδαγωγικού Ινστιτούτου Κύπρου* συμπεριλαμβάνει και τις επιβλαβείς συμπεριφορές που ενδέχεται να εκδηλώσει ο οποιοσδήποτε χρήστης του Διαδικτύου. Οι επιβλαβείς συμπεριφορές μπορούν να εμφανιστούν κατά την πλοήγηση του χρήστη σε οποιαδήποτε ιστοσελίδα, κάτι που οφείλεται στην αδυναμία ελέγχου του περιεχομένου εξαιτίας του γεγονότος πως το Διαδίκτυο δεν ανήκει στην ιδιοκτησία κανενός φυσικού ή νομικού προσώπου. Με τον τρόπο αυτό το άτομο έρχεται πολύ εύκολα σε επαφή με ακατάλληλο περιεχόμενο αφού οι ιστοσελίδες που παροτρύνουν τους επισκέπτες στην ανορεξία, τη βουλιμία, την αυτοκτονία, τον ηλεκτρονικό τζόγο κ.ά. παραμένουν προσβάσιμες σε όλους.

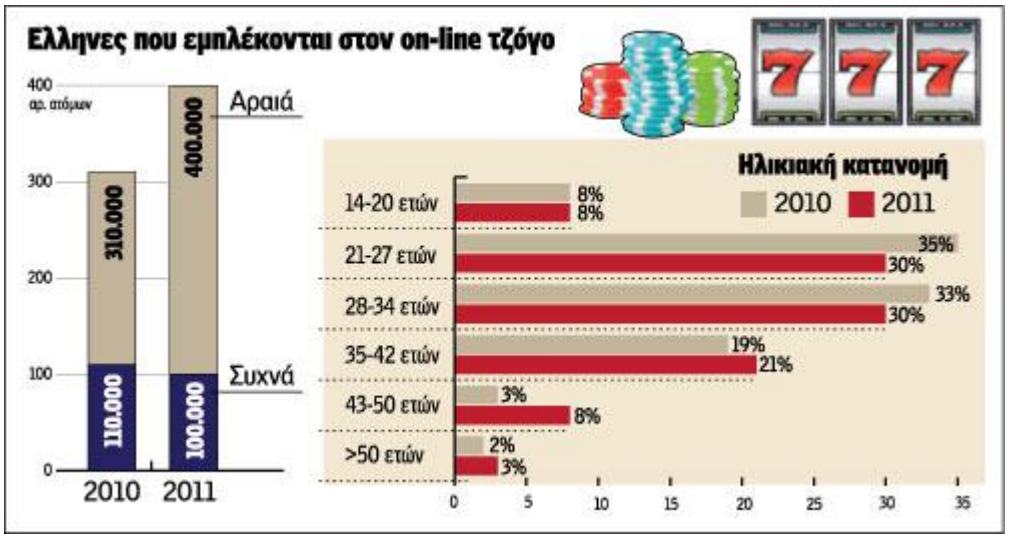
Χαρακτηριστικό παράδειγμα, σύμφωνα με τον παραπάνω ιστότοπο, είναι η έρευνα που διεξήχθη από την *British Medical Journal* όπου διαπιστώθηκε ότι οι χρήστες του Διαδικτύου που αναζητούν πληροφορίες για πιθανούς τρόπους αυτοκτονίας είναι πιθανότερο να βρουν ιστοσελίδες που την ενθαρρύνουν παρά που παρέχουν βοήθεια

και στήριξη· συγκεκριμένα από τις 240 ιστοσελίδες που βρέθηκαν το 2008 να αναφέρουν την αυτοκτονία, οι 45 περίπου την ενθάρρυναν, την προωθούσαν ή την διευκόλυναν.

2.2.9 Ηλεκτρονικός τζόγος (Online gambling)

Ο Ηλεκτρονικός τζόγος πραγματοποιείται όταν δύο ή περισσότερα άτομα συναντιούνται Διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων. Οι συμμετέχοντες σε αυτή την ανταλλαγή ρισκάρουν ανάμεσα στο κέρδος και την πραγματική οικονομική απώλεια με την τελευταία εκδοχή να αποτελεί ένα από τα βασικότερα προβλήματα του τζόγου. Πράγματι, ο συμμετέχων διατρέχει έντονα τον κίνδυνο απώλειας μεγάλων χρηματικών ποσών, ακίνητης περιουσίας, ακόμη και του/της συζύγου της/του! Σημαντική είναι η διαπίστωση πως η ευκολία πρόσβασης σε ιστοσελίδες ηλεκτρονικού τζόγου αυξάνει τον κίνδυνο συμμετοχής νεαρών ατόμων σε τέτοιου είδους δραστηριότητες [50].

Ανησυχητικά, σύμφωνα με άρθρο στο *«Ημερησία.gr»* [51], είναι τα ευρήματα της ετήσιας έρευνας του Εργαστηρίου Ηλεκτρονικού Επιχειρείν (ELTRUN) [52] του Οικονομικού Πανεπιστημίου Αθηνών για το έτος 2011 σύμφωνα με τα οποία περίπου 400.000 Έλληνες Διαδικτυακοί καταναλωτές ασχολούνται με τον Διαδικτυακό τζόγο, αριθμός που είναι κατά 25% μεγαλύτερος από τον αντίστοιχο αριθμό για το 2010. Κρίνεται σκόπιμο να επισημανθεί πως ένας στους τέσσερις Έλληνες Διαδικτυακοί καταναλωτές το κάνουν σε τακτική βάση.



Σχήμα 3: Στατιστικά στοιχεία ηλεκτρονικού τζόγου (Ελλάδα 2010-2011)

Ας σημειωθεί πως αναφορικά με τα ηλικιακά χαρακτηριστικά των Ελλήνων συμμετεχόντων στον Διαδικτυακό τζόγο σημαντικό είναι το ποσοστό 8% των νεαρών ατόμων ηλικίας 14 έως 20 ετών που δήλωσαν πως το έτος 2011 έπαιξαν στο Διαδικτυακό καζίνο, σε τυχερά παιχνίδια και σε στοιχήματα, καθώς αντιστοιχεί σε 30.000 περίπου νέους.

2.2.10 Κακόβουλο λογισμικό που μολύνει Ηλεκτρονικούς Υπολογιστές (Η/Υ) (Malware) [53] [54] [55] [56]

Το κακόβουλο λογισμικό δεν είναι τίποτα περισσότερο από μικρά προγράμματα λογισμικού που εξαπλώνονται από έναν Η/Υ σε έναν άλλο και παρεμβαίνουν στη λειτουργία τους· εμφανίστηκε για πρώτη φορά το έτος 1986 με τον επονομαζόμενο ιό «Brain» (Brain virus) [57]. Έκτοτε, το κακόβουλο λογισμικό διαφοροποιήθηκε και ιδίως με την εξάπλωση του Διαδικτύου απέκτησε ποικίλες μορφές ενώ η πιθανότητα προσβολής, υποκλοπής δεδομένων και προσωπικών πληροφοριών των χρηστών είναι πλέον ιδιαίτερα αυξημένη.

Όλες οι κατηγορίες κακόβουλου λογισμικού εγκαθίστανται στον Η/Υ, συνήθως εν αγνοία του χρήστη, και ενεργοποιούνται είτε αμέσως, είτε έπειτα από την παρέλευση κάποιου χρονικού διαστήματος ή από κάποια προκαθορισμένη ενέργεια. Η εγκατάσταση του λογισμικού αυτού μπορεί να γίνει μέσω του ανοίγματος μολυσμένων συνημμένων αρχείων του ηλεκτρονικού ταχυδρομείου (e-mail attached files), μέσω της ανταλλαγής αρχείων (file sharing), της εγκατάστασης μολυσμένων προγραμμάτων (infected programs) ή της πλοήγησης σε μολυσμένες ιστοσελίδες κατασκευασμένες με τρόπο που να εξυπηρετείται η μετάδοσή του. Τα αποτελέσματα της ενεργοποίησης αυτής ενδέχεται να είναι από πολύ απλά, όπως το επαναλαμβανόμενο άνοιγμα παραθύρων στην οθόνη (pop-ups), έως και πολύ σοβαρά, όπως η καταστροφή αρχείων, η πρόκληση βλαβών, ο μη εξουσιοδοτημένος απομακρυσμένος έλεγχος του Η/Υ (remote control), η αποστολή προσωπικών δεδομένων και πληροφοριών σε τρίτους, η υποκλοπή στοιχείων και προσωπικών αριθμών (πιστωτικών καρτών, κωδικών πρόσβασης, κ.ά.), καθώς και οτιδήποτε άλλο εξυπηρετεί τον προγραμματιστή του κακόβουλου λογισμικού.

Οι πιο συνηθισμένες και σημαντικές κατηγορίες κακόβουλου λογισμικού που απαντώνται στο Διαδίκτυο είναι οι ακόλουθες:

- Ιοί αρχείων (File Viruses),
- Δούρειοι ίπποι (Trojan Horses)
- Σκουλήκια (Worms),
- Ιοί απάτης (Hoax viruses),
- Πολυμορφικοί ιοί (Polymorphic viruses),
- Αόρατοι ιοί (Stealth Viruses),
- Καταγραφείς πληκτρολόγησης (Keyloggers)
- Rootkits,
- Bots,
- Λογισμικό Spyware – Adware.

2.2.11 Παιδική πορνογραφία (Child pornography)

Ο ορισμός της παιδικής πορνογραφίας διαφέρει ανάλογα με τη νομοθεσία κάθε χώρας, ωστόσο κοινό κριτήριο αποτελούν οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή σε καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές στον ορισμό περιλαμβάνονται και εικόνες που έχουν υποστεί επεξεργασία από Η/Υ ή και καρτούν [58].

Σύμφωνα με την παράγραφο 2 του άρθρου 9 της Σύμβασης για τα Διαδικτυακά Εγκλήματα (Convention on Cybercrime) του Συμβουλίου της Ευρώπης (Council of Europe) [59] 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 έναν ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Στην Ελλάδα οι έννοιες του υλικού της παιδικής πορνογραφίας και της πορνογραφικής παράστασης ορίζονται νομικά με την παράγραφο 3 του άρθρου 348Α και την παράγραφο 3 του άρθρου 348Γ του Ποινικού Κώδικα, αντίστοιχα. Οι ορισμοί αυτοί έχουν ως ακολούθως:

*«**Υλικό παιδικής πορνογραφίας**, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση, σε ηλεκτρονικό ή άλλο υλικό φορέα, των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.»* [60]

*«**Πορνογραφική παράσταση**, κατά την έννοια των προηγουμένων παραγράφων, συνιστά η οργανωμένη απευθείας έκθεση, που προορίζεται για θέαση ή ακρόαση, μεταξύ άλλων και με χρήση της τεχνολογίας των πληροφοριών και επικοινωνιών:*

α) ανηλίκου που επιδίδεται σε πραγματική ή εικονική πράξη γενετήσιου χαρακτήρα ή

β) των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση.» [61]

Με την έλευση του Διαδικτύου και κυρίως με τις υψηλές πλέον ταχύτητες μεταφοράς δεδομένων η παιδική πορνογραφία «άνθισε» προσφέροντας πλήθος υλικού στο Διαδίκτυο. Μία διενεργηθείσα έρευνα στο εξωτερικό κατέγραψε ότι ο μέσος όρος ηλικίας των ατόμων που εκτίθενται στη βιομηχανία της Διαδικτυακής πορνογραφίας είναι τα 11 χρόνια, ενώ υπάρχουν περίπου 100.000 ιστοσελίδες που προσφέρουν παράνομο υλικό παιδικής πορνογραφίας. Επίσης, έχουν καταγραφεί περίπου 116.000 αιτήματα χρηστών ανά ημέρα για ανεύρεση περιεχομένου παιδικής πορνογραφίας στο δίκτυο διαμοιρασμού αρχείων (file sharing network) «Gnutella» [62].

Η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις, ενώ υπάρχουν σημαντικές διαφορές στην αντιμετώπισή της από χώρα σε χώρα, όπως για παράδειγμα στην Ισπανία όπου ακόμη και η εν γνώση κατοχή υλικού παιδικής πορνογραφίας είναι έγκλημα.

Στην ελληνική επικράτεια ο Ποινικός Κώδικας με τα άρθρα 348Α, 348Β και 348Γ, καθορίζει τις κυρώσεις ανά περίπτωση οι οποίες (κυρώσεις) σε κάποιες περιπτώσεις είναι αυστηρότατες και μπορεί να ξεπεράσουν ακόμη και τα 15 έτη στην ποινή της κάθειρξης (άρθρο 348Γ παράγραφος 2 περίπτωση α').

Χαρακτηριστικός είναι ο χαρακτηρισμός ως ποινικά κολάσιμης πράξης της παραγωγής, προσφοράς, πώλησης, διάθεσης, διανομής, διαβίβασης, αγοράς, προμήθειας κατοχής ή πρόσβασης σε υλικό παιδικής πορνογραφίας μέσω της τεχνολογίας των πληροφοριών και των επικοινωνιών.

Συγκεκριμένα, οι παράγραφοι 2 και 5 του άρθρου 348Α ορίζουν αντίστοιχα:

«Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, ***μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών****, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.»* [63]

«Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας ***μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών****, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους.»* [64]

2.2.12 Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy) [65] [66] [67]

Δεδομένου πως η περιήγηση στο Διαδίκτυο έχει πολλά κοινά στοιχεία με τη ζωή του ατόμου στον πραγματικό κόσμο, τίθενται έντονα τα ζητήματα της προστασίας των προσωπικών δεδομένων, της ορθής και ηθικής επικοινωνίας μέσω της τεχνολογίας και του γεγονότος πως κάθε Διαδικτυακή δραστηριότητα αφήνει ηλεκτρονικά αποτυπώματα του χρήστη (user traces).

Η επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου, η πλοήγηση στο Διαδίκτυο, η αποστολή άμεσων μηνυμάτων (instant messages), η συμμετοχή σε σελίδες κοινωνικής δικτύωσης (π.χ. Facebook, Instagram) και ομάδες συζητήσεων (groups ή LISTSERVes), καθώς και οι επισκέψεις ιστολογίων του Διαδικτύου αποτελούν τα μέσα με τα οποία ο χρήστης του Διαδικτύου εκθέτει-παρέχει προσωπικά στοιχεία, που όταν συνδυαστούν συνθέτουν την πραγματική ταυτότητα της ιδιωτικής του ζωής. Η αποτύπωση των στοιχείων αυτών είναι άλλοτε ηθελημένη, όπως στην περίπτωση ανάρτησης φωτογραφιών στα μέσα κοινωνικής δικτύωσης, και άλλοτε ακούσια, όπως στην περίπτωση πλοήγησης στο Διαδίκτυο μέσω κάποιου φυλλομετρητή (browser) ο οποίος κρατάει αποθηκευμένα στοιχεία για τον Η/Υ και τις προτιμήσεις του χρήστη (cookies), τους ιστότοπους που επισκέφθηκε (browsing history), το υλικό που αναζήτησε ή «κατέβασε» από το Διαδίκτυο (search history, download history), κ.λπ..

2.2.13 Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation) [68] [69]

Το Διαδίκτυο αφενός μεν παρέχει αναρίθμητους πόρους και ευκαιρίες μάθησης, αφετέρου δε, σε αντίθεση με τα παραδοσιακά έντυπα μέσα, δεν διαθέτει τις απαραίτητες δικλείδες ασφαλείας για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται, με αποτέλεσμα σε κάποιες περιπτώσεις με τη δημοσίευση αναληθών, τροποποιημένων ή ελλιπών πληροφοριών μπορεί ο χρήστης να οδηγηθεί σε λανθασμένα, ανακριβή και αναξιόπιστα συμπεράσματα.

Χαρακτηριστικό παράδειγμα της παραπληροφόρησης είναι οι αστικοί μύθοι (urban legends) οι οποίοι λόγω του Διαδικτύου διαδίδονται με μεγαλύτερη ευκολία, σε περισσότερο πληθυσμό. Ο Connie Chesner, εκπαιδευτής στο Πανεπιστήμιο Wake Forest των Η.Π.Α. αναφέρει πως νέα χαρακτηριστικά, όπως η κακόβουλη πρόθεση, ο εμπλουτισμός με τεχνολογία υψηλότερης ποιότητας και με γνωρίσματα που παρέχουν φαινομενική αυθεντικότητα, κάνουν τους σημερινούς Διαδικτυακούς αστικούς μύθους πιο αληθοφανείς και ενδεχομένως πιο επιβλαβείς [70].

Κατά συνέπεια, κρίνεται αναγκαία η ανάπτυξη κριτικής σκέψης από το χρήστη του Διαδικτύου, προκειμένου κρίνει την ακρίβεια των πληροφοριών αυτών και ξεχωρίσει τη μη έγκυρη πληροφορία. Όπως είναι φυσικό ο κίνδυνος της παραπληροφόρησης είναι

ιδιαίτερα αυξημένος με απρόβλεπτα αποτελέσματα σε νεαρά άτομα τα οποία λόγω ηλικίας δεν έχουν οξυμένη την κριτική τους σκέψη και ικανότητα.

2.2.14 Υποκλοπή προσωπικών δεδομένων των χρηστών

2.2.14.1 «Phishing» [71] [72] [73]

Ο όρος «phishing» προσομοιάζει και παραπέμπει στον όρο «fishing», που σημαίνει «ψάρεμα». Η τεχνική που ακολουθείται είναι παρόμοια με την τεχνική ψαρέματος σε μία λίμνη με τη διαφορά πως στον ρόλο του ψαριού βρίσκονται οι προσωπικές, εμπιστευτικές πληροφορίες και τα ευαίσθητα δεδομένα (π.χ. κωδικοί πρόσβασης, αριθμοί ταυτότητας, διαβατηρίου, πιστωτικών καρτών) των υποψήφιων θυμάτων.

Η διαδικασία της υποκλοπής προσωπικών δεδομένων μέσω του «phishing» είναι συνήθως με αποστολή παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) ή άμεσων μηνυμάτων σε προγράμματα άμεσης επικοινωνίας (instant messagers) ή μηνυμάτων σε δωμάτια συνομιλιών (chat-rooms), τα οποία (μηνύματα) είναι ιδιαίτερα αληθοφανή καθώς φέρονται να προέρχονται από αξιόπιστες και έγκυρες πηγές, που καλούν τον χρήστη-θύμα να τους παρέξει εμπιστευτικές πληροφορίες ή να επισκεφτούν «παγιδευμένες» τοποθεσίες στον Ιστό (Web).

Μια τέτοιου είδους δραστηριότητα παρέχει τη δυνατότητα στο άτομο που εξαπατά (phisher) να κλέψει ή να πλαστογραφήσει τα στοιχεία του ατόμου που εξαπατάται ή/και να αποκτήσει παράνομη πρόσβαση στα δεδομένα του, όπως σε προσωπικούς λογαριασμούς, συνδρομές, ηλεκτρονικό ταχυδρομείο και αλλού, ενώ σε πιο σοβαρές περιπτώσεις απώτερος σκοπός του «phisher» είναι η κλοπή χρημάτων, η διενέργεια πλαστών συναλλαγών ή η μεταφορά κλεμμένων χρημάτων σε χρηματοπιστωτικά ιδρύματα ή σε άλλους παραλήπτες που εμπλέκονται στο έγκλημα.

Σημειώνεται στο σημείο αυτό ότι οι προαναφερθείσες «παγιδευμένες» τοποθεσίες χρησιμοποιούν ελεγχόμενα δίκτυα παγιδευμένων υπολογιστών που αλλάζουν συνεχώς Διαδικτυακή διεύθυνση (zombie networks), αποφεύγοντας να συμπεριληφθούν στις αναφορές για γνωστές τοποθεσίες «phishing» που λειτουργούν με σκοπό την προστασία των χρηστών.

Εικόνα 6: Αναπαριστώντας την έννοια «Phishing»

2.2.14.2 «Pharming» [74] [75] [76]

Το «Pharming» θεωρείται ως εξέλιξη του «Phishing» καθώς αποτελεί ιδιαιτέρως πιο επικίνδυνη μέθοδο εξαπάτησης μέσω Διαδικτύου. Συγκεκριμένα, πρόκειται για μια μορφή απάτης του ονόματος του ηλεκτρονικού τομέα (domain name) που δημιουργεί την εντύπωση στο χρήστη πως βρίσκεται σε γνήσια ιστοσελίδα στη σωστή ηλεκτρονική διεύθυνση (URL), ενώ στην πραγματικότητα οι απατεώνες έχουν καταφέρει να τον εκτρέψουν σε πλαστή ιστοσελίδα. Με τον τρόπο αυτό επιτυγχάνεται η απόσπαση στοιχείων του χρήστη που σχετίζονται συνήθως με οικονομικές συναλλαγές με αποτέλεσμα την οικονομική του εξαπάτηση. Για παράδειγμα, όταν ο χρήστης επισκέπτεται την ιστοσελίδα κάποιας Τράπεζας προκειμένου να πραγματοποιήσει ηλεκτρονικές συναλλαγές (on-line banking) οδηγείται μέσω εξαπάτησης σε πλαστή σελίδα πανομοιότυπη με αυτή της Τράπεζας, με τελικό αποτέλεσμα είτε την υποκλοπή των κωδικών του και την χρησιμοποίηση αυτών για παράνομες δραστηριότητες είτε ακόμη και την εν αγνοία του μεταφορά των χρημάτων του στους δράστες.

Σύμφωνα με δημοσίευση της ηλεκτρονικής εφημερίδας «Νομικά Επίλεκτα» το «pharming» εξελίσσεται σε μία από τις σοβαρότερες μορφές εγκληματικότητας στο Διαδίκτυο. Δεδομένου ότι η απόσπαση δεδομένων από τον χρήστη του Διαδικτύου γίνεται χωρίς τη συγκατάθεσή του και βασίζεται σε δόλο, η πράξη αυτή είναι και ποινικά κολάσιμη. Βάσει της παραγράφου 2 του άρθρου 370Γ του Ποινικού Κώδικα *«όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ ή σε περιφερειακή μνήμη Η/Υ ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα είκοσι εννέα (29) ευρώ. […]»* [77]

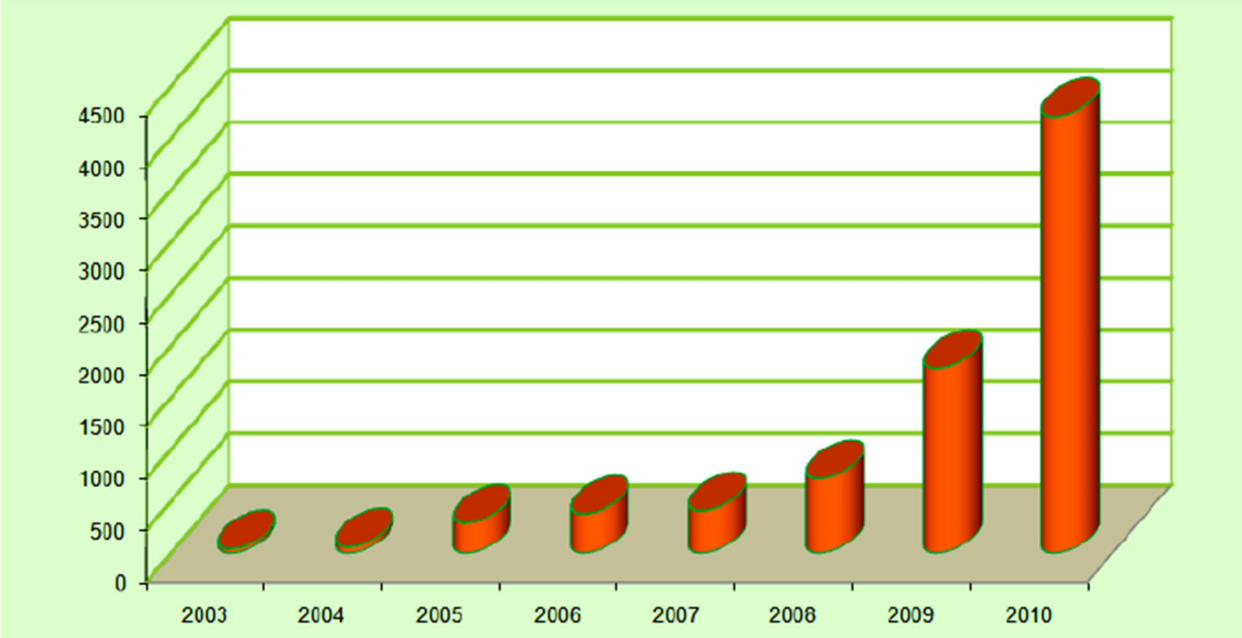
2.2.15 Φυσικές Παθήσεις που προκαλούνται από παρατεταμένη χρήση του Η/Υ [78] [79]

Η ανάπτυξη του Διαδικτύου ανά τον Κόσμο και η συνεχής ενασχόληση των ανθρώπων με αυτό λειτουργεί καταλυτικά στην εμφάνιση διαφόρων παθήσεων, που όμως είναι ανεξάρτητες από το είδος της Διαδικτυακής δραστηριότητας. Ως εκ τούτου, οι φυσικές παθήσεις αυτές θα μπορούσαν να χαρακτηριστούν ως ένα είδος κινδύνων του Διαδικτύου.

Οι παθήσεις αυτές σχετίζονται με την πολύωρη και χωρίς διάλλειμα χρήση του Η/Υ, την κακή στάση του σώματος κατά τη χρήση αυτού, τη λανθασμένη απόσταση των ματιών από την οθόνη και τη θέση της οθόνης αναφορικά με το επίπεδο των ματιών. Επιπλέον, σε περίπτωση που ο φωτισμός του χώρου δεν είναι επαρκής ή οι προδιαγραφές εξοπλισμού του Η/Υ δεν είναι τουλάχιστον εργονομικές, τότε επιβαρύνεται ακόμη περισσότερο η υγεία του χρήστη. Τα συνηθέστερα προβλήματα που εντοπίζονται αφορούν σε διαταραχές στην όραση και σε μυοσκελετικές παθήσεις που οφείλονται, πέραν της πολύωρης και χωρίς διάλλειμα ενασχόλησης με τον Η/Υ, και στην παράλληλη επανάληψη συγκεκριμένων κινήσεων. Άλλες παθήσεις είναι η τενοντίτιδα, το σύνδρομο του καρπιαίου σωλήνα, ο ευθειασμός του αυχένα και ο πόνος του αγκώνα.

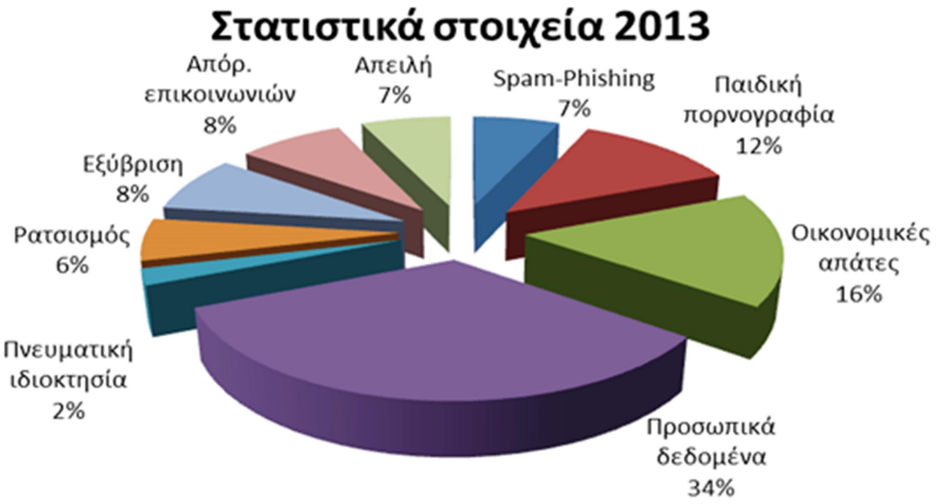
2.3 Οι κίνδυνοι του Διαδικτύου με αριθμούς [80] [81]

Ολοκληρώνοντας την αναφορά των κινδύνων του Διαδικτύου κρίνεται χρήσιμη η αναφορά στα στατιστικά στοιχεία που προκύπτουν από τον αριθμό των καταγγελιών που πραγματοποιήθηκαν κατά την τελευταία 10ετία στην ανοιχτή γραμμή καταγγελιών *«SafeLine»*, με το έτος 2013 το πλήθος των καταγγελιών να ανέρχεται στις 3904. Στο παρακάτω γράφημα απεικονίζεται η αυξητική τάση των καταγγελιών όπως αυτές καταγράφηκαν έως το έτος 2010:



Σχήμα 4: Στατιστικά στοιχεία καταγγελιών στη SafeLine.gr ανά έτος (2003-2010)

Σύμφωνα με τα στοιχεία, οι καταγγελίες αυτές αφορούν σε ένα ευρύ φάσμα επικίνδυνων και παράνομων δραστηριοτήτων στο Διαδίκτυο ενώ η κατηγορία που διακρίνεται από τον μεγαλύτερο αριθμό καταγγελιών είναι αυτή της παραβίασης Προσωπικών Δεδομένων (34%) και έπονται οι καταγγελίες για οικονομικές απάτες (16%), όπως φαίνεται και στο παρακάτω γράφημα:



Σχήμα 5: Στατιστικά στοιχεία καταγγελιών στη SafeLine.gr ανά κατηγορία (2013)

Η κατηγορία της Παιδικής Πορνογραφίας (12%) έρχεται τρίτη στη σειρά και καταλαμβάνει ένα αξιοσημείωτο ποσοστό καταγγελιών το οποίο συγκριτικά με το 2012, είναι αυξημένο κατά μία ποσοστιαία μονάδα καθώς το 2012, η κατηγορία αυτή αφορούσε το 11% των ληφθέντων καταγγελιών.

Αξίζει ακόμη να σημειωθεί, ότι το 2012, παρουσιάστηκε μια ραγδαία αύξηση των καταγγελιών (845 καταγγελίες) που αφορούσαν το μέσο κοινωνικής δικτύωσης *«Facebook»* και ο αριθμός αυτός αυξήθηκε ακόμη περισσότερο το 2013 αφού οι καταγγελίες ανήλθαν αριθμητικά στις 1551.

3. ΜΕΘΟΔΟΙ ΚΑΙ ΠΟΡΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Όπως έχει ήδη επισημανθεί στην παρούσα εργασία, το Διαδίκτυο προσφέρει εξαιρετικά οφέλη στην ανάπτυξη και υλοποίηση των δραστηριοτήτων του ανθρώπου, παρέχοντας άμεση πρόσβαση σε τεράστιο πλήθος πληροφοριών από όλο τον Κόσμο και προσφέροντας νέους τρόπους επικοινωνίας, ενώ διευρύνει τον πνευματικό ορίζοντα και τη δημιουργικότητα ιδίως των νεαρών ατόμων που βρίσκονται στο στάδιο ανάπτυξης της προσωπικότητάς τους. Ωστόσο, όπως αναλύθηκε νωρίτερα, οι χρήστες του Διαδικτύου υφίστανται μια σειρά από κινδύνους που ελλοχεύουν διαρκώς.

Με σκοπό, λοιπόν, την προστασία των χρηστών του Διαδικτύου και ιδιαιτέρως των ατόμων νεαρής ηλικίας, διάφοροι κρατικοί και ιδιωτικοί Φορείς διεθνώς έχουν ανά τα χρόνια αναπτύξει, ενώ εξελίσσουν συνεχώς, μία σειρά από **μεθόδους** και **πόρους** για την κατά το δυνατό αποτελεσματικότερη αντιμετώπιση των κινδύνων του Διαδικτύου.

3.1 Μέθοδοι Αντιμετώπισης των Κινδύνων του Διαδικτύου

Οι μέθοδοι αντιμετώπισης των κινδύνων του Διαδικτύου αποτελούν τους τρόπους και τα εργαλεία που έχει στη διάθεσή του ο εκάστοτε χρήστης προκειμένου προφυλαχθεί ο ίδιος ή προφυλάξει άμεσα ή έμμεσα άλλους χρήστες, συνήθως άτομα νεαρής ηλικίας και περιορισμένης κριτικής ικανότητας ή γνώσεων, από τους κινδύνους στους οποίους εκτίθενται.

Οι μέθοδοι αυτοί διακρίνονται σε δύο κύριες κατηγορίες:

(1) στις Τεχνικές Μεθόδους, και

(2) στις Μεθόδους Παιδαγωγικού Χαρακτήρα.

3.1.1 Τεχνικές Μέθοδοι Αντιμετώπισης

Οι Τεχνικές μέθοδοι αφορούν α) σε εργαλεία προστασίας από τους κινδύνους του Διαδικτύου δρώντας κατασταλτικά σε περίπτωση έκθεσης ή β) σε μέσα πρόληψης με τα οποία επιδιώκεται η αποτροπή έκθεσης του χρήστη στους κινδύνους αυτούς.

Συνήθως απαντώνται υπό τη μορφή λογισμικού (π.χ. φίλτρα), στις Τεχνικές όμως μεθόδους συμπεριλαμβάνονται και τρόποι - εργαλεία που παρέχουν πληροφόρηση στον χρήστη για τον τρόπο λειτουργίας κάποιου λογισμικού ή και των κινδύνων που ενδέχεται να εκτεθεί ο χρήστης κατά τη χρήση αυτού χωρίς να προσβλέπουν στην διαπαιδαγώγησή του παρά μόνο στην ενημέρωσή του (π.χ. σύστημα PEGI).

Παρακάτω, παρουσιάζονται οι σημαντικότερες Τεχνικές μέθοδοι αντιμετώπισης κινδύνων του Διαδικτύου.

3.1.1.1 Φίλτρα

Τα Φίλτρα αποτελούν εργαλεία λογισμικού τα οποία ρυθμίζουν την προσβασιμότητα του Η/Υ σε πληροφορίες και υπηρεσίες στο Διαδίκτυο βάσει προκαθορισμένων κριτηρίων.

Παρέχεται η δυνατότητα εγκατάστασής τους τόσο σε ατομικούς Η/Υ, όσο και σε κεντρικούς Η/Υ ενός δικτύου που ανήκει σε κάποιο κεντρικό φορέα, όπως για παράδειγμα σε σχολείο, και λειτουργούν άλλοτε προειδοποιητικά σε περίπτωση εντοπισμού προβληματικής ιστοσελίδας, μηνύματος ηλεκτρονικού ταχυδρομείου, κ.λπ., άλλοτε καταγράφοντας λεπτομερώς τις ενέργειες στις οποίες προβαίνει ο χρήστης και

άλλοτε επιτρέπουν την πρόσβαση σε συγκεκριμένες ημέρες και ώρες ή την απαγορεύουν σε ύποπτους ιστοχώρους, απενεργοποιώντας εφόσον απαιτηθεί ακόμα και τον Η/Υ [82].

Τα σημαντικότερα είδη φίλτρων που διατίθενται περιγράφονται παρακάτω:

3.1.1.1.1 Περιφραγμένες τοποθεσίες (Walled gardens) [83] – Λευκές λίστες (White lists [84])

Τα φίλτρα αυτά επιτρέπουν την ανταλλαγή πληροφοριών και την επίσκεψη ιστότοπων αποκλειστικά και μόνο υπό την προϋπόθεση ότι ο προς επίσκεψη ή ανταλλαγή πληροφοριών ιστότοπος βρίσκεται μέσα στην περιφραγμένη τοποθεσία ή εμπεριέχεται στη λευκή λίστα. Τα φίλτρα αυτά εντάσσονται στις πλέον αυστηρότερες πολιτικές προστασίας, αποκλείοντας κάθε ιστότοπο που δεν βρίσκεται εντός της περιφραγμένης τοποθεσίας ή δεν κατονομάζεται συγκεκριμένα ως «εγκεκριμένος» με αποτέλεσμα να αποκόπτονται και ιστότοποι των οποίων το περιεχόμενο δεν αποτελεί απαραίτητα απειλή.

3.1.1.1.2 Μαύρες λίστες (Black lists) [85]

Αποτελούνται από λίστες είτε ιστοσελίδων και Διαδικτυακών τοποθεσιών που πρέπει να αποφευχθούν λόγω ακατάλληλου περιεχομένου ή ύπαρξης άλλου κινδύνου (κακόβουλου λογισμικού, υποκλοπή προσωπικών δεδομένων, κ.λπ.), είτε απαγορευμένων λέξεων. Σε κάθε περίπτωση η απαγόρευση πρόσβασης έγκειται αποκλειστικά και μόνο στις τοποθεσίες που περιέχονται στη μαύρη λίστα, λειτουργώντας ουσιαστικά αντίστροφα σε σχέση με τις λευκές λίστες. Μειονέκτημα αυτού του φίλτρου αποτελεί ωστόσο η ανάγκη διαρκούς ενημέρωσης των μαύρων λιστών, με αποτέλεσμα τη μη εύκολη αποκοπή όλων των ιστότοπων που αποτελούν απειλή.

3.1.1.1.3 Ουδέτερες ζώνες (Demilitarized zones – DMZs) [86]

Αποτελούν ένα είδος ασφάλειας το οποίο εκθέτει στους κινδύνους του Διαδικτύου ένα τμήμα ενός δικτύου Η/Υ το οποίο δεν περιέχει σημαντικά δεδομένα. Έτσι, δημιουργεί μία ζώνη προστασίας και λειτουργεί ως ενδιάμεσο επίπεδο επικοινωνίας με τον κόσμο του Διαδικτύου μη επιτρέποντας σε τρίτους να έλθουν σε άμεση επαφή με το τοπικό δίκτυο Η/Υ (LAN – Local Area Network). Με άλλα λόγια θα μπορούσαμε να χαρακτηρίσουμε το ενδιάμεσο αυτό επίπεδο ως «ουδέτερη ζώνη». Το φίλτρο αυτό προστατεύει μόνο από κινδύνους σε επίπεδο λογισμικού (π.χ. εισερχόμενες επιθέσεις από κακόβουλο λογισμικό ή χρήστες) ενώ η πρόσβαση στο περιεχόμενο οποιασδήποτε ιστοσελίδας του Διαδικτύου δεν αποκόπτεται, συνεπώς δεν παρέχει προστασία από ενδεχόμενη επαφή με ακατάλληλο περιεχόμενο.

3.1.1.1.4 Διαχωρισμός ανεπιθύμητης – ομαδικής αλληλογραφίας (Spam – Bulk mail filtering) [87] [88]

Ίσως το πιο γνωστό φίλτρο ακόμα και στους αρχάριους χρήστες καθώς εφαρμόζεται σχεδόν από το σύνολο των παρόχων υπηρεσιών ηλεκτρονικού ταχυδρομείου ενώ όλοι οι χρήστες κάποια στιγμή έχουν δεχθεί ανεπιθύμητη ηλεκτρονική αλληλογραφία. Αποτελεί ουσιαστικά συνδυασμό διαφόρων μεθόδων ελέγχου και αξιολόγησης των εισερχόμενων μηνυμάτων ηλεκτρονικής αλληλογραφίας, οι οποίες έχουν ως σκοπό την εύρεση και τον διαχωρισμό τους (των μηνυμάτων) σε ανεπιθύμητα και μη. Οι μέθοδοι

αυτές ποικίλουν στον τρόπο προσέγγισης και διαχείρισης των μηνυμάτων ενώ διαχωρίζονται κυρίως σε μεθόδους *α)* βασισμένες σε λίστες όπως μαύρες λίστες, λευκές λίστες, γκρίζες λίστες (grey lists), κ.λπ., και *β)* βασισμένες στο περιεχόμενο όπως λεξικογραφικές (word-based), ευρεστικές (heuristic), πιθανοτικές (Bayesian), κ.λπ., χωρίς αυτό να σημαίνει ότι δεν υπάρχουν και πολλές άλλες. Αξίζει να σημειωθεί ότι όποια μέθοδος ή συνδυασμός μεθόδων και αν χρησιμοποιηθεί το αποτέλεσμα δεν είναι ποτέ 100% ακριβές με άμεση συνέπεια να παρατηρείται πολλές φορές το φαινόμενο της σήμανσης ενός εισερχόμενου μηνύματος ως ανεπιθύμητο χωρίς πραγματικά να είναι, και αντίστροφα.

3.1.1.1.5 Αξιολόγηση - Βαθμολόγηση ιστοσελίδων (Website rating)

Ταξινόμηση ολόκληρου του περιεχομένου που περιέχεται σε μια ιστοσελίδα, χρησιμοποιώντας στατιστικές μεθόδους, όπως αυτές που εφαρμόζουν τα φίλτρα ανεπιθύμητης αλληλογραφίας ή με μεθόδους βαθμολόγησης από την παγκόσμια κοινότητα χρηστών του Διαδικτύου (crowdsourcing approach) [89] [90].

3.1.1.1.6 Αυτοαξιολόγηση ιστοσελίδων [91] [92]

Οι πάροχοι της Διαδικτυακής πληροφορίας τοποθετούσαν στον αντίστοιχο ιστοχώρο, εθελοντικά, μια ετικέτα που περιέγραφε τον βαθμό κατά τον οποίο περιέχεται υλικό ακατάλληλο για ανηλίκους (π.χ. βία, Διαδικτυακός τζόγος, κ.ά.). Οι ετικέτες, που δημιουργήθηκαν από την Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου «ICRA» (Internet Content Rating Association), διαβάζονται από το φίλτρο και αυτό με τη σειρά του αποφασίζει αν θα επιτρέψει την πρόσβαση σε αυτές ανάλογα με τις επιλογές που έχουν προηγουμένως τεθεί από τον χρήστη ή τους επιβλέποντες (π.χ. γονείς). Δυστυχώς, τροχοπέδη σε αυτή τη μορφή φιλτραρίσματος αποτέλεσε ο περιορισμένος αριθμός των παρόχων που εκδήλωσαν ενδιαφέρον συμμετοχής στην εν λόγω δράση, λόγω του εθελοντικού και όχι υποχρεωτικού χαρακτήρα της τοποθέτησης των ετικετών αυτών, με αποτέλεσμα την παύση λειτουργίας του οργανισμού «ICRA» το έτος 2010. Γίνεται μνεία ότι τα φίλτρα που χρησιμοποιούσαν τις ετικέτες αυτές εξακολουθούν να λειτουργούν μέχρι και σήμερα με τις υπάρχουσες ετικέτες που εκδόθηκαν πριν την παύση λειτουργίας του οργανισμού.

3.1.1.1.7 Συνδυασμός μεθόδων φιλτραρίσματος

Με σκοπό τον αποτελεσματικότερο έλεγχο των ιστοσελίδων παράλληλα με τη διαφοροποίηση στην προσβασιμότητα ανάλογα με την ηλικία του χρήστη και την επιθυμία έκθεσής του στο Διαδικτυακό περιεχόμενο, υπάρχουν λογισμικά πακέτα και εργαλεία που ενσωματώνουν πολλά είδη φίλτρων ταυτόχρονα τα οποία λειτουργούν σε συνδυασμό μεταξύ τους.

3.1.1.2 Γονικός Έλεγχος (Parental control) [93] [94]

Ο Γονικός Έλεγχος είναι ένα εργαλείο λογισμικού ή πρόγραμμα Η/Υ το οποίο χρησιμοποιεί διάφορα είδη φίλτρων προκειμένου περιορίσει την πρόσβαση των ανήλικων χρηστών, μέσα από προκαθορισμένους κανόνες που τίθενται αυτόματα από το λογισμικό ή από τον επιβλέποντα γονέα.

Τα είδη του Γονικού Ελέγχου διακρίνονται σε τρεις βασικές κατηγορίες:

- **στα φίλτρα περιεχομένου**, που απαγορεύουν την πλοήγηση σε ιστοχώρους με ακατάλληλο για ανηλίκους περιεχόμενο ή περιεχόμενο που ενέχει άλλα είδη κινδύνων (π.χ. κακόβουλο λογισμικό, κ.λπ.).
- **στα εργαλεία περιορισμού χρήσης του Η/Υ**, που καθορίζουν τις επιτρεπόμενες ώρες πρόσβασης στον Η/Υ και τη χρονική διάρκεια χρήσης αυτού.
- **στα εργαλεία παρακολούθησης της χρήσης του Η/Υ**, που καταγράφουν τις κινήσεις του ανήλικου χρήστη ή και ενημερώνουν τον επιβλέποντα γονέα (π.χ. μέσω κάποιου e-mail).

3.1.1.3 Προγράμματα προστασίας και καταπολέμησης κακόβουλου λογισμικού (Antivirus – Antimalware) [95] [96] [97] [98]

Τα προγράμματα προστασίας από κακόβουλο λογισμικό (antivirus – antimalware) είναι λογισμικά πακέτα ή προγράμματα τα οποία εντοπίζουν ιούς, spywares, adwares, trojans και άλλο κακόβουλο λογισμικό. Αυτά τα λογισμικά πακέτα-προγράμματα προστασίας εγκαθίστανται από τον χρήστη στον Η/Υ του προκειμένου ελέγχουν συστηματικά όλα τα αποθηκευμένα αρχεία, τις τρέχουσες διεργασίες (processes) στη μνήμη (RAM), καθώς και κάθε αρχείο που λαμβάνεται με κάθε τρόπο από το δίκτυο (network) ή το Διαδίκτυο. Σημαντικό πλεονέκτημα αυτών των προγραμμάτων αποτελεί το γεγονός πως λειτουργούν σε πραγματικό χρόνο (real time) με αποτέλεσμα κάθε δραστηριότητα (activity) του χρήστη να ελέγχεται αυτοστιγμής και σε περίπτωση που ανιχνευθεί κάτι κακόβουλο τον ενημερώνει άμεσα ενώ παράλληλα απομονώνει (quarantines) ή επιδιορθώνει (cleans) τα προσβεβλημένα αρχεία (infected files) αποτρέποντας την περαιτέρω μόλυνση και διάδοση του κακόβουλου λογισμικού. Προκειμένου διατηρείται η αποτελεσματικότητα αυτών των προγραμμάτων προστασίας στην πάροδο του χρόνου κρίνεται αναγκαία η συχνή αναβάθμιση (upgrade) και ενημέρωσή τους (update).

Εικόνα 7: Λογότυπα δημοφιλέστερων προγραμμάτων «Antivirus» με άδεια ελεύθερης χρήσης

3.1.1.4 Τείχος Προστασίας «Firewall» [99] [100] [101]

Το Τείχος Προστασίας «Firewall» είναι μια συσκευή ή λογισμικό το οποίο είναι κατάλληλα σχεδιασμένο ώστε να αποτρέπει ή να διακόπτει τη μη εξουσιοδοτημένη πρόσβαση από τον «έξω» κόσμο του δικτύου ή Διαδικτύου στον ή στους προστατευόμενους Η/Υ και αντίστροφα την ανεξέλεγκτη ροή πληροφορίας προς τον «έξω» κόσμο.

Ο βασικός τρόπος λειτουργίας ενός τείχους προστασίας «firewall» έγκειται στον διαρκή έλεγχο της κίνησης δεδομένων (traffic control) από και προς το δίκτυο ή Διαδίκτυο επιτρέποντας ή απαγορεύοντας την κίνηση αυτή ανάλογα με τους κανόνες που έχει ορίσει ο χρήστης ή ο διαχειριστής του συστήματος (administrator). Το τείχος προστασίας πάντα παρεμβάλλεται ανάμεσα στον «έξω» κόσμο του δικτύου ή Διαδικτύου και στον Η/Υ ή το τοπικό δίκτυο Η/Υ, λειτουργώντας ως συνδετικός κρίκος εξαναγκάζοντας κάθε λαμβανόμενη ή αποστελλόμενη πληροφορία να διέλθει και να ελεγχθεί από αυτό.

Τα «firewalls» διακρίνονται σε δύο μεγάλες κατηγορίες:

(i) στα *Hardware Firewalls*, τα οποία είναι είτε αυτόνομες συσκευές (stand-alone devices) που συνδέονται απευθείας στο δίκτυο, είτε Η/Υ που διαθέτουν συγκεκριμένα ειδικά λογισμικά και λειτουργούν αποκλειστικά για τον έλεγχο και την προστασία ενός δικτύου Η/Υ, και

(ii) στα *Software Firewalls*, τα οποία είναι προγράμματα Η/Υ που εγκαθίστανται από τον χρήστη στον προσωπικό του Η/Υ. Για τον λόγο αυτό πολλές φορές τα τείχη προστασίας αυτά αποκαλούνται και «Personal Firewalls».

Εικόνα 8: Αναπαράσταση της έννοιας του Τείχους προστασίας «firewall»

3.1.1.5 PEGI (Pan-European Game Information) [102] [103]

Το σύστημα ηλικιακών διαβαθμίσεων με την ονομασία *«Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια» (Pan-European Game Information – PEGI)* δημιουργήθηκε από την Ευρωπαϊκή Ομοσπονδία Αλληλεπιδραστικού Λογισμικού (Interactive Software Federation of Europe – ISFE) προκειμένου βοηθηθούν οι Ευρωπαίοι γονείς στη λήψη σωστών αποφάσεων σχετικά με την αγορά παιχνιδιών που παίζονται μέσω Η/Υ για τα παιδιά τους, με απώτερο σκοπό να διασφαλιστούν τα ανήλικα άτομα από ακατάλληλα για αυτά παιχνίδια. Τέθηκε σε εφαρμογή το έτος 2003 αντικαθιστώντας τα συστήματα ηλικιακών διαβαθμίσεων που λειτουργούσαν σε εθνικό επίπεδο διαφόρων ευρωπαϊκών χωρών με ένα ενιαίο σύστημα που εφαρμόζεται στο μεγαλύτερο μέρος της Ευρώπης, ενώ υποστηρίζεται από τους κυριότερους κατασκευαστές παιχνιδομηχανών (game consoles) και τους εκδότες και προγραμματιστές αλληλεπιδραστικών παιχνιδιών (interactive games) σε όλη την Ευρώπη.

Το σύστημα «PEGI» αποτελείται από δύο μέρη:

1. την κατάταξη του παιχνιδιού σε ηλικιακές ομάδες, και
2. τον χαρακτηρισμό του περιεχομένου του παιχνιδιού.

Η ετικέτες πληροφόρησης «PEGI» βρίσκονται συνήθως στο πίσω ή και εμπρός μέρος της συσκευασίας του παιχνιδιού (DVD box).

3.1.1.5.1 PEGI: Κατάταξη του παιχνιδιού σε ηλικιακές ομάδες [104]

Σύμφωνα με το σύστημα «PEGI» οι ηλικιακές ομάδες στις οποίες κατατάσσονται τα παιχνίδια είναι οι 3+, 7+, 12+, 16+, και 18+ και υποδηλώνουν την κατώτατη ηλικία στην οποία απευθύνεται το παιχνίδι ώστε να θεωρείται κατάλληλο. Αξίζει να τονιστεί πως ο χαρακτηρισμός του «PEGI» δεν αναφέρεται στο βαθμό δυσκολίας του παιχνιδιού ή τις ικανότητες που απαιτούνται, αλλά αποκλειστικά και μόνο στο βαθμό επικινδυνότητάς του και κατ' επέκταση α-καταλληλότητας.

Οι ετικέτες ηλικιακής κατάταξης του συστήματος «PEGI» αποτυπώνονται στην εικόνα που ακολουθεί:

Εικόνα 9: Ετικέτες κατάταξης σε ηλικιακές ομάδες «PEGI»

3.1.1.5.2 PEGI: Χαρακτηρισμός του περιεχομένου [105]

Προκειμένου ένα παιχνίδι λάβει έναν συγκεκριμένο ηλικιακό χαρακτηρισμό λαμβάνεται υπόψη το περιεχόμενο αυτού. Έτσι, στο πίσω μέρος της συσκευασίας ενός παιχνιδιού αναφέρονται οι περιγραφικές ομάδες που αποτέλεσαν τους κύριους λόγους κατάταξης του εν λόγω παιχνιδιού στον συγκεκριμένο ηλικιακό χαρακτηρισμό.

Οι περιγραφικές αυτές ομάδες είναι οκτώ και αποτυπώνονται υπό τη μορφή διαφορετικών ετικετών, οι οποίες έχουν ως ακολούθως:

Εικόνα 10: Ετικέτες χαρακτηρισμού περιεχομένου «PEGI»

Πιο αναλυτικά οι ετικέτες-ενδείξεις αυτές υποδεικνύουν για το εκάστοτε παιχνίδι:

- **Χυδαία γλώσσα (Bad Language)**: Εμπεριέχεται χυδαία γλώσσα.
- **Διακρίσεις (Discrimination)**: Απεικονίζονται διακρίσεις ή εμπεριέχεται υλικό που μπορεί να τις ενθαρρύνει.
- **Ναρκωτικά (Drugs)**: Απεικονίζεται η χρήση ναρκωτικών ή εμπεριέχονται αναφορές σε αυτή.
- **Φόβος (Fear)**: Ενδέχεται να είναι τρομακτικό για τα μικρά παιδιά.
- **Τζόγος (Gambling)**: Παροτρύνει σε τζόγο ή τον διδάσκει.
- **Σεξ (Sex)**: Απεικονίζεται γυμνό ή και σεξουαλική συμπεριφορά ή εμπεριέχονται σεξουαλικές αναφορές.
- **Βία (Violence):** Εμπεριέχονται απεικονίσεις βίας.
- **Διαδικτυακό παιχνίδι (Online):** Το παιχνίδι δύναται να παιχτεί μέσω Διαδικτύου *(βλ. παράγραφο «3.1.1.5.4 PEGI Online»)*.

3.1.1.5.3 Η ένδειξη «PEGI OK» [106]

Με την ανάπτυξη των Διαδικτυακών παιχνιδιών, μικρού συνήθως μεγέθους που προσφέρονται μέσω ποικίλων ιστότοπων, υπήρξε ανάγκη για τη σήμανσή τους σχετικά με την καταλληλότητά τους.

Με αφορμή την ανάγκη αυτή δημιουργήθηκε η σήμανση «PEGI OK» την οποία φέρει ένας δικτυακός τόπος όταν το παιχνίδι που προσφέρει μπορεί να παιχτεί από παίκτες όλων των ηλικιακών ομάδων, καθώς δεν περιλαμβάνει δυνητικά ακατάλληλο περιεχόμενο και συγκεκριμένα δεν περιέχει τρομακτικές σκηνές ή στοιχεία βίας, σεξουαλικής δραστηριότητας, σεξουαλικών υπονοούμενων, γυμνού, χυδαίας γλώσσας, τζόγου, προώθησης ή χρήσης ναρκωτικών και προώθησης αλκοόλ ή καπνού.

Σε περίπτωση που το παιχνίδι περιέχει οποιοδήποτε από αυτά τα στοιχεία, τότε η διαβάθμιση πραγματοποιείται μέσω του συνήθους συστήματος κατάταξης PEGI όπως περιγράφηκε στις προηγούμενες παραγράφους.

Εικόνα 11: Η ένδειξη «PEGI OK»

3.1.1.5.4 PEGI Online [107]

Το σύστημα «PEGI» επεκτάθηκε με την προσθήκη του «PEGI Online» ώστε να παρέχει στα ανήλικα άτομα προστασία από πιθανό ακατάλληλο περιεχόμενο των Διαδικτυακών παιχνιδιών (online games) και να βοηθήσει τους γονείς στην κατανόηση των κινδύνων και της βλαπτικής πιθανότητας στα πλαίσια του εν λόγω περιβάλλοντος. Για τον λόγο αυτόν, τα Διαδικτυακά παιχνίδια που φέρουν την ένδειξη «PEGI Online» υποχρεούνται να *α)* αφαιρούν από την ιστοσελίδα τους παράνομο ή προσβλητικό περιεχόμενο που έχει δημιουργηθεί από χρήστες, *β)* αφαιρούν ανεπιθύμητους συνδέσμους και *γ)* λαμβάνουν τα απαιτούμενα μέτρα προστασίας των ατόμων νεαρής ηλικίας και του ιδιωτικού τους απορρήτου κατά τη διάρκεια της συμμετοχής τους στο Διαδικτυακό παιχνίδι.

Εικόνα 12: Τα λογότυπα «PEGI Online»

Το Διαδικτυακό λογότυπο του «PEGI Online» εμφανίζεται στη συσκευασία του παιχνιδιού αν αυτό πωλείται σε μορφή CD/DVD ή στον ίδιο τον δικτυακό τόπο του παιχνιδιού.

Με το λογότυπο αυτό υποδεικνύεται τόσο ότι το παιχνίδι επιτρέπεται να παίζεται σε Διαδικτυακή σύνδεση, όσο και ότι το συγκεκριμένο παιχνίδι ή ο δικτυακός τόπος βρίσκεται υπό τον έλεγχο κάποιου φορέα ο οποίος ενδιαφέρεται για την προστασία των νέων ατόμων.

3.1.2 Μέθοδοι Αντιμετώπισης Παιδαγωγικού Χαρακτήρα

Οι μέθοδοι Αντιμετώπισης Παιδαγωγικού Χαρακτήρα αφορούν σε τρόπους και μέσα διαπαιδαγώγησης των χρηστών και των επιβλεπόντων προσώπων αυτών (π.χ. γονείς, δάσκαλοι, κ.λπ.) με σκοπό την ασφαλή επαφή με το Διαδίκτυο, την αναγνώριση των κινδύνων, την αντιμετώπιση αυτών, κ.λπ..

Οι διαπαιδαγώγηση αυτή πραγματοποιείται με κάθε πρόσφορο τρόπο επικοινωνίας όπως μέσω του ιδίου του Διαδικτύου, των Μέσων Μαζικής Ενημέρωσης, την αυτοπρόσωπη παρουσία των χρηστών και λοιπών ενδιαφερομένων σε διοργανώσεις ποικίλων Αρχών, Φορέων, Οργανώσεων και Οργανισμών.

Παρακάτω, παρουσιάζονται μερικοί από το πιο ευρέως διαδεδομένους τρόπους διαπαιδαγώγησης στον ελληνικό χώρο.

3.1.2.1 Τηλεδιασκέψεις – Διαδικτυακά σεμινάρια (Webinars)

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας στα πλαίσια του προγράμματος «Cyberkid» πραγματοποιεί διαδραστικές τηλεδιασκέψεις στα σχολεία όλης της Χώρας με θέμα την *Ασφαλή Πλοήγηση των Μαθητών στο Διαδίκτυο.* Το πρόγραμμα αποτελεί μια σύμπραξη του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη, της Ελληνικής Αστυνομίας και του Υπουργείου Παιδείας και Θρησκευμάτων [108]. Στην υλοποίηση αυτών των τηλεδιασκέψεων συμμετέχει το Πανελλήνιο Σχολικό Δίκτυο που μέσω του συστήματος *meetings.sch.gr* εντάσσει τα σχολεία που συμμετέχουν στις τηλεδιασκέψεις [109] [110]. Ενδεικτικά αναφέρεται ότι τριακόσια σχολεία τις Δευτεροβάθμιας Εκπαίδευσης της χώρας συμμετείχαν στην τηλεδιάσκεψη που πραγματοποιήθηκε την 21/10/2014 [111], κατά τη διάρκεια της οποίας προσεγγίστηκαν οι παρακάτω θεματικές ενότητες:

- Τα αδικήματα μέσω Διαδικτύου, ο τρόπος με τον οποίο διαπράττονται και πρακτικές πρόληψης.
- Τα φαινόμενα Διαδικτυακής Βίας, οι κίνδυνοι που ελλοχεύουν από τις ιστοσελίδες κοινωνικής δικτύωσης και γενικότερα η πρόληψη και η αντιμετώπιση κινδύνων που σχετίζονται με τις νέες τεχνολογίες.
- Στατιστικά στοιχεία που αφορούν στη διείσδυση των Ελλήνων στο Διαδίκτυο καθώς και τις υποθέσεις που καλείται να αντιμετωπίσει η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Η εν λόγω προσπάθεια έχει ως στόχο την ενημέρωση όλων των μαθητών της Χώρας σε βάθος οκταμήνου (Σεπτέμβριος 2014 – Απρίλιος 2015) ενώ σημαντική κρίνεται η δυνατότητα υποβολής ερωτήσεων-αποριών των μαθητών, από τον υπεύθυνο κάθε σχολείου στους εξειδικευμένους Αξιωματικούς που πραγματοποιούν την τηλεδιάσκεψη, μέσω άμεσης γραπτής ηλεκτρονικής συνομιλίας (chat).

Στο ίδιο περίπου πλαίσιο κινούνται και τα διάφορα Διαδικτυακά σεμινάρια (webinars) που αποτελούν μία νέα τάση στην εύκολη και γρήγορη επιμόρφωση των ενδιαφερομένων.

Ενδεικτικά αναφέρονται: *α)* το Διαδικτυακό σεμινάριο που πραγματοποιήθηκε τον Ιανουάριο του 2014 με αφορμή την 8^{η} Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων, από την Περιφερειακή Διεύθυνση Εκπαίδευσης Δυτικής Ελλάδας, τους σχολικούς συμβούλους Πληροφορικής σε συνεργασία με τον ενημερωτικό κόμβο του Πανελλήνιου Σχολικού Δικτύου «Ασφάλεια στο Διαδίκτυο» και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, έχοντας ως θέμα «Προστασία Προσωπικών Δεδομένων και Κοινωνικά Δίκτυα» [112], και *β)* τα ενημερωτικά Διαδικτυακά σεμινάρια της Δράσης Ενημέρωσης «*Saferinternet.gr»* του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου που υπάρχουν διαθέσιμα προς παρακολούθηση από τον κάθε ενδιαφερόμενο με μεγάλο εύρος θεματολογίου, όπως «Ασφαλείς Διαδικτυακές συναλλαγές», «Βασικές συμβουλές για την online ασφάλεια», «Υπερβολική χρήση του Διαδικτύου», κ.ά. [113].

3.1.2.2 Συνέδρια – Σεμινάρια – Ημερίδες

Τα τελευταία τρία χρόνια η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διοργανώνει Συνέδρια Ασφαλούς Πλοήγησης στο Διαδίκτυο κατά τη διάρκεια των οποίων εισηγούνται διακεκριμένοι επιστήμονες και καταξιωμένοι ειδικοί από την Ελλάδα και το εξωτερικό. Η πρόσβαση είναι ελεύθερη για το κοινό και πραγματοποιούνται σε κεντρικά σημεία της Αθήνας και της Θεσσαλονίκης προς διευκόλυνση των συμμετεχόντων. Ως εκ τούτου και δεδομένης της επίκαιρης και ενδιαφέρουσας

θεματολογίας η προσέλευση του κόσμου είναι συνήθως μεγαλύτερη των προσδοκιών των διοργανωτών [114] [115]. Συνέδρια με τον ίδιο σκοπό διοργανώνονται και από άλλους Φορείς όπως για παράδειγμα από το Διεθνές Πανεπιστήμιο της Ελλάδος (Νοέμβριος 2013) [116].

Αντίστοιχα, διάφορες Αρχές και Φορείς πραγματοποιούν σεμινάρια επιμορφωτικού χαρακτήρα με σκοπό επίσης την Ασφαλή πλοήγηση και χρήση του Διαδικτύου. Ενδεικτικά αναφέρονται: *α)* το επιμορφωτικό σεμινάριο μαθητών Γυμνασίου που πραγματοποίησε τον Μάρτιο του 2014 το Υπουργείο Μεταφορών και Επικοινωνών σχετικά με την οδική ασφάλεια, τις συμπεριφορές εξάρτησης στο Διαδίκτυο, την ασφαλή πλοήγηση στο Διαδίκτυο και την ασφαλή χρήση ασύρματων συσκευών [117] και *β)* το σεμινάριο για την ασφαλή πλοήγηση και εξάρτηση των εφήβων από το Διαδίκτυο που πραγματοποιήθηκε στον Βόλο με μέριμνα του προγράμματος «ΣΤΡΟΦΗ» του Κέντρου Θεραπείας Εξαρτημένων Ατόμων (ΚΕ.Θ.Ε.Α. ΣΤΡΟΦΗ) με θεματολόγιο που αφορούσε στη βελτίωση των γνώσεων των γονέων και εκπαιδευτικών προκειμένου κατανοήσουν τη συμπεριφορά των εφήβων σε σχέση με το Διαδίκτυο και την ασφαλή πλοήγηση σε αυτό [118] [119].

Την ευαισθητοποίηση της ελληνικής κοινωνίας αναφορικά με την ασφαλή πλοήγηση στο Διαδίκτυο διαπιστώνει κανείς λαμβάνοντας υπόψη και τον αριθμό των ημερίδων που έχουν πραγματοποιηθεί σχετικά με το εν λόγω θέμα σε συνδυασμό με τη διαφορετικότητα των φορέων υλοποίησης τους. Ενδεικτικά, ημερίδες Ασφαλούς Πλοήγησης στο Διαδίκτυο έχουν πραγματοποιηθεί από το Δήμο Κορωπίου [120], την Ιερά Μητρόπολη Αλεξανδρουπόλεως [121] και το Πρότυπο Κέντρο Ξένων Γλωσσών της πόλης των Τρικάλων [122].

3.1.2.3 Τηλεοπτικές εκπομπές – Ντοκιμαντέρ – Τηλεοπτικά σποτ

Τα Μέσα Μαζικής Ενημέρωσης (Μ.Μ.Ε.) όπως είναι ευρέως αποδεκτό κατακλύζουν την καθημερινότητά μας, αποτελώντας τη βασική πηγή εύκολης και άμεσης ενημέρωσης και ψυχαγωγίας του μέσου πολίτη, γονέα και μαθητή. Είναι φυσικό, λοιπόν, τα μηνύματα που προωθούνται μέσω των Μ.Μ.Ε., και κυρίως της τηλεόρασης, να εντυπώνονται ευκολότερα στη συνείδηση των ανθρώπων.

Ως εκ τούτου, ένα σημαντικό μέσο ενημέρωσης για τα οφέλη και τους κινδύνους του Διαδικτύου αποτελούν οι τηλεοπτικές εκπομπές, τα ντοκιμαντέρ και τα τηλεοπτικά σποτ τα οποία όλο και πιο συχνά πλέον παρουσιάζονται στα Μ.Μ.Ε..

Ενδεικτικά αναφέρονται *α)* το ντοκιμαντέρ με τίτλο «Εθισμός στο Διαδίκτυο» που μεταδόθηκε από το τηλεοπτικό σταθμό της ΝΕΡΙΤ τον Ιανουάριο του 2014 [123] και *β)* «Οι κίνδυνοι στο Ίντερνετ» που αφορά σε ρεπορτάζ από την Ελλάδα και τον κόσμο στην εκπομπή «Οι νέοι φάκελοι» του τηλεοπτικού σταθμού ΣΚΑΪ [124].

Παράλληλα, μεταδίδονται διάφορα τηλεοπτικά σποτ προωθώντας μηνύματα για την ορθή και ασφαλή χρήση του Διαδικτύου. Ενδεικτικά μνημονεύονται τα τηλεοπτικά σποτ *α)* της Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας που αφορά στον Διαδικτυακό εκφοβισμό και προτρέπει τη συμμετοχή του κοινού στις ημερίδες ενημέρωσης που διοργανώνει [125] και *β)* της Μονάδας Εφηβικής Υγείας του Πανεπιστημίου Αθηνών και του Υπουργείου Υγείας που αφορά στην ασφάλεια των εφήβων στο Διαδίκτυο [126].

3.1.2.4 Κοινωνικό Σχολείο [127]

Το Κοινωνικό Σχολείο, το οποίο λειτουργεί υπό την αιγίδα των Υπουργείων Παιδείας και Θρησκευμάτων, Υγείας, Πολιτισμού και Αθλητισμού, έχει ως στόχο να προσφέρει εμπειρίες, γνώσεις και δεξιότητες που είναι απαραίτητες για τους μαθητές και τις μαθήτριες της Χώρας για να εξελιχθούν σε υγιείς και ενεργούς πολίτες μέσα από διάφορες δράσεις και με την ενεργό συμμετοχή μαθητών, εκπαιδευτικών και γονέων.

Κύρια δομή υλοποίησης του Κοινωνικού Σχολείου είναι οι «Σχολές Γονέων» που λειτουργούν στα σχολεία κάθε Νομού και σε συνεργασία με τους λοιπούς εμπλεκόμενους Φορείς απευθύνονται στο σύνολο των γονέων με σκοπό τη στήριξή τους και την προσφορά γνώσεων και ευκαιριών για προβληματισμό με την παρουσία ειδικών επιστημόνων από διάφορους Φορείς ανά άξονα θεματικής ενότητας.

Στους άξονες αυτούς εμπεριέχεται και η θεματική ενότητα του «Διαδικτύου» με ανάπτυξη διαφόρων ζητημάτων, δίδοντας παράλληλα τη δυνατότητα μέσα και από βιωματικές δράσεις εμπεριστατωμένης ενημέρωσης και θωράκισης των γονέων και μαθητών απέναντι στους κινδύνους του Διαδικτύου, να συνειδητοποιήσουν πως αυτοί οι κίνδυνοι συνυπάρχουν με τα απεριόριστα οφέλη του Διαδικτύου. Με τον τρόπο αυτό εξασκούνται στην ορθή και ασφαλή χρήση του Διαδικτύου.

3.2 Πόροι Αντιμετώπισης των Κινδύνων του Διαδικτύου

Οι πόροι αντιμετώπισης των κινδύνων του Διαδικτύου είναι οι Αρχές, οι Φορείς, οι Οργανώσεις και οι Οργανισμοί, τόσο με κρατική όσο και με ιδιωτική πρωτοβουλία, οι οποίοι παρέχουν τις διάφορες μεθόδους αντιμετώπισης των κινδύνων του Διαδικτύου. Η δράση των πόρων αυτών έγκειται κυρίως στην πρόληψη, λειτουργώντας κατά περίπτωση και κατασταλτικά εφόσον απαιτηθεί.

Μπορούν να διαχωριστούν ανάλογα με το κατά πόσο η δράσεις του πόρου λειτουργούν μόνο σε Διαδικτυακό επίπεδο ή εντοπίζονται και στον πραγματικό κόσμο. Κατά συνέπεια οι πόροι διακρίνονται σε δικτυακούς και μη-δικτυακούς.

Στους δικτυακούς πόρους συμπεριλαμβάνονται το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, ο δικτυακός τόπος Ασφάλεια στο Διαδίκτυο του Υπουργείου Παιδείας και Πολιτισμού Κύπρου σε συνεργασία με το Παιδαγωγικό Ινστιτούτο Κύπρου, ο δικτυακός τόπος Ασφάλεια στο σπίτι της Microsoft, ο Ενημερωτικός Κόμβος του Πανελλήνιου Σχολικού Δικτύου, κ.ά..

Οι μη-δικτυακοί πόροι περιλαμβάνουν την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, την Ελληνική Εταιρία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, τη Μονάδα εφηβικής Υγείας του Νοσοκομείου Παίδων «Π. & Α. Κυριακού», το Εξειδικευμένο Ψυχιατρικό Ιατρείο για την Αντιμετώπιση του Εθισμού Παιδιών και Εφήβων στο Διαδίκτυο και τους Η/Υ του Ιπποκράτειου Νοσοκομείου Θεσσαλονίκης, τους Συμβουλευτικούς Σταθμούς Νέων που λειτουργούν στις Πρωτοβάθμιες και Δευτεροβάθμιες Διευθύνσεις Εκπαίδευσης του Υπουργείου Παιδείας και Θρησκευμάτων, κ.ά..

Στο παρόν υποκεφάλαιο θα αναπτυχθούν οι κυριότεροι από αυτούς, όπως επιλέχθηκαν σύμφωνα με την κρίση του συγγραφέα.

3.2.1 Δικτυακοί Πόροι Αντιμετώπισης

3.2.1.1 Ελληνικό Κέντρο Ασφαλούς Διαδικτύου [128]

Το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου αποτελεί τον εθνικό εκπρόσωπο του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης *«Insafe»* [129] που αριθμεί τριάντα ένα μέλη από όλα τα κράτη της Ευρωπαϊκής Ένωσης πλέον της Ισλανδίας, της Νορβηγίας, της Σερβίας και της Ρωσίας. Μεταξύ των μελών ανταλλάσσονται απόψεις, εμπειρίες, βέλτιστες πρακτικές και πληροφοριακό υλικό.

Η λειτουργία του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου ξεκίνησε το έτος 2009 από τη συνένωση της υπάρχουσας Δράσης Ενημέρωσης «Saferinternet.gr» και της υπάρχουσας Γραμμής Καταγγελιών «Safeline.gr», με τη νέα Γραμμή Βοήθειας «ΥποΣΤΗΡΙΖΩ».

3.2.1.1.1 Δράση Ενημέρωσης «Saferinternet.gr» [130]

Η Δράση Ενημέρωσης «Saferinternet.gr» και η εκστρατεία ενημέρωσης και επαγρύπνησης διεξάγεται στη Χώρα μας από το έτος 2004 στο πλαίσιο του προγράμματος *Safer Internet*.

Οι κύριοι στόχοι της Δράσης Ενημέρωσης είναι:

- 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 μας 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.

Προκειμένου επιτευχθούν οι στόχοι αυτοί, η «Saferinternet.gr», η οποία υλοποιείται από την αστική μη κερδοσκοπική εταιρία *Safer Internet Hellas*, πραγματοποιεί μια σειρά δράσεων στις οποίες συγκαταλέγονται τα σεμινάρια προς εκπαιδευτικούς, οι ενημερωτικές εκδηλώσεις για το ευρύ κοινό, η δημιουργία ενημερωτικού υλικού τόσο Διαδικτυακού όσο και εντύπου, η προώθηση θεμάτων στα Μ.Μ.Ε. που σχετίζονται με την ασφάλεια στο Διαδίκτυο και οι τηλεοπτικές και ραδιοφωνικές καμπάνιες. Παράλληλα, προς επίτευξη των στόχων της, συνεργάζεται με εκπροσώπους του κράτους, της βιομηχανίας των Νέων Τεχνολογιών και με Μη-Κυβερνητικές Οργανώσεις στην Ελλάδα και το εξωτερικό.

3.2.1.1.2 Γραμμή Καταγγελιών «SafeLine» [131] [132]

Η «SafeLine.gr» αποτελεί την Ελληνική Ανοιχτή Γραμμή Καταγγελιών για το παράνομο περιεχόμενο στο Διαδίκτυο. Ιδρύθηκε το έτος 2003 από την Ελληνική Εταιρία Τηλεπικοινωνιών και Τηλεματικών Εφαρμογών «FORTHNET», το Ίδρυμα Μείζονος Ελληνισμού (ΙΜΕ), το Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Διαδικτύου (SAFENET), το Ίδρυμα Τεχνολογίας και Έρευνας - Ινστιτούτο Πληροφορικής (ΙΤΕ-ΙΠ) ενώ πλέον υλοποιείται από τα δύο τελευταία. Συνεργάζεται με το Πανελλήνιο Σχολικό Δίκτυο, τους Φορείς Παροχής Υπηρεσιών Διαδικτύου (Internet Service Providers – ISPs), το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ) και την Ελληνική Αστυνομία.

Κεντρικός στόχος της Γραμμής Καταγγελιών «SafeLine.gr» είναι η προάσπιση του δικαιώματος της ασφαλούς πλοήγησης του παιδιού στο Διαδίκτυο, ενώ οι καταγγελίες που δέχεται αφορούν σε εικόνες και βίντεο κακοποίησης ανηλίκων σε οποιοδήποτε σημείο του κόσμου, σε ρατσιστικό, βίαιο και ξενοφοβικό υλικό, στη Διαδικτυακή παρενόχληση και γενικότερα σε οτιδήποτε κείται ενάντια στην ελληνική νομοθεσία.

Τέλος, η «SafeLine.gr» από το έτος 2005 είναι μέλος του Διεθνούς Συνδέσμου Ανοικτών Γραμμών Διαδικτύου «INHOPE», ο οποίος είναι ένα ενεργό και συνεργατικό δίκτυο πενήντα ενός Γραμμών Καταγγελιών σε σαράντα πέντε Χώρες παγκοσμίως για την αντιμετώπιση του παράνομου Διαδικτυακού περιεχομένου και της παιδικής σεξουαλικής κακοποίησης μέσω Διαδικτύου [133].

3.2.1.1.3 Γραμμή Βοηθείας «ΥποΣΤΗΡΙΖΩ» [134] [135] [136]

Η Γραμμή Βοηθείας «ΥποΣΤΗΡΙΖΩ» λειτουργεί στη Μονάδα Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών που στεγάζεται στο Παράρτημα του Νοσοκομείου Παίδων «Π. &. Α. Κυριακού».

Στελεχώνεται από εξειδικευμένους παιδοψυχολόγους σε θέματα χρήσης και κατάχρησης στο Διαδίκτυο από άτομα νεαρής ηλικίας, οι οποίοι απαντούν στον τηλεφωνικό αριθμό *800 11 800 15* και στη διεύθυνση ηλεκτρονικού ταχυδρομείου *help@saferinternet.gr*.

Εικόνα 13: Λογότυπο Μονάδας Εφηβικής Υγείας «ΥποΣΤΗΡΙΖΩ»

Η επικοινωνία γίνεται χωρίς οικονομική επιβάρυνση από πλευράς των ενδιαφερομένων, δηλαδή των παιδιών, των εφήβων και των οικογενειών τους που χρήζουν υποστήριξης και συμβουλευτικής σε θέματα αναφορικά με τη χρήση του Διαδικτύου, του κινητού τηλεφώνου και των ηλεκτρονικών παιχνιδιών.

3.2.1.2 Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου «sch.gr» [137] [138]

Ο Ενημερωτικός Κόμβος του Πανελλήνιου Σχολικού Δικτύου «sch.gr» έχει δημιουργήσει την υπηρεσία *Ασφάλεια στο Διαδίκτυο*, βασισμένη στο προηγούμενο ομώνυμο έργο του ιστολογίου του [139], η οποία απευθύνεται κυρίως σε σχολεία, διοικητικές υπηρεσίες, εκπαιδευτικούς, μαθητές πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, το προσωπικό του Υπουργείου Παιδείας και Θρησκευμάτων, αλλά και σε κάθε ενδιαφερόμενο.

Εικόνα 14: Ενημερωτικός Κόμβος «sch.gr» – υπηρεσία «Ασφάλεια στο Διαδίκτυο»

Σκοπός της υπηρεσίας αυτής είναι η αξιόπιστη και επίκαιρη ενημέρωση σε θέματα ασφαλούς πρόσβασης των μαθητών στο Διαδίκτυο, η προβολή καλών πρακτικών, η παροχή οδηγιών και συμβουλών, η ευαισθητοποίηση των εκπαιδευτικών, των μαθητών, των γονέων και κηδεμόνων αυτών, σε θέματα της ασφαλούς χρήσης του Διαδικτύου.

Παρέχοντας στοχευμένη και συγκεντρωμένη πληροφόρηση στους εμπλεκόμενους με την εκπαίδευση και τη διαπαιδαγώγηση των νέων, αλλά και στους ίδιους τους νέους, με πληθώρα θεματικών ενοτήτων, υλικού και συνδέσμων σε άλλους Φορείς, αποτελεί αναμφίβολα ένα σημαντικό χώρο ενημέρωσης και πρόληψης κατά των κινδύνων του Διαδικτύου τόσο για τους μαθητές όσο και για τους εκπαιδευτικούς, για τους οποίους ο Κόμβος του Πανελλήνιου Σχολικού Δικτύου [140] γενικότερα είναι ένα σημαντικό εργαλείο στη μάθηση και την εκπαίδευση στα Σχολεία.

3.2.2 Μη-Δικτυακοί Πόροι Αντιμετώπισης

3.2.2.1 Ελληνική Εταιρία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο [141] [142]

Εικόνα 15: Λογότυπο Ελληνικής Εταιρείας Μελέτης Διαταραχής Εθισμού Διαδίκτυο

Η Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο ιδρύθηκε το έτος 2008 με επιστημονικό και κοινωφελή σκοπό. Δραστηριοποιείται σε ένα πεδίο δράσης που βασίζεται στους παρακάτω άξονες από τους οποίους προκύπτει πως αποτελεί βασικό πόρο αντιμετώπισης των κινδύνων του Διαδικτύου.

Πιο συγκεκριμένα, οι άξονες αυτοί συνοψίζονται στους εξής:

- αναγνώριση, μελέτη και αντιμετώπιση της διαταραχής του Εθισμού στο Διαδίκτυο,
- πρόληψη των δυσμενών συνεπειών της ετεροχρονισμένης διάγνωσης της εν λόγω διαταραχής,
- ευαισθητοποίηση της κοινωνίας, της επιστημονικής κοινότητας και της Πολιτείας αναφορικά με της επιπτώσεις της διαταραχής αυτής,
- ευαισθητοποίηση και εκπαίδευση των ειδικών της Ψυχικής υγείας, αλλά και άλλων εμπλεκομένων ιατρικών ειδικοτήτων,
- εφαρμογή προγραμμάτων στήριξης των ατόμων που είναι εθισμένα στο Διαδίκτυο και των οικογενειών τους, καθώς και
- διαρκή εκπαίδευση διεπιστημονικών ομάδων που εργάζονται πάνω στη Διαταραχή του Εθισμού στο Διαδίκτυο.

Αξίζει να σημειωθεί πως η Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο είναι επίσημα διασυνδεδεμένη με τον μη κερδοσκοπικό Διεθνή Σύνδεσμο για τη Διαδικτυακή Ψυχολογία, την Εξάσκηση και την Επανένταξη (International Association of CyberPsychology, Training, and Rehabilitation - iACToR) [143].

3.2.2.2 Μονάδα Εφηβικής Υγείας του Πανεπιστημιακού Νοσοκομείου Παίδων «Π. & Α. Κυριακού» [144]

Μια πρότυπη δομή, το Τμήμα Ασφαλούς Διαδικτύου της Μονάδας Εφηβικής Ηλικίας (Μ.Ε.Υ.), λειτουργεί από τη Β' Παιδιατρική Κλινική του Πανεπιστημίου Παίδων «Π. & Α. Κυριακού» για εφήβους ηλικίας 11 έως 18 ετών και τις οικογένειες τους προσφέροντας υπηρεσίες από εξειδικευμένο προσωπικό σε θέματα που σχετίζονται με πληθώρα προβλημάτων, όπως τα οργανικά-χρόνια νοσήματα, θέματα ανάπτυξης, μαθησιακά, ψυχοκοινωνικά, κ.ά., ενώ τα τελευταία επτά χρόνια έχουν συμπεριληφθεί και οι δυσκολίες που αντιμετωπίζουν οι νέοι σχετικά με την ορθή χρήση του Διαδικτύου.

Αξίζει να σημειωθεί πως η Μ.Ε.Υ. αποτελεί την πρώτη δομή στην Ελλάδα που έθεσε στην επιστημονική κοινότητα το θέμα της υπερβολικής χρήσης του Διαδικτύου. Επ' αυτού, η Μ.Ε.Υ. εργάζεται κλινικά, ερευνητικά αλλά και εκπαιδευτικά σχετικά με την Διαδικτυακή Ασφάλεια προσφέροντας φροντίδα και εξατομικευμένη προσέγγιση-αντιμετώπιση στα προβλήματα των εφήβων που απευθύνονται σε αυτή. Τα συνηθέστερα προβλήματα αφορούν το ακατάλληλο περιεχόμενο, τον εκφοβισμό, την κακοποίηση και τον εθισμό. Σημαντικό σημείο της προσφοράς της Μ.Ε.Υ. αποτελεί το γεγονός πως λειτουργεί πρόγραμμα με το οποίο παρέχονται στους νέους συμβουλευτική και προτάσεις δημιουργικής χρήσης του Διαδικτύου παράλληλα με την εκπαίδευση αποφυγής των κινδύνων του Διαδικτύου.

3.2.2.3 Ελληνική Αστυνομία: Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος [145]

Σημαντικό αρωγό στην πρόληψη και καταστολή (διερεύνηση, εξιχνίαση και δίωξη) εγκλημάτων που τελούνται μέσω Διαδικτύου αποτελεί η Ελληνική Αστυνομία που ευαισθητοποιημένη αναφορικά με το εν λόγω θέμα έχει συστήσει την Υπηρεσία

Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΠ.Ο.Α.Δ.Η.Ε.), μία ειδική αυτοτελή Κεντρική Υπηρεσία υπαγόμενη απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας και εποπτευόμενη σε προανακριτικό επίπεδο από τον Εισαγγελέα του Οργανωμένου Εγκλήματος.

Η Υπηρεσία αυτή διαρθρώνεται στην Υποδιεύθυνση Οικονομικής Αστυνομίας και στην Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, με την τελευταία να έχει ως αποστολή την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών που διαπράττονται με τη χρήση του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Προκειμένου λειτουργήσει αποτελεσματικότερα, η Δίωξη Ηλεκτρονικού Εγκλήματος διαρθρώνεται επιπλέον σε τέσσερα Τμήματα, τα οποία δρουν εξειδικευμένα σε καθένα από τους ακόλουθους τομείς:

- Εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή που διαπράττονται με τη χρήση των μέσων αυτών *(Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων)*
- Εγκλήματα που διαπράττονται σε βάρος ανήλικων ατόμων μέσω του Διαδικτύου ή άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης *(Τμήμα Προστασίας Ανηλίκων)*
- Παράνομη διείσδυση σε υπολογιστικά συστήματα, κλοπή, καταστροφή ή παράνομη διακίνηση λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων (*Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων)*
- Πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών *(Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών)*

Ανάμεσα στις δράσεις της Δίωξης Ηλεκτρονικού Εγκλήματος συγκαταλέγεται η λειτουργία 24ωρης τηλεφωνικής γραμμής καταγγελιών *11012***,** η επικοινωνία μέσω των ηλεκτρονικών διευθύνσεων *ccu@cybercrimeunit.gov.gr*, *cybercrimeunit@hellenicpolice.gr*, καθώς και η πραγματοποίηση σειράς ημερίδων, σεμιναρίων και τηλεδιασκέψεων, προκειμένου ενημερωθούν οι πολίτες ολόκληρης της Χώρας σχετικά με τις νέες τεχνολογίες και το Διαδίκτυο, αλλά και τους κινδύνους που ελλοχεύουν κατά τη χρήση τους.

Εικόνα 16: Δίωξη Ηλεκτρονικού Εγκλήματος – πρωτοβουλία «Cyberkids»

Εξαιρετικά αξιόλογη κρίνεται επίσης η δημιουργία του Διαδικτυακού διαδραστικού ιστότοπου *«Cyberkid»*, ο οποίος αποτελεί μια πρωτοβουλία του Υπουργείου Προστασίας του Πολίτη και του Αρχηγείου της Ελληνικής Αστυνομίας και υλοποιείται

από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με τη χορηγία γνωστής εταιρείας παροχής υπηρεσιών Διαδικτύου, κινητής και σταθερής τηλεφωνίας .

Βασικός στόχος της πρωτοβουλίας αυτής είναι η ασφαλής εξοικείωση του κοινού με τις νέες τεχνολογίες και ειδικότερα με το Διαδίκτυο, αποτελώντας παράλληλα πηγή ενημέρωσης και ευαισθητοποίησης των παιδιών ηλικίας έως και 12 ετών, καθώς και των γονέων τους, σε θέματα σχετικά με την ασφαλή πλοήγηση στο Διαδίκτυο. Θετικό, επίσης, είναι το γεγονός πως η ενημέρωση για τους πιθανούς κινδύνους του Διαδικτύου συνδυάζεται με την προβολή των θετικών πλευρών του, όπως είναι η ανεύρεση χρήσιμων πληροφοριών και η ψυχαγωγία [146].

4. ΟΔΗΓΙΕΣ ΑΣΦΑΛΟΥΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στο σημείο αυτό της παρούσας εργασίας και στα πλαίσια ανάλυσης των κινδύνων του Διαδικτύου και των μεθόδων και πόρων για την αντιμετώπισής τους, κρίνεται σκόπιμο να αναφερθούν οι βασικοί τρόποι Ασφαλούς Χρήσης του Διαδικτύου, οι οποίοι προσανατολίζονται ιδίως στην προστασία των νεαρών ατόμων που λόγω ηλικίας αντιμετωπίζουν περισσότερους κινδύνους με τις συνέπειες αυτών να είναι σοβαρότερες.

Με γνώμονα λοιπόν αυτό, στο παρόν κεφάλαιο καταγράφονται βασικές οδηγίες Ασφαλούς χρήσης του Διαδικτύου από άτομα νεαρής ηλικίας, τους γονείς τους και τους εκπαιδευτικούς, όπως αυτές αποτυπώνονται από τους αρμόδιους φορείς.

4.1 Ασφαλής χρήση του Διαδικτύου από Νεαρά Άτομα: Οδηγίες για Γονείς και Κηδεμόνες

Η Ελληνική Αστυνομία προτείνει στους γονείς να υιοθετήσουν συγκεκριμένες συμπεριφορές προκειμένου συμβάλλουν από την πλευρά τους στην ασφαλέστερη χρήση του Διαδικτύου από τα παιδιά τους. Αναλυτικότερα, προτείνεται [147]:

- η τοποθέτηση του Η/Υ σε χώρους του σπιτιού στους οποίους συγκεντρώνεται όλη η οικογένεια, όπως είναι το σαλόνι, και να αποφεύγεται η τοποθέτηση του στα υπνοδωμάτια όπου καθένας μπορεί να απομονώνεται. Με τον τρόπο αυτό οι γονείς επιβλέπουν με διακριτικότητα το παιδί τους χωρίς το ίδιο να αισθάνεται πως του ασκείται αυστηρός έλεγχος.
- συζήτηση μεταξύ γονέων και παιδιών σχετικά με θέματα ασφάλειας που αφορούν στην πλοήγηση στο Διαδίκτυο. Παραδείγματος χάρη, ενημέρωση των νέων για την επικινδυνότητα της συνομιλίας με αγνώστους στις σελίδες κοινωνικής δικτύωσης και της επίσκεψης σε ιστοσελίδες με βλαβερό περιεχόμενο.
- να γίνει η πλοήγηση στο Διαδίκτυο μια οικογενειακή δραστηριότητα, χρησιμοποιώντας τον Η/Υ μαζί με τα παιδιά. Η κοινή δραστηριότητα μπορεί να επιφέρει πολλαπλά οφέλη, κυριότερο από τα οποία είναι η δυνατότητα να διδάξουν οι γονείς τα παιδιά τους να προστατεύουν τα προσωπικά τους δεδομένα όπως το επίθετο, το όνομα, την ηλικία τους, τη διεύθυνση της κατοικίας και του σχολείου, τον αριθμό τηλεφώνου, το οικογενειακό εισόδημα, τα ονόματα φίλων, κ.ά..
- η αποτροπή των παιδιών από κατ' ιδίαν συνάντηση με άτομα που γνώρισαν μέσω του Διαδικτύου, όχι με τρόπο απαγορευτικό, αλλά παρέχοντας τους την απαραίτητη παιδεία ώστε να είναι σε θέση να αρνηθούν αναγνωρίζοντας τα ίδια την επικινδυνότητα μιας τέτοιας συνάντησης.
- ο έλεγχος του περιεχομένου του οπτικοακουστικού υλικού που έχουν στην κατοχή τους τα παιδιά είτε αυτό προέρχεται από αγορά είτε από ανταλλαγή με φίλους.
- η χρήση ειδικών λογισμικών πακέτων, των «φίλτρων», τα οποία επιτυγχάνουν την παρεμπόδιση πρόσβασης σε ανεπιθύμητες ιστοσελίδες.

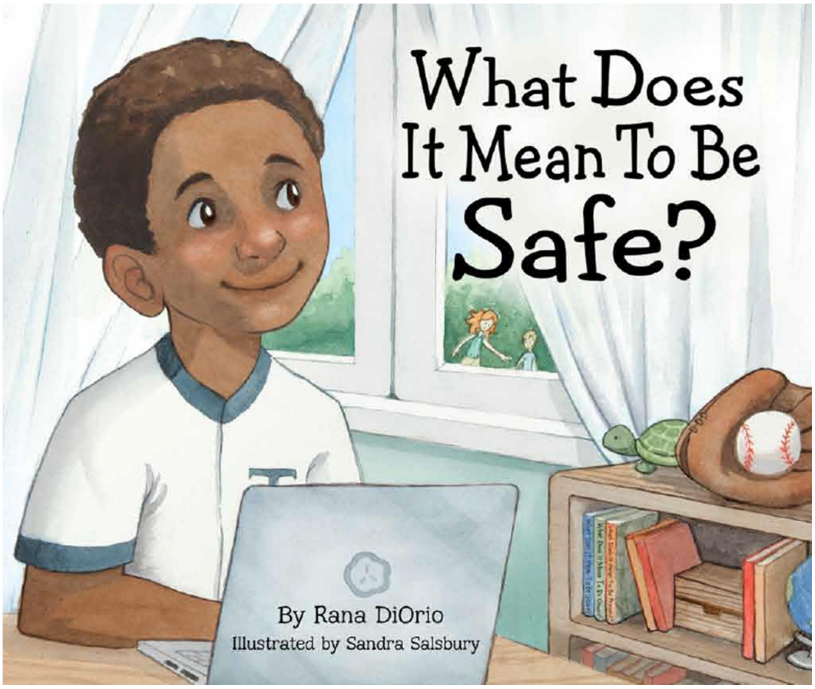
Εικόνα 17: Αφίσα «Keep your kids SAFE on the Internet»

Σύμφωνα με τη Δράση Ενημέρωσης «*Saferinternet.gr»* του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου προτείνεται επιπλέον στους γονείς νεαρών ατόμων [148]:

- η εκπαίδευση των παιδιών τους σχετικά με τη σημασία αποφυγής δημοσίευσης φωτογραφιών και βίντεο στο Διαδίκτυο, ιδιαίτερα σε περιπτώσεις που αποτυπώνουν προσωπικές στιγμές, δεδομένου πως δεν είναι δυνατό να γνωρίζουν ποια άτομα μπορούν να έχουν πρόσβαση σε αυτά.
- η διδασκαλία των παιδιών από τους γονείς προκειμένου να χρησιμοποιούν δύσκολους κωδικούς πρόσβασης στο Διαδίκτυο, αποτελούμενους από τουλάχιστον οκτώ χαρακτήρες που περιλαμβάνουν γράμματα, αριθμούς και σύμβολα. Τους κωδικούς αυτούς δεν θα πρέπει να τους γνωστοποιούν σε κανένα και προτείνεται να αποφεύγουν τη χρήση τους από Η/Υ εκτός του δικού τους.
- η προώθηση μέσα στην οικογένεια μιας ατμόσφαιρας που δεν ανέχεται την παρενόχληση και η διδασκαλία των παιδιών πως η ανωνυμία στο Διαδίκτυο δεν θα πρέπει να νοείται ως ευκαιρία για ανεύθυνη συμπεριφορά. Απεναντίας, με δεδομένο πως ούτως ή άλλως ο κάθε χρήστης αφήνει τα ηλεκτρονικά του ίχνη στο Διαδίκτυο, χρειάζεται υιοθέτηση ευγενικής συμπεριφοράς που χαρακτηρίζεται από ήθος, σεβασμό των δικαιωμάτων και υλοποίηση των υποχρεώσεων μας, κατ' αντιστοιχία με τον πραγματικό κόσμο.

- η αφιέρωση χρόνου από πλευράς του γονέα προκειμένου παίξει μαζί με το κάθε παιδί του τα ηλεκτρονικά του παιχνίδια. Με τον τρόπο αυτό είναι ευκολότερος ο εντοπισμός σημαδιών υπερβολικής ενασχόλησης ή «εξάρτησης». Επιπλέον, εκπαιδεύεται το παιδί ώστε να αναπτύξει την απαραίτητη κριτική ικανότητα που θα τον κάνει να ξεχωρίζει την πληροφορία από το διαφημιστικό περιεχόμενο, κάτι που είναι ιδιαίτερα σημαντικό καθώς τα άτομα νεαρής ηλικίας αποτελούν εύκολο στόχο από τις διαφημιστικές εταιρίες.
- Η εγκατάσταση στον Η/Υ ενός προγράμματος προστασίας από ιούς «antivirus» και ενός τείχους προστασίας «firewall», καθώς και η ενεργοποίηση του γονικού ελέγχου που παρέχεται από το λειτουργικό σύστημα του Η/Υ και το ηλεκτρονικό ταχυδρομείο.

4.2 Ασφαλής χρήση του Διαδικτύου: Οδηγίες για Νεαρά Άτομα



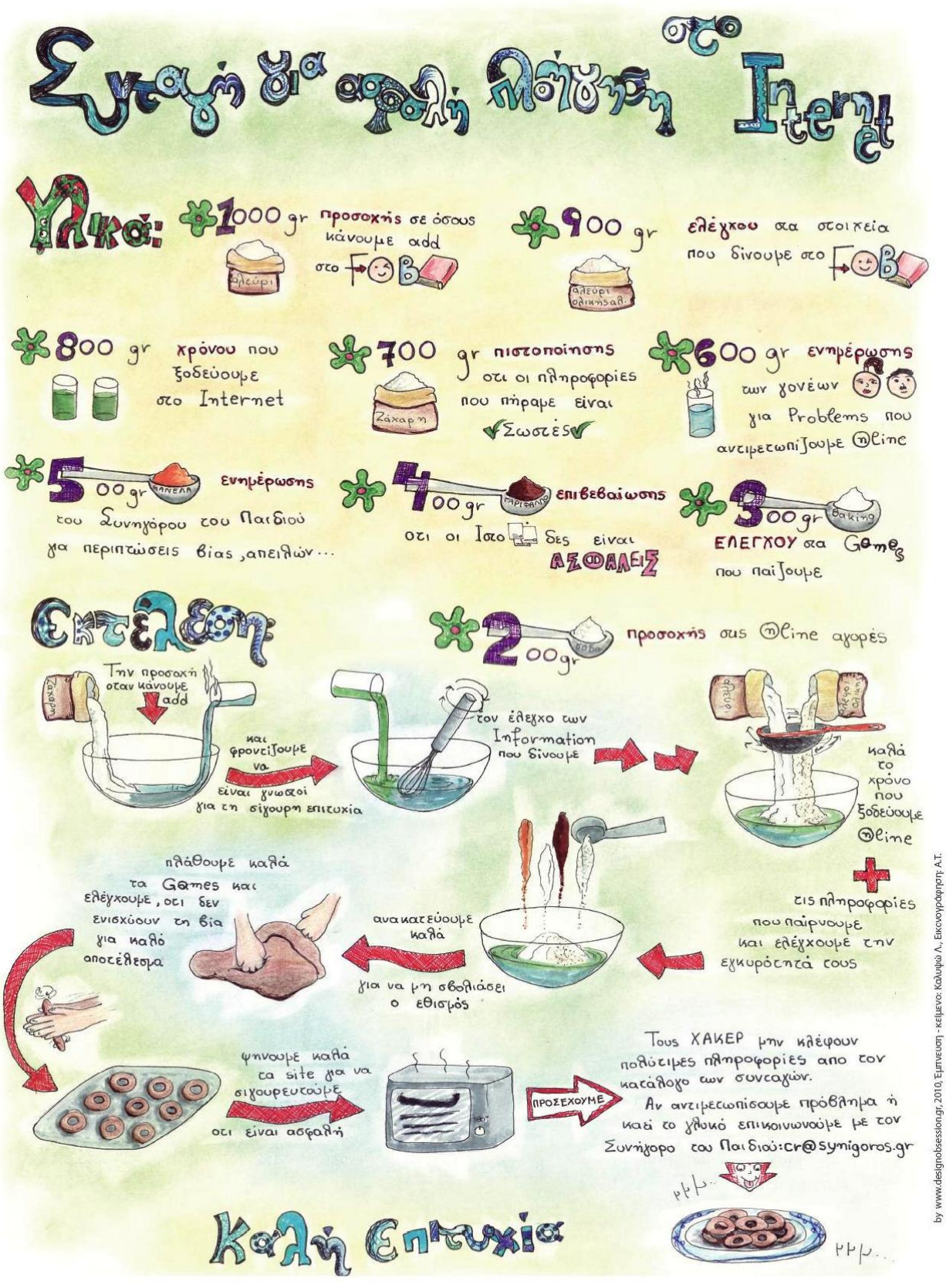
Εικόνα 18: Τι σημαίνει να είμαι Ασφαλής;

Το Υπουργείο Παιδείας και Θρησκευμάτων σε συνεργασία με τη Μονάδα Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών – Μέλους του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, συνέταξε Συνοπτικό Οδηγό για τους Μαθητές με σκοπό να τους υποστηρίξει στην αναγνώριση πιθανών Διαδικτυακών κινδύνων, στην προστασία της ιδιωτικής τους ζωής και την αντιμετώπιση δυσμενών καταστάσεων με τις οποίες ενδεχομένως να βρεθούν αντιμέτωποι στο ψηφιακό κόσμο [149].

Ακολούθως παρουσιάζονται συνοπτικά οι κυριότερες οδηγίες:

- Δεν αποκαλύπτω ποτέ προσωπικές λεπτομέρειες στο Διαδίκτυο, γιατί εκείνη τη στιγμή παύει να είναι προσωπική και γίνεται δημοσίως προσβάσιμη παντού στον κόσμο.
- Δεν αποκαλύπτω σε κανέναν τον κωδικό πρόσβασης του λογαριασμού μου στο Διαδίκτυο, καθώς μπορεί να τον χρησιμοποιήσει κάποιος εν αγνοία μου και να προσποιείται κακόβουλα πως είμαι εγώ.
- Ενημερώνω τους γονείς μου ή τους δασκάλους μου σχετικά με καθετί το οποίο με κάνει να αισθάνομαι άβολα, με τρομάζει ή προσβάλλει την ηθική μου. Μπορώ, επίσης, να καλέσω ανώνυμα και χωρίς χρέωση στο Ελληνικό Κέντρο Ασφαλούς Διαδικτύου στον αριθμό 800 11 800 15, προκειμένου ζητήσω βοήθεια.
- Ποτέ δεν συναντώ στον πραγματικό κόσμο κάποιον που γνώρισα μέσω Διαδικτύου και σε περίπτωση που μου ζητήσει να κρατήσω τη φιλία μας μυστική, διαπιστώνω πως πρόκειται για ύποπτη συμπεριφορά και την αναφέρω άμεσα στους γονείς ή τους δασκάλους μου.
- Σβήνω αμέσως την ηλεκτρονική αλληλογραφία που έχω λάβει από άγνωστα άτομα, χωρίς να ανοίξω οποιοδήποτε συνημμένο αρχείο και χωρίς να ενεργοποιήσω τους συνδέσμους του Διαδικτύου που περιέχονται σε αυτά τα μηνύματα.
- Δεν κάνω ποτέ αγορές από το Διαδίκτυο αν δεν είναι δίπλα μου κάποιος από τους γονείς μου.
- Κάνω συχνά διαλείμματα και φροντίζω ο χρόνος που αφιερώνω στην ενασχόληση μου με τον Η/Υ να μη μου στερεί χρόνο από άλλες δραστηριότητες όπως το παιχνίδι με τους φίλους μου, τα χόμπι μου, το διάβασμα και τον ύπνο μου.

Σε αυτό το σημείο κρίνεται σκόπιμη η αναφορά στην πρωτοβουλία της Μη-Κυβερνητικής Οργάνωσης «Συνήγορος του Παιδιού» που μέσω του κλειστού ηλεκτρονικού φόρουμ της Κοινότητας Εφήβων Συμβούλων του Συνηγόρου του Παιδιού δημιούργησε τη Συνταγή Ασφαλούς Πλοήγησης στο Διαδίκτυο η οποία παρουσιάζεται στην εικόνα που ακολουθεί στην επόμενη σελίδα:



ΣΥΝΗΓΟΡΟΣ ΤΟΥ ΠΟΛΙΤΗ
Συνήγορος του Παιδιού
ΟΜΑΔΑ ΕΦΗΒΩΝ ΣΥΜΒΟΥΛΩΝ 2011-2012
www.0-18.gr
τηλ.: 800.11.32000 (δωρεάν γραμμή για παιδιά)
210.7289703, 210.7289605 (Γραμματεία)
Η συνταγή προέκυψε μέσα από συζήτηση στο κλειστό ηλεκτρονικό φόρουμ της Κοινότητας Εφήβων Συμβούλων του Συνηγόρου του Παιδιού.

Εικόνα 19: Αφίσα «Συνταγή για Ασφαλή πλοήγηση στο Internet»

4.3 Ασφαλής χρήση του Διαδικτύου από Νεαρά Άτομα: Οδηγίες για Εκπαιδευτικούς

Ο ρόλος του σχολείου, δια μέσου των εκπαιδευτικών λειτουργών, αναφορικά με την Ασφαλή Χρήση του Διαδικτύου κρίνεται ιδιάζουσας σημασίας, γεγονός που αποτυπώνεται από τα ευρήματα Διαδικτυακής έρευνας που πραγματοποίησε η Δράση Ενημέρωσης «*Saferinternet.gr»* του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου το έτος 2009 σε 679 εκπαιδευτικούς όλων των βαθμίδων από όλη την Ελλάδα σε συνεργασία με το Πανελλήνιο Σχολικό Δίκτυο «*sch.gr»* [150].

Στην εν λόγω έρευνα η συντριπτική πλειοψηφία των εκπαιδευτικών, σε ποσοστό που ανέρχεται στο 99% των ερωτηθέντων, θεωρεί πως η Ασφαλής Χρήση του Διαδικτύου πρέπει να διδάσκεται στο σχολείο, με το 70% να υποστηρίζει πως καταλληλότερη βαθμίδα για να ξεκινήσει η εκπαίδευση είναι η πρωτοβάθμια, δεδομένου πως τότε οι μαθητές αποκτούν Η/Υ.

Σύμφωνα με τις απαντήσεις που συγκεντρώθηκαν, οι εκπαιδευτικοί εστιάζουν την προσοχή τους σε θέματα εκπαίδευσης, όπως:

- Βασικές αρχές σωστής χρήσης του Διαδικτύου
- Προστασία προσωπικής ζωής
- Σωστή διαχείριση της επικοινωνίας μέσω Διαδικτύου
- Αξιοπιστία Διαδικτυακού περιεχομένου
- Αξιοποίηση της θετικής πλευράς του Διαδικτύου

Αξιοσημείωτο είναι το γεγονός πως δόθηκε ιδιαίτερη έμφαση στην ανάπτυξη της κριτικής ικανότητας και σκέψης των μαθητών, στην ανάπτυξη μηχανισμών αυτοπροστασίας, στην κατανόηση των κινδύνων, στη διαφύλαξη των προσωπικών τους δεδομένων, στη σωστή διαχείριση και χρήση των Διαδικτυακών Μορφών Επικοινωνίας και την αξιοπιστία της Διαδικτυακής Πληροφορίας.

Τέλος, τονίσθηκε η ανάγκη ουσιαστικής επιμόρφωσης των εκπαιδευτικών ώστε να καταστούν ικανοί να εκπαιδεύσουν τους μαθητές στην Ασφαλή Χρήση του Διαδικτύου.

Στα πλαίσια αυτά το Υπουργείο Παιδείας και Θρησκευμάτων σε συνεργασία με τη Μονάδα Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών προκειμένου εφοδιάσει κατά το δυνατόν τους εκπαιδευτικούς με χρήσιμες συμβουλές και οδηγίες προς την κατεύθυνση αυτή, συνέταξε την επόμενη χρονιά (2010) *Συνοπτικό Οδηγό προς Εκπαιδευτικούς* [151]. Τα κυριότερα σημεία του οδηγού αυτού καταγράφονται ως ακολούθως:

- Ενθάρρυνση των μαθητών για Χρήση του Διαδικτύου με σκοπό την επικοινωνία, τη μελέτη, τη διασκέδαση, την εύρεση πληροφοριών όντας ενημερωμένοι και σε επαγρύπνιση.
- Χρήση του Διαδικτύου ως εργαλείου γνώσης και εξερεύνησης κατά τη διάρκεια της διδασκαλίας εντός σχολικής τάξης.
- Εύρεση κατάλληλων ιστοχώρων για νέους με επιμορφωτικό περιεχόμενο ανάλογα με το αντικείμενο διδασκαλίας και πλοήγηση σε αυτούς κατά τη διάρκεια της διδασκαλίας.
- Εκπαίδευση των μαθητών ώστε να αποκτήσουν κριτική σκέψη για να εξετάζουν το περιεχόμενο του Διαδικτύου το οποίο θα πρέπει να διασταυρώνεται με άλλες πηγές, όπως οι εγκυκλοπαίδειες. Σημαντική σε αυτό το σημείο είναι η διδασκαλία της στοχευμένης αναζήτησης πληροφοριών στο Διαδίκτυο.

- Εκπαίδευση των μαθητών ώστε να διαχωρίζουν την πληροφορία από τη διαφήμιση, καθώς υπάρχουν ιστοσελίδες κερδοσκοπικών εταιριών που μέσω κρυμμένων διαφημίσεων παρακινούν τους χρήστες στην αγορά αγαθών όπως είναι τα Διαδικτυακά Παιχνίδια.
- Ανάπτυξη διαδραστικής συζήτησης ως μέσον με το οποίο οι μαθητές μπορούν να μάθουν πώς να προστατεύουν τα προσωπικά τους δεδομένα, όπως η διεύθυνση κατοικίας, ο αριθμός τηλεφώνου, κωδικοί πρόσβασης στο Διαδίκτυο, διεύθυνση σχολείου στο οποίο φοιτούν. Μεγάλη προσοχή πρέπει να δοθεί στη σημασία αποφυγής δημοσίευσης προσωπικών πληροφοριών στο Διαδίκτυο, μια διαδικασία ιδιαίτερα προσφιλή στους μεγαλύτερους μαθητές, ιδιαίτερα σε ιστότοπους κοινωνικής δικτύωσης.
- Προσέγγιση της χρήσης των «Greeklish» ως άτυπη μορφή γρήγορης επικοινωνίας με φίλους που σε καμία περίπτωση δεν αντικαθιστά την Ελληνική Γλώσσα την οποία θα πρέπει να γνωρίζουν σωστά.
- Καλλιέργεια διαλόγου σχετικά με τους αγνώστους στο Διαδίκτυο προκειμένου οι μαθητές αντιληφθούν πως οι άνθρωποι δεν είναι πάντα αυτοί που δηλώνουν, κάτι που ισχύει ακόμη και για αυτούς που συνομιλούν και αλληλογραφούν για καιρό, αλλά δεν τους γνωρίζουν στον πραγματικό κόσμο. Ως εκ τούτου, θα πρέπει να προσέχουν κατά τις συνομιλίες τους στο Διαδίκτυο.
- Επικοινωνία με τη γραμμή βοηθείας «*ΥποΣΤΗΡΙΖΩ 800 11 800 15 - help@saferinternet.gr»* του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου σε περίπτωση που εντοπιστούν συμπτώματα όπως:

  1. Εκνευρισμός όταν ο μαθητής δεν βρίσκεται σε ενασχόληση με το Διαδίκτυο,
  2. Χρήση του Διαδικτύου για περισσότερο χρόνο από την αρχική του πρόθεση,
  3. Ξαφνική σχολική αποτυχία,
  4. Κούραση και υπνηλία μέσα στην τάξη,
  5. Μειωμένη φυσική δραστηριότητα,
  6. Διαταραχή στις διαπροσωπικές σχέσεις,
  7. Παραμέληση φίλων ή αγαπημένης ενασχόλησης,
  8. Παραμέληση της προσωπικής υγιεινής,

  καθώς αυτά υποδηλώνουν πως ο μαθητής οδεύει προς τον «εθισμό του Διαδικτύου».

5. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΠΡΟΤΑΣΕΙΣ

Μελετώντας τους επιμέρους άξονες πάνω στους οποίους στηρίχθηκε και υλοποιήθηκε η παρούσα βιβλιογραφική και δικτυογραφική έρευνα προκύπτει ένα πλήθος συμπερασμάτων και προτάσεων, όπως αυτά αξιολογούνται από την κριτική ματιά του συγγραφέα.

Αρχικά, κρίνεται σκόπιμο να τονιστεί πως τα οφέλη και η προσφορά του Διαδικτύου σε ποικίλους τομείς όπως η εκπαίδευση, η μόρφωση, η υγεία, η έρευνα, η ψυχαγωγία, η επικοινωνία στις κοινωνίες των πολιτών, η ανταλλαγή πληροφοριών και απόψεων, κ.ά., το καθιστούν αναμφισβήτητα το σπουδαιότερο μέσο νέων τεχνολογιών της σύγχρονης εποχής. Ωστόσο, υπάρχουν αρκετοί ποικιλόμορφοι κίνδυνοι που συνοδεύουν τα αναρίθμητα αυτά οφέλη, τους οποίους οι χρήστες και ιδιαίτερα οι νέοι, τόσο σε ηλικία όσο και σε εμπειρία, θα πρέπει να γνωρίζουν για να λαμβάνουν τα κατάλληλα κάθε φορά μέτρα που θα τους επιτρέπουν να απολαμβάνουν τα θετικά στοιχεία του Διαδικτύου απαλλαγμένοι από την επιρροή κακόβουλων παρεμβάσεων. Στα πλαίσια αυτά, η παρούσα εργασία εξέτασε τους κυριότερους κινδύνους του Διαδικτύου, όχι για να αποτρέψει τη χρήση του, απεναντίας, μέσα από μια συγκεντρωτική επισκόπηση να βοηθήσει στο βαθμό που της αναλογεί στην ορθή χρήση του Διαδικτύου.

5.1 Συμπερασματική απόδοση της έρευνας σύμφωνα με την κριτική άποψη του συγγραφέα

Τα τελευταία χρόνια ετερόκλητες δομές και οργανισμοί, όπως ενορίες, δήμοι, σχολεία, κ.λπ., έχουν ευαισθητοποιηθεί σχετικά με τους κινδύνους που ελλοχεύει η χρήση του Διαδικτύου και υλοποιούν δράσεις ενημέρωσης των νεαρών ατόμων, των γονέων και κηδεμόνων τους, καθώς και των εκπαιδευτικών που στελεχώνουν την πρωτοβάθμια και δευτεροβάθμια εκπαίδευση· γεγονός που αναδεικνύει τη σπουδαιότητα του φαινομένου και την ύπαρξή του ως πραγματικό πρόβλημα της ελληνικής κοινωνίας. Σκοπός τους είναι τόσο η ενημέρωση και η πρόληψη, όσο και η καταπολέμηση φαινομένων που παρεκκλίνουν της ορθής χρήσης του Διαδικτύου από νεαρά άτομα. Στην προσπάθεια αυτή σημαίνουσας σημασίας είναι η συμβολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και της Μονάδας Εφηβικής Υγείας του Νοσοκομείου Παίδων «Α. & Π. Κυριακού».

Οι δράσεις αυτές αποσκοπούν στη διαπαιδαγώγηση των χρηστών έχοντας συνήθως τη μορφή τηλεδιασκέψεων, συνεδρίων, ημερίδων, κ.λπ. ενώ η προσφορά τους έχει πολλαπλές διαστάσεις δεδομένου πως αφενός μεν θωρακίζουν τα άτομα που σήμερα διανύουν την ευαίσθητη σε κινδύνους νεότητά τους, αφετέρου δε καθίσταται η σωστή χρήση του Διαδικτύου κτήμα τους. Με τον τρόπο αυτό, γεννιέται ο πρώτος πυρήνας ατόμων που βιωματικά πλέον αποκτά σωστές και ασφαλείς συνήθειες χρήσης του Διαδικτύου με αποτέλεσμα να είναι σε θέση να τις μεταλαμπαδεύσει και να προστατεύσει και τις επόμενες γενιές από τους κινδύνους του Διαδικτύου.

Καθοριστικός για τη σωστή χρήση του Διαδικτύου κρίνεται, επίσης, ο ρόλος των γονέων, των κηδεμόνων και των εκπαιδευτικών λειτουργών, καθώς έρχονται σε επαφή πολλές ώρες ημερησίως με τα νεαρά άτομα με τα οποία αναπτύσσουν σχέσεις οικειότητας και εμπιστοσύνης. Είναι σημαντικό, άλλωστε, οι νέοι να νιώθουν πως σε περίπτωση ανάγκης μπορούν να απευθυνθούν σε αυτούς και να δεχθούν μια υπεύθυνη αντιμετώπιση που θα τους βοηθήσει να ξεπεράσουν ενδεχόμενα προβλήματα που προέκυψαν από τη χρήση του Διαδικτύου. Επιπροσθέτως, μέσω της επαγρύπνησης των γονέων, των κηδεμόνων και των εκπαιδευτικών είναι δυνατός ο εντοπισμός της αλλαγής συμπεριφοράς του νεαρού κατά περίπτωση ατόμου και η άμεση παρέμβαση με τη βοήθεια των ειδικών επί του θέματος στους οποίους είναι εύκολο να απευθυνθούν

καθώς η βοήθεια παρέχεται δωρεάν, σε εικοσιτετράωρη βάση και με ποικίλους τρόπους (μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου, κ.ά.) διατηρώντας παράλληλα πλήρη εχεμύθεια.

Αναφερόμενοι στους κινδύνους γενικότερα, αλλά και στους κινδύνους που συνοδεύουν τη χρήση του Διαδικτύου ειδικότερα, θεωρείται απαραίτητη η εξέταση και ο διαχωρισμός τους κατά τρόπο που να προκύπτει το πολυδιάστατο του χαρακτήρα τους.

Πιο συγκεκριμένα, οι κίνδυνοι του Διαδικτύου μπορούν να ειδωθούν ***τοπικά, κοινωνικά*** *και* ***χρονικά***.

Αναλυτικότερα, ο **τόπος** στον οποίο δραστηριοποιείται ο χρήστης του Διαδικτύου διαφοροποιεί τους κινδύνους από τους οποίους απειλείται, άλλοτε αυξάνοντας και άλλοτε μειώνοντας τη συχνότητα εμφάνισης ή το βαθμό έντασής τους. Λόγου χάρη, ο μεγάλος πληθυσμός των μεγαλουπόλεων σε συνδυασμό με την αποξένωση που συχνά χαρακτηρίζει τις σχέσεις μεταξύ των κατοίκων τους, θέτει εντονότερο τον κίνδυνο αποπλάνησης ενός ατόμου, συγκριτικά με το χρήστη του Διαδικτύου μιας μικρότερης επαρχιακής περιοχής όπου οι κάτοικοι γνωρίζονται καλύτερα και έχουν αναπτύξει στενότερους κοινωνικούς δεσμούς.

Όσον αφορά στην **κοινωνική** διάσταση του φαινομένου, μπορεί να θεωρηθεί πως άτομα αλλοδαπής καταγωγής ιδιαίτερα όταν προέρχονται από υποανάπτυκτες χώρες, καθώς επίσης και ομοφυλόφιλα άτομα, θηλυπρεπή αγόρια, ή κορίτσια με αρρενωπά χαρακτηριστικά ανήκουν σε πιο ευάλωτες κοινωνικές ομάδες σε θέματα αποπλάνησης και Διαδικτυακού εκφοβισμού (cyber bullying). Επίσης, η ηλικία στην οποία βρίσκεται ο χρήστης του Διαδικτύου έχει εξέχοντα ρόλο αρχικά στο κατά πόσον κινδυνεύει ή όχι από μια Διαδικτυακή δραστηριότητα, και δευτερευόντως σε θετική περίπτωση σε πιο βαθμό, καθώς μια δραστηριότητα ή το περιεχόμενο με το οποίο έρχεται σε επαφή μπορεί για μία συγκεκριμένη ηλικία να θεωρείται επικίνδυνο ενώ για μία άλλη ακίνδυνο.

Επιπλέον, η **χρονική** στιγμή κατά την οποία λαμβάνει χώρα μία Διαδικτυακή δραστηριότητα καθορίζει και την έκταση του κινδύνου που τη συνοδεύει. Για παράδειγμα, κατά τις εορταστικές περιόδους αυξάνεται τόσο ο αριθμός διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, όσο και η συχνότητα ανταλλαγής ευχητήριων παραδείγματος χάριν μηνυμάτων με γνωστούς και φίλους, με αποτέλεσμα αφενός μεν να κατακλύζονται οι χρήστες ηλεκτρονικής αλληλογραφίας από ανεπιθύμητα μηνύματα, αφετέρου δε η πιθανότητα ανάγνωσης αυτών και έκθεσης των χρηστών σε ποικίλους άλλους κινδύνους, ακόμη και εκ παραδρομής, να είναι ιδιαίτερα αυξημένη. Επίσης, η ολίσθηση στον ηλεκτρονικό τζόγο είναι πιο πιθανή κατά την περίοδο εορτών δεδομένου ότι ο τζόγος, εν γένει, κατά τις περιόδους αυτές αποτελεί ένα ιδιαίτερο έθιμο στην εποχή μας.

Στο σημείο αυτό κρίνεται σκόπιμο να τονισθεί ότι πολλές φορές οι κίνδυνοι του Διαδικτύου επηρεάζονται και από τον ***συνδυασμό*** των προαναφερθέντων ***τοπικών***, ***κοινωνικών*** και ***χρονικών κριτηρίων***. Ένα τέτοιο παράδειγμα θα μπορούσε να αποτελέσει ένα κοινωνικό γεγονός που μπορεί να συμβεί για συγκεκριμένη χρονική περίοδο και σε συγκεκριμένη περιοχή, όπως μία ενδεχόμενη εξαγορά τράπεζας που δραστηριοποιείται σε μία μόνο περιοχή της Χώρας (π.χ. Δωδεκάνησα) η οποία θα αποτελούσε μία καλή ευκαιρία για επιτήδειους να υποκλέψουν μέσω Διαδικτύου ευαίσθητα προσωπικά δεδομένα χρησιμοποιώντας τεχνικές «phishing» ή «pharming».

5.2 Προτάσεις βελτιστοποίησης του υφιστάμενου πλαισίου για την αντιμετώπιση των κινδύνων του Διαδικτύου

Δεδομένων των παραπάνω συμπερασμάτων και αναγνωρίζοντας πως οι κίνδυνοι του Διαδικτύου αποτελούν, ιδιαίτερα για τους νέους χρήστες, μια πραγματική απειλή που δεν θα πρέπει όμως να αποτελέσει σε καμία περίπτωση τροχοπέδη στην αποδοχή και απόλαυση των αναρίθμητων οφελών του, προτείνεται να κινητοποιηθούν εντονότερα η πολιτεία, η κοινωνία και κάθε άτομο ξεχωριστά, προς την κατεύθυνση αντιμετώπισης των κινδύνων μέσω της πρόληψης και δευτερευόντως μέσω της καταστολής. Άλλωστε, η καλή, οργανωμένη και συστηματική πρόληψη προστατεύει σε μεγαλύτερο βαθμό και πιο αποτελεσματικά τον κάθε χρήστη σε αντιδιαστολή με το οποιοδήποτε είδους μέτρο καταστολής κινδύνου και αν εφαρμοστεί, δεδομένου ότι ο χρήστης στην πρώτη περίπτωση δεν θα έρθει καν σε επαφή με τον κίνδυνο αυτόν.

Πιο συγκεκριμένα, η ενημέρωση και η εκπαίδευση των χρηστών, και ιδίως των νεαρών, κρίνεται πρωταρχικής σημασίας δεδομένου πως ο κάθε χρήστης χρειάζεται πρωτίστως να χαρακτηρίζεται από παιδεία στην ορθολογική χρήση του Διαδικτύου («μέτρο πρόληψης»), παρά να επαναπαύεται στη χρήση των διαφόρων τεχνικών μεθόδων προστασίας («μέτρα καταστολής») καθόσον εν τέλει η προστασία που αυτές παρέχουν δεν είναι απόλυτη και ολοκληρωτική. Είναι γνωστό, άλλωστε, πως οποιαδήποτε τεχνική μέθοδος και αν επιλεγεί δεν εφαρμόζεται μεμονωμένα αλλά λειτουργεί παράλληλα και σε συνδυασμό με άλλες, ώστε να καλύπτονται όσο το δυνατόν περισσότερα κενά προστασίας που παρουσιάζονται.

Κατά συνέπεια, η έμφαση στις παιδαγωγικές μεθόδους αντιμετώπισης των κινδύνων του Διαδικτύου αποτελούν την πλέον ενδεδειγμένη λύση και για το σκοπό αυτό προτείνεται η εισαγωγή στα αναλυτικά προγράμματα σπουδών της πρωτοβάθμιας και της δευτεροβάθμιας εκπαίδευσης συγκεκριμένου μαθήματος που θα παρέχει στους μαθητές τις απαιτούμενες γνώσεις και συμβουλές. Το μάθημα αυτό θα πρέπει να έχει μια λογική συνέχεια από τάξη σε τάξη ώστε να μην καταλήξει σε στείρα επανάληψη, καθώς επίσης να προάγει και τη βιωματική μάθηση η οποία αποτελεί ίσως έναν από τους πιο αποτελεσματικούς τρόπους πραγματικής κτήσης της γνώσης. Βέβαια, προϋπόθεση για την υλοποίηση αυτής της ιδέας αποτελεί η προηγούμενη εκπαίδευση των ιδίων των εκπαιδευτικών σε θέματα Διαδικτύου η οποία εν τέλει θα έχει διττό όφελος, δεδομένου ότι οι γνώσεις δεν θα χρησιμοποιηθούν αποκλειστικά και μόνο για τη διδασκαλία του συγκεκριμένου μαθήματος, αλλά θα συντελέσουν και στη δημιουργία αντιλήψεων και στάσεων σωστής χρήσης του Διαδικτύου και από τους ίδιους τους εκπαιδευτικούς, ενώ θα τους ευαισθητοποιήσουν κατάλληλα με αποτέλεσμα να εντοπίζουν τις πρώιμες συμπεριφορές των μαθητών τους, οι οποίες δηλώνουν την ύπαρξη προβλημάτων από τη χρήση του Διαδικτύου.

Επιπροσθέτως, σημαίνουσας σημασίας κρίνεται πως είναι και η δραστηριοποίηση των συλλόγων γονέων και κηδεμόνων κάθε σχολείου με στόχο την ενημέρωση όχι μόνο των νέων που φοιτούν στα σχολεία της Χώρας, αλλά κυρίως των γονέων και των κηδεμόνων τους. Οι τελευταίοι σύμφωνα με τα δεδομένα της εποχής απαιτείται να γνωρίζουν σε βάθος τη χρήση των μέσων της τεχνολογίας και του Διαδικτύου, κυρίως για να είναι σε θέση να συμβουλεύσουν, να βοηθήσουν και να καθοδηγήσουν τα παιδιά τους προς την κατεύθυνση της ασφαλούς χρήσης του Διαδικτύου. Επιπρόσθετα, τα νεαρά άτομα τείνουν να μιμηθούν τη συμπεριφορά προτύπων που θαυμάζουν κάτι που επιφορτίζει τους ενήλικες με μεγαλύτερη ευθύνη για εκδήλωση σωστής συμπεριφοράς σε όλους τους τομείς της ζωής τους και κυρίως σε αυτούς που οι νέοι ακόμη διαμορφώνουν τη στάση τους.

Πέραν αυτών, μείζονος σημασίας θεωρείται η συχνή και συστηματική προβολή τηλεοπτικών σποτ, που προβάλλουν τους κινδύνους του Διαδικτύου και προτείνουν οδηγίες αντιμετώπισης τους, κυρίως σε ώρες που παρατηρείται αυξημένη τηλεθέαση από τα νεανικά κοινά σε συνδυασμό με ώρες προβολής οικογενειακών σειρών κατά τις οποίες τα μέλη της οικογένειας συχνά συγκεντρώνονται και τις παρακολουθούν σε κοινόχρηστο χώρο του σπιτιού. Με τον τρόπο αυτόν, δίδεται η δυνατότητα συζήτησης επί του θέματος καθώς θα δημιουργηθεί κατάλληλο κλίμα για ευκολότερη έκφραση των προβληματισμών ή ακόμη και των προβλημάτων των νέων. Στην ίδια λογική, προτείνεται επιπλέον και η οργανωμένη διαφήμιση των δικτυακών και μη-δικτυακών πόρων αντιμετώπισης των κινδύνων του Διαδικτύου (π.χ. Γραμμή Βοήθειας «ΥποΣΤΗΡΙΖΩ») προκειμένου γνωρίζουν οι ενδιαφερόμενοι νεαροί χρήστες, γονείς, κηδεμόνες και εκπαιδευτικοί πού μπορούν να απευθυνθούν για μια έγκυρη και υπεύθυνη αντιμετώπιση των κινδύνων του Διαδικτύου.

Τέλος, δεδομένου πως οι συνήθειες χρήσης του Διαδικτύου και κατ' επέκταση οι κίνδυνοι του Διαδικτύου αλλάζουν δυναμικά, θα πρέπει να υπάρχει διαρκής ενημέρωση σχετικά με τις νέες εφαρμογές, δραστηριότητες και δυνατότητες που παρέχει το Διαδίκτυο συνοδευόμενες πάντοτε από τους κινδύνους που ελλοχεύουν και τους τρόπους αντιμετώπισής τους, προκειμένου προληφθούν, κατά το ει δυνατόν, ενδεχόμενοι νέοι κίνδυνοι που εμφανίζονται, ενώ σε περίπτωση μη δυνατότητας έγκαιρης πρόληψής τους να αντιμετωπιστούν τουλάχιστον εν τη γενέσει τους ώστε να αποφευχθεί ενδεχόμενη διόγκωσή τους. -

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Action games	Παιχνίδια δράσης
Activity	Δραστηριότητα
Administrator	Διαχειριστής
Antimalware	Πρόγραμμα προστασίας και καταπολέμησης κακόβουλου λογισμικού
Antivirus	Πρόγραμμα προστασίας και καταπολέμησης από ιούς
Avatar	Εικονικός εαυτός
Bad Language	Χυδαία γλώσσα
Bayesian	Πιθανοτικός
Beat ‘em up games	Παιχνίδια ξυλοδαρμού – πολεμικών τεχνών
Black lists	Μαύρες λίστες
Blogs	Ιστολόγια
Brain virus	Ιός «Brain»
Broadband connections	Ευρυζωνικές συνδέσεις
Browser	Φυλλομετρητής
Browsing history	Ιστορικό πλοήγησης
Bulk mails	Ομαδική αλληλογραφία
Chain e-mails	Αλυσιδωτά μηνύματα ηλεκτρονικού ταχυδρομείου
Chat	Συνομιλία
Chat-rooms	Δωμάτια συνομιλίας
Child pornography	Παιδική πορνογραφία
Clean	Επιδιόρθωση
Convention on Cybercrime	Σύμβαση για τα Διαδικτυακά Εγκλήματα
Council of Europe	Συμβούλιο της Ευρώπης
Crowdsourcing approach	Προσέγγιση με τη μέθοδο πληροφόρησης από το κοινό
Cyber bullying	Διαδικτυακός εκφοβισμός
Demilitarized zones	Ουδέτερες ζώνες
Discrimination	Διάκριση
Download history	Ιστορικό «κατεβασμένων» αρχείων
Drugs	Ναρκωτικά
DVD box	Συσκευασία παιχνιδιού
E-mail	Ηλεκτρονικό ταχυδρομείο
E-mail addresses	Διευθύνσεις ηλεκτρονικού ταχυδρομείου
E-mail attached files	Συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου
Excessive use	Υπερβολική χρήση
Face-to-face contact	Επαφή πρόσωπο με πρόσωπο
Fear	Φόβος
Fighting games	Παιχνίδια πάλης
File sharing network	Δίκτυο διαμοιρασμού αρχείων
File viruses	Ιοί αρχείων
Firewall	Τείχος προστασίας

Ξενόγλωσσος όρος	Ελληνικός Όρος
Gambling	Τζόγος
Game consoles	Παιχνιδομηχανές
Grey lists	Γκρίζες λίστες
Hack and slash games	Παιχνίδια ξυλοδαρμού – πολεμικών τεχνών
Heuristic	Ευρεστικός
Hoax viruses	Ιοί απάτης
Infected files	Μολυσμένα αρχεία
Infected programs	Μολυσμένα προγράμματα
Instant messagers	Προγράμματα άμεσης επικοινωνίας
Instant messages	Άμεσα μηνύματα
Interactive games	Αλληλεπιδραστικά – Διαδραστικά παιχνίδια
Interactive Software Federation of Europe	Ευρωπαϊκή Ομοσπονδία Αλληλεπιδραστικού Λογισμικού
International Association of CyberPsychology, Training, and Rehabilitation	Διεθνής Σύνδεσμος για τη Διαδικτυακή Ψυχολογία, την Εξάσκηση και την Επανένταξη
International Telecommunications Union	Διεθνής Ένωση Τηλεπικοινωνιών
Internet	Διαδίκτυο
Internet addiction	Διαδικτυακός εθισμός
Internet Content Rating Association	Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου
Internet privacy	Διαδικτυακή ιδιωτικότητα
Internet Service Providers	Φορείς Παροχής Υπηρεσιών Διαδικτύου
Keyloggers	Καταγραφείς πληκτρολόγησης
Local Area Network	Τοπικό δίκτυο
Malware	Κακόβουλο λογισμικό
Misinformation	Παραπληροφόρηση
Multiplayer LAN games	Παιχνίδια πολλαπλών παικτών σε τοπικό δίκτυο
Negative repercussions	Αρνητικές επιπτώσεις
Network	Δίκτυο
Networking	Δικτύωση
Offensive content	Ακατάλληλο – προσβλητικό περιεχόμενο
On-line banking	Ηλεκτρονική τραπεζική
Online gambling	Ηλεκτρονικός τζόγος
Online games	Διαδικτυακά παιχνίδια
Pan-European Game Information	Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια
Parental control	Γονικός έλεγχος
Polymorphic viruses	Πολυμορφικοί ιοί
Pop-ups	Αναδυόμενα παράθυρα
Processes	Διεργασίες
Quarantine	Απομόνωση
Real time	Σε πραγματικό χρόνο
Remote control	Απομακρυσμένος έλεγχος
Rutgers University	Πανεπιστήμιο του Ράτγκερς
Search history	Ιστορικό αναζήτησης
Sex	Σεξ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Shooter games	Παιχνίδια βολών
Social isolation	Κοινωνική αποξένωση
Social networking	Κοινωνική δικτύωση
Social networking sites	Ιστότοποι κοινωνικής δικτύωσης
Spam – Bulk mail filtering	Διαχωρισμός ανεπιθύμητης – ομαδικής αλληλογραφίας
Spam messages	Ανεπιθύμητα μηνύματα
Stand-alone devices	Αυτόνομες συσκευές
Stanford Research Institute	Ινστιτούτο Ερευνών του Στάνφορντ
Stealth viruses	Αόρατοι ιοί
Texas A&M International University	Πανεπιστήμιο του Τέξας
Tolerance	Ανοχή
Traffic control	Έλεγχος κίνησης δεδομένων
Trojan horses	Δούρειοι ίπποι
University of California, Los Angeles	Πανεπιστήμιο της Καλιφόρνια
University of Iowa	Πανεπιστήμιο της Αϊόβα
Unsolicited material	Ανεπιθύμητο υλικό
Update	Ενημέρωση
Upgrade	Αναβάθμιση
Urban legends	Αστικοί μύθοι
User	Χρήστης
User traces	Ηλεκτρονικά αποτυπώματα του χρήστη
Video games	Παιχνίδια κονσόλας
Villanova University	Πανεπιστήμιο της Βιλανόβα
Violence	Βία
Violent games	Βίαια παιχνίδια
Virtual reality	Εικονική πραγματικότητα
Visuospatial cognition	Οπτικοχωρική νόηση
Walled gardens	Περιφραγμένες τοποθεσίες
Web	Ιστός
Web sites	Ιστοσελίδες
Web threat	Απειλή στον Ιστό
Webinars	Διαδικτυακά σεμινάρια
Website rating	Αξιολόγηση – Βαθμολόγηση ιστοσελίδας
White lists	Λευκές λίστες
Withdrawal	Απόσυρση
Word-based	Λεξικογραφικός
World Wide Web	Παγκόσμιος Ιστός
Worms	Σκουλήκια
Zombie networks	«Παγιδευμένα» δίκτυα

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ARPAnet	Advanced Research Projects Agency Network
DMZ	Demilitarized zones
iACToR	International Association of CyberPsychology, Training, and Rehabilitation
ICRA	Internet Content Rating Association
ISFE	Interactive Software Federation of Europe
ISFE	Interactive Software Federation of Europe
ISP	Internet Service Provider
ITU	International Telecommunications Union
kWh	Kilowatt hour
LAN	Local Area Network
PEGI	Pan-European Game Information
RAM	Random Access Memory
SRI	Stanford Research Institute
UCLA	University of California, Los Angeles
WWW	World Wide Web
βλ.	βλέπε
ΕΔΕΤ	Εθνικό Δίκτυο Έρευνας και Τεχνολογίας
Η.Π.Α.	Ηνωμένες Πολιτείες Αμερικής
Η/Υ	Ηλεκτρονικός Υπολογιστής
ΙΜΕ	Ίδρυμα Μείζονος Ελληνισμού
ΙΤΕ-ΙΠ	Ίδρυμα Τεχνολογίας και Έρευνας - Ινστιτούτο Πληροφορικής
ΚΕ.Θ.Ε.Α.	Κέντρου Θεραπείας Εξαρτημένων Ατόμων
ΚΕ.ΠΛΗ.ΝΕ.Τ.	Κέντρο Πληροφορικής & Νέων Τεχνολογιών
Μ.Ε.Υ.	Μονάδα Εφηβικής Υγείας
Μ.Μ.Ε.	Μέσα Μαζικής Ενημέρωσης
ΥΠ.Ο.Α.Δ.Η.Ε.	Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

ΑΝΑΦΟΡΕΣ

[1] "Τι είναι το Internet", *Κέντρο Δικτύου, Πανεπιστήμιο Θράκης*, Δεκ. 1997; www.uth.gr/main/help/help-desk/internet/internet2.html [Προσπελάστηκε 07/11/2014]

[2] L. M. Barry et al., "A Brief History of the Internet", *Internet Sociaty*; www.internethalloffame.org/brief-history-internet#Origins [Προσπελάστηκε 07/11/2014]

[3] "A History of the Internet: 1962-1992"*, Computer History Museum*, 2004; www.computerhistory.org/internet_history/index.html [Προσπελάστηκε 07/11/2014]

[4] D. Harper, "Arpanet", *Online Etymology Dictionary,* 2010; http://dictionary.reference.com/browse/arpanet [Προσπελάστηκε 07/11/2014]

[5] "Exhibits: Timeline of Computer History", *Computer History Museum,* 2006; www.computerhistory.org/timeline/?category=net [Προσπελάστηκε 08/11/2014]

[6] "Ιστορία", *Οργανισμός Τηλεπικοινωνιών Ελλάδος (ΟΤΕ);* https://www.ote.gr/web/guest/corporate/company/who-we-are/history [Προσπελάστηκε 08/11/2014]

[7] "Percentage of Individuals using the Internet 2000-2013", *International Telecommunications Union (ITU)*, 2014; http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls [Προσπελάστηκε 08/11/2014]

[8] Ν. Τζιμόπουλος, Α. Πόρποδα και Π. Προβελέγγιος, "Ασφαλής χρήση του Διαδικτύου", *2ο Πανελλήνιο Συνέδριο Ημαθίας (ΠΣΗ 2010),* σ. 1723-1730.

[9] Safer Internet: Cyberethics", 2011; www.cyberethics.info [Προσπελάστηκε 09/11/2014]

[10] M. J. Matthew, "Internet Dangers", *Education Technology Center,* 23 Oct. 2010; https://wiki.uiowa.edu/display/edtech/Internet+Dangers [Προσπελάστηκε 09/11/2014]

[11] M. Jennifer, "What are "Internet dangers?'", *Education Technology Center,* 23 Mar. 2011; https://wiki.uiowa.edu/pages/viewpage.action?pageId=49483037 [Προσπελάστηκε 09/11/2014]

[12] "The Online Protection Talk", *Trend Micro,* 2011; www.trendmicro.tw/cloud-content/us/pdfs/internet-safety/br_the-online-protection-talk.pdf [Προσπελάστηκε 09/11/2014]

[13] "Web treat", *Wikipedia;* http://en.wikipedia.org/wiki/Web_threat [Προσπελάστηκε 09/11/2014]

[14] Τριανταφυλλίδης, επιμ., "Λεξικό της Κοινής Νεοελληνικής", *Κέντρο Ελληνικής Γλώσσας, 2006-2008;* www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=κίνδυνος [Προσπελάστηκε 09/11/2014]

[15] Τριανταφυλλίδης, επιμ., "Λεξικό της Κοινής Νεοελληνικής", *Κέντρο Ελληνικής Γλώσσας, 2006-2008;* www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=ασφάλεια&dq [Προσπελάστηκε 09/11/2014]

[16] "Κίνδυνοι στο Διαδίκτυο", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_akatalperiex.html [Προσπελάστηκε 09/11/2014]

[17] "Ακατάλληλο Περιεχόμενο", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?objId=Category291&parentobjId=Page187 [Προσπελάστηκε 11/11/2014]

[18] "Ακατάλληλο ή παράνομο υλικό", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου;* www.saferinternet.gr/index.php?childobjId=Category120&objId=Category38&parentobjId=Page2 [Προσπελάστηκε 11/11/2014]

[19] Commonwealth of Australia, "Dealing with offensive content (Greek)", *Cybersmart*, 2015; www.cybersmart.gov.au/Parents/Resources/Educate%20yourself/Dealing%20with%20offensive%20content%20Greek.aspx [Προσπελάστηκε 11/11/2014]

[20] "Κίνδυνοι: Ανεπιθύμητα Μηνύματα", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_anepithminimata.html [Προσπελάστηκε 12/11/2014]

[21] Καριοφύλλης Α., "Ανεπιθύμητα e-mails (spam)", W-Learn: *Πρόσβαση στη Γνώση*, 2005-2014; www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam [Προσπελάστηκε 12/11/2014]

[22] "Ανεπιθύμητη Αλληλογραφία (Spam)", *Κέντρο Δικτύων Ε.Μ.Π., 06 Οκτ. 2010;* www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104 [Προσπελάστηκε 12/11/2014]

[23] "Spam e-mails produce the same amount of greenhouse gas as 3,1 million cars", *Mail Online,* 15 April 2009; www.dailymail.co.uk/sciencetech/article-1170177/Spam-emails-produce-greenhouse-gas-3-1million-cars.html [Προσπελάστηκε 16/11/2014]

[24] Κίνδυνοι: Αποξένωση από τον πραγματικό κόσμο", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_apoxenosi.html [Προσπελάστηκε 17/11/2014]

[25] M. Popova and Br. Pickings, *"Alter Ego, Portraits of Gamers next to their Avatars"*, 14 Dec. 2011; www.brainpickings.org/index.php/2011/12/14/alter-ego-robbie-cooper/ [Προσπελάστηκε 17/11/2014]

[26] Τολούδης Α., "Τι συμβαίνει όταν τα avatar εισβάλλουν στη ζωή μας", *Τεχνολογικές Συναντήσεις,* 16 Οκτ. 2012; http://tech.in.gr/presentations/article/?aid=1231217957 [Προσπελάστηκε 17/11/2014]

[27] Γραμμή Καταγγελιών Safeline.gr, "Σε ποιο κόσμο ζεις;", *YouTube,* 20 Ιαν. 2010; www.youtube.com/watch?v=8hJpgtJMNBc&list=UUP6b_h1QMIrgFWRWW5NPoiQ&index=3&feature=plcp [Προσπελάστηκε 17/11/2014]

[28] Ελληνικό Κέντρο Ασφαλούς Διαδικτύου; www.saferinternet.gr/ [Προσπελάστηκε 17/11/2014]

[29] "Κίνδυνοι: Αποπλάνηση", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_apoplanisi.html [Προσπελάστηκε 18/11/2014]

[30] Internet Safety 101, "How Do Predators Groom Kids", *Enough Is Enough;* www.internetsafety101.org/grooming.htm [Προσπελάστηκε 17/11/2014]

[31] Parents Protect, "*What is Grooming*"; www.parentsprotect.co.uk/online_grooming.htm [Προσπελάστηκε 17/11/2014]

[32] Κίνδυνοι: Βίαια παιχνίδια", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_biaiapaixnidia.html [Προσπελάστηκε 19/11/2014]

[33] "List of video game genres", *Wikipedia;* http://en.wikipedia.org/wiki/List_of_video_game_genres #Action [Προσπελάστηκε 19/11/2014]

[34] ProCon.org, *"Do Violent Video Games Contribute to Youth Violence?",* 10 June 2014; http://videogames.procon.org/#Background [Προσπελάστηκε 19/11/2014]

[35] Video Games Addiction, "*Violence and Video Games*"; www.video-game-addiction.org/ violence.html [Προσπελάστηκε 19/11/2014]

[36] C. F. Ferguson, "*The Good, The Bad and The Ugly: A meta-analytic Review of Possitive and Negative Effects of Violent Video Games*", Springer Science and Busyness Media, Vol. 78, No 4, Dec. 2007, pp. 309-316; http://link.springer.com/article/10.1007%2Fs11126-007-9056-9 [Προσπελάστηκε 19/11/2014]

[37] R. Boyle and M. Hibberd, "*Review of research on the impact of violent computer games on young people*" Stirling Media Research Institute, Mar. 2005.

[38] P. M. Markey, C. N. Markey and J. E. French, "*Violent Video Games and Real-World Violence: Rhetoric Versus Data*", Psychology of Popular Media Culture. 18 Aug. 2014; http://dx.doi.org/10.1037/ppm0000030 [Προσπελάστηκε 19/11/2014]

[39] Κίνδυνοι: Εθισμός", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_ethismos.html [Προσπελάστηκε 19/11/2014]

[40] Α. Τσίτσικα, *"Χρήση και Κατάχρηση του Διαδικτύου"*, Ιάτωρ, 20 Απρ. 2010; www.iator.gr/ 2010/04/20/internet-kataxrisi-diadiktyou/#more-10683 [Προσπελάστηκε 25/11/2014]

[41] Θ. Τσώλη, "Εθισμός στο Internet: μια υπαρκτή απειλή", *Το Βήμα Science*, 11 Nov 2008; www.tovima.gr/science/article/?aid=244780 [Προσπελάστηκε 22/11/2014]

[42] K.E. Siomos et al. "Internet Addiction among Greek Adolescent Students", *Cyberpsychology & Behavior*, vol. 11, no 6, 2009, pp. 653-657.

[43] K. Chakraborty, D. Basu, K. G. Vijaya Kumar , "Internet Addiction: Consensus, Controversies, and the Way Ahead", *East Asian Arch Psychiatry,* 2010, vol 20., pp.123-32; http://easap.asia/journal_file/1003_V20N3_p123.pdf [Προσπελάστηκε 22/11/2014]

[44] Σ. Μανουσέλης, "Όταν δεν επικοινωνούμε, νιώθουμε κοινωνικά ανύπαρκτοι", *Ελευθεροτυπία,* 24 Οκτ. 2009; www.enet.gr/?i=news.el.episthmh-texnologia&id=94965 [Προσπελάστηκε 22/11/2014]

[45] P.K. Smith, J. Madhavi, M. Carvalho, M. Fisher, S. Russell and N. Tippett, Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry,* vol. 49, no 4, 2008, pp. 376-385.

[46] M. Cart, A literature of risk, *American Library Association,* vol. 41. no 5, pp. 32-35.

[47] Κίνδυνοι: Εκφοβισμός (Cyberbulling)", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_ekfobismos.html [Προσπελάστηκε 22/11/2014]

[48] Η. Σπύρου, επιμ., "Beat bulling¨εντείνεται ο διαδικτυακός εκφοβισμός", *StudyCyprus.eu;* www.studycyprus.eu/easyconsole.cfm/id/930 [Προσπελάστηκε 22/11/2014]

[49] Κίνδυνοι: Επιβλαβείς συμπεριφορές", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_epiblabeissimber.html [Προσπελάστηκε 22/11/2014]

[50] Κίνδυνοι: Ηλεκτρονικός Τζόγος", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_eltzogos.html [Προσπελάστηκε 22/11/2014]

[51] Δ. Μαλλάς, "Κέρδισε 400.000 Έλληνες ο ηλεκτρονικός τζόγος", *Ημερήσια "Η"*, 08 Μαρ 2012; www.imerisia.gr/article.asp?catid=26510&subid=2&pubid=112831604 [Προσπελάστηκε 23/11/2014]

[52] Οικονομικό Πανεπιστήμιο Αθηνών (ELTRUN); www.eltrun.gr/ [Προσπελάστηκε 23/11/2014]

[53] Γλωσσάρι Ορολογίας για το Διαδίκτυο; http://gr.norton.com/glossary-of-online-security-terms/article [Προσπελάστηκε 26/11/2014]

[54] Εργαστήριο Εφαρμογών Πληροφορικής στα ΜΜΕ, "*Ιοί Υπολογιστών*", 2004; http://pacific .jour.auth.gr/virus/page_7.htm [Προσπελάστηκε 23/11/2014]

[55] "What is the Difference: Viruses, Worms, Trojans and Bots?", *CISCO*; www.cisco.com/ web/about/security/intelligence/virus-worm-diffs.html [Προσπελάστηκε 23/11/2014]

[56] "Common Malware Types: Cybersecurity 101", *VERACODE*, 12 Oct. 2012*;* https://www .veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 [Προσπελάστηκε 25/11/2014]

[57] "History of Viruses", *National Institute of Standards and Technology (NIST): Computer Security Resource Center (CSRC)*, 10 Mar. 1994; http://csrc.nist.gov/publications/nistir/threats/ subsubsection3_3_1_1.html [Προσπελάστηκε 26/11/2014]

[58] "Παιδική Πορνογραφία: Frequently Asked Questions", Ελληνικός Κόμβος Ασφαλούς Διαδικτύου – Μέλος του Πανευρωπαϊκού Δικτύου Εθνικών Κόμβων; www.saferinternet.gr/ index.php?action=download&objId=File192 [Προσπελάστηκε 26/11/2014]

[59] Council of Europe: Convention of Cybercrime, Chapter II, Title 3, Article 9, Section 2, 23/11/2001

[60] Ποινικός Κώδικας, Βιβλίο Β' - Ειδικό μέρος, Κεφάλαιο 19, Άρθρο 348Α, παράγραφος 3

[61] Ποινικός Κώδικας, Βιβλίο Β' - Ειδικό μέρος, Κεφάλαιο 19, Άρθρο 348Γ, παράγραφος 3

[62] J. Ropelato, "Internet Pornography Statistics", *TopTenREVIEWS,* 28 Mar 2014; www.ministryoftruth.me.uk/wp-content/uploads/2014/03/IFR2013.pdf [Προσπελάστηκε 26/11/2014]

[63] Ποινικός Κώδικας, Βιβλίο Β' - Ειδικό μέρος, Κεφάλαιο 19, Άρθρο 348Α, παράγραφος 2

[64] Ποινικός Κώδικας, Βιβλίο Β' - Ειδικό μέρος, Κεφάλαιο 19, Άρθρο 348Α, παράγραφος 5

[65] Κίνδυνοι: Παραβίαση Ιδιωτικής Ζωής", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_parabiidiotik.html [Προσπελάστηκε 26/11/2014]

[66] S. Lohr, "*How Privacy Can Vanish Online, a Bit at a Time*", The New York Times, 17 Mar 2010; www.nytimes.com/2010/03/17/technology/17privacy.html?scp=1&sq=how%20privacy%20can%20v anish%20steve%20lohr&st=cse&_r=0 [Προσπελάστηκε 26/11/2014]

[67] "Privacy, Web Storage", *WHATWG,* 11 Dec. 2012; https://html.spec.whatwg.org/multipage/webstorage.html#privacy [Προσπελάστηκε 26/11/2014]

[68] "Η Ασφάλεια στο Διαδίκτυο-Γεγονότα και Παραπληροφόρηση στο Διαδίκτυο", *Υπουργείου Παιδείας και Πολιτισμού Κύπρου: Εκπαιδευτική Πύλη;* www.schools.ac.cy/parapliroforisi.html [Προσπελάστηκε 26/11/2014]

[69] Κίνδυνοι: Παραπληροφόρηση", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_parapliroforisi.html [Προσπελάστηκε 26/11/2014]

[70] S. Mansell, "*WFU expert cautions new internet myths may be more harmful*", Wake Forest University, 6 Jun. 2003; www.wfu.edu/wfunews/2003/060603r.html [Προσπελάστηκε 26/11/2014]

[71] Γλωσσάρι Ορολογίας για το Διαδίκτυο; http://gr.norton.com/glossary-of-online-security-terms/article [Προσπελάστηκε 26/11/2014]

[72] "Phishing", *Tech.Terms.com;* www.techterms.com/definition/phishing [Προσπελάστηκε 26/11/2014]

[73] "Αλφαβητάρι", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?objId=Category62&parentobjId=Page5 [Προσπελάστηκε 26/11/2014]

[74] "Αλφαβητάρι", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?objId=Category62&parentobjId=Page5 [Προσπελάστηκε 27/11/2014]

[75] "Pharming", *Tech.Terms.com;* www.techterms.com/definition/pharming [Προσπελάστηκε 27/11/2014]

[76] Σ. Δημητρακάκη, "Phishing and Pharming", *Νομικά Επίλεκτα, 4 Νοεμ. 2014;* www.nomika-epilekta.gr/arthra/koinonika-arthra/phishing-and-pharming [Προσπελάστηκε 27/11/2014]

[77] Ποινικός Κώδικας, Βιβλίο Β' - Ειδικό μέρος, Κεφάλαιο 22, Άρθρο 370Γ, παράγραφος 2

[78] Κίνδυνοι: Φυσικές παθήσεις", *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_fysikespathiseis.html [Προσπελάστηκε 27/11/2014]

[79] "Οδηγός σωστής χρήσης του Διαδικτύου", *Microsoft;* www.microsoft.com/hardware/el-gr/support/healthy-computing-guide [Προσπελάστηκε 27/11/2014]

[80] Π. Φωτιάδου, Ε. Πολίτου, Ε. Τσαρτσίδου και Α.-Μ. Σιδηρά, "Διαδικτυακοί Κίνδυνοι"*, SCRIBD,* 2012*;* www.scribd.com/doc/80766050/ΔΙΑΔΙΚΤΥΑΚΟΙ-ΚΙΝΔΥΝΟΙ [Προσπελάστηκε 29/11/2014]

[81] "Καταγγελίες-Στατιστικά Στοιχεία", *Ελληνική Γραμμή για το Παράνομο Περιεχόμενο στο Διαδίκτυο;* www.safeline.gr/kataggelies/statistika-stoiheia [Προσπελάστηκε 29/11/2014]

[82] "Φίλτρα/ Εργαλεία Γονικού Ελέγχου", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?childobjId=Category113&objId=Category36&parentobjId=Page2 [Προσπελάστηκε 29/11/2014]

[83] "Γονικός Έλεγχος", *Ιστοσελίδα για την Α/θμια και τη Β/θμια Εκπαίδευση Ημαθίας,* 2011*;* www.techopedia.com/definition/2541/walled-garden-technology [Προσπελάστηκε 29/11/2014]

[84] "Use A Whitelist to Control Website Logging", *Rescue Time;* https://www.rescuetime.com/whitelists [Προσπελάστηκε 30/11/2014]

[85] "Blacklists" *Blacklistedip,* 2010; www.blacklistedip.com/faq.php [Προσπελάστηκε 31/11/2014]

[86] M. Rousse, "DMZ (Demilitarized Zone) Definition", *TechTarget;* http://searchsecurity.techtarget.com/definition/DMZ [Προσπελάστηκε 29/11/2014]

[87] "How to Avoid Spam Filters", *MailClimp;* http://mailchimp.com/resources/guides/how-to-avoid-spam-filters/html/ [Προσπελάστηκε 29/11/2014]

[88] Br. Satterfield, "*Learn How Different Spam-fighting Techniques Work*", TechSoup, 30 Nov. 2006; www.techsoupcanada.ca/learning_center/10_sfm_explained [Προσπελάστηκε 31/11/2014]

[89] "Crowdsourced web safety", *Web Of Trust (WOT);* https://www.mywot.com/en/aboutus [Προσπελάστηκε 01/12/2014]

[90] "What is Crowdsource?", *Daily Crowdsource;* http://dailycrowdsource.com/training/crowdsourcing/what-is-crowdsourcing [Προσπελάστηκε 01/12/2014]

[91] "Thank you for inquiring about ICRA", *Family Online Safety Institute (FOSI);* https://www.fosi.org/icra/ [Προσπελάστηκε 01/12/2014]

[92] Internet Content Rating Association; https://www.icann.org/tlds/agreements/xxx/about-icra-05jan07.pdf [Προσπελάστηκε 01/12/2014]

[93] Κ. Καραΐσκος, "Γονικός Έλεγχος", *Α/βάθμια και Β/βάθμια Διεύθυνση Ημαθίας,* 2011; http://ima-edu.webnode.gr/products/γονικός-έλεγχος-/ [Προσπελάστηκε 02/12/2014]

[94] "How does the Parental Controls Web Filter works?", *Microsoft;* http://windows.microsoft.com/en-us/windows-vista/how-does-the-parental-controls-web-filter-work [Προσπελάστηκε 02/12/2014]

[95] "Τι είναι antivirus?", *Τι είναι;* http://ti-einai.gr/antivirus/ [Προσπελάστηκε 02/12/2014]

[96] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για Μπαμπάδες και Μαμάδες, για Παππούδες και Γιαγιάδες", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File483 [Προσπελάστηκε 05/12/2014], pp. 20.

[97] "What is Anti-Virus Software?", *Webroot;* www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software [Προσπελάστηκε 02/12/2014]

[98] M. Rousse, "Antivirus Software Definition", *TechTarget;* http://searchsecurity.techtarget.com/definition/antivirus-software [Προσπελάστηκε 02/12/2014]

[99] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για Μπαμπάδες και Μαμάδες, για Παππούδες και Γιαγιάδες", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File483 [Προσπελάστηκε 05/12/2014], pp. 20.

[100] J. Tyson, "How Firewalls Work?", *How Stuff Works,* http://computer.howstuffworks.com/firewall.htm [Προσπελάστηκε 05/12/2014]

[101] "Τα Firewalls", ΚΕ.ΠΛΗ.ΝΕ.Τ. Ν. Φλώρινας; http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html [Προσπελάστηκε 05/12/2014]

[102] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για Μπαμπάδες και Μαμάδες, για Παππούδες και Γιαγιάδες", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File483 [Προσπελάστηκε 05/12/2014], pp. 20.

[103] "Σχετικά με το PEGI", *Pan European Game Information (PEGI);* www.pegi.info/gr/index/id/217/ [Προσπελάστηκε 06/12/2014]

[104] "Σχετικά με το PEGI: Τι σημαίνουν οι επισημάνσεις;", *Pan European Game Information (PEGI);* www.pegi.info/gr/index/id/222/ [Προσπελάστηκε 07/12/2014]

[105] "Σχετικά με το PEGI: Τι σημαίνουν οι επισημάνσεις;", *Pan European Game Information (PEGI);* www.pegi.info/gr/index/id/222/ [Προσπελάστηκε 07/12/2014]

[106] "Σχετικά με το PEGI: Επισήμανση PEGI OK", *Pan European Game Information (PEGI);* www.pegi.info/gr/index/id/1427/ [Προσπελάστηκε 07/12/2014]

[107] "Τι είναι το PEGI On-line;", *Pan European Game Information (PEGI);* www.pegionline.eu/el/index/id/106 [Προσπελάστηκε 08/12/2014]

[108] Αρχηγείο Ελληνικής Αστυνομίας, *"Με επιτυχία πραγματοποιούνται από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος τηλεδιασκέψεις σε σχολεία της χώρας, με θέμα την ασφαλή πλοήγηση στο Διαδίκτυο",* Ελληνική Αστυνομία: Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης, 15 Οκτ. 2014; www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=47010&Itemid=1386&lang= [Προσπελάστηκε 08/12/2014]

[109] "Σύγχρονη Τηλεκπαίδευση και Τηλεδιάσκεψη", *Πανελλήνιο Σχολικό Δίκτυο*; www.sch.gr/conf [Προσπελάστηκε 08/12/2014]

[110] Dim, "*Τηλεδιάσκεψη σε 300 σχολεία για την ασφαλή πλοήγηση στο Internet*", 22 Οκτ. 2014; https://iguru.gr/2014/10/22/cyberkid-internet-project-cyber-crime-unit/ [Προσπελάστηκε 08/12/2014]

[111] Δίωξη Ηλεκτρονικού Εγκλήματος, "Cyberkid: Τηλεδιασκέψεις στα σχολεία για την ασφαλή πλοήγηση στο Internet", *Ημερήσια "Η",* 22 Οκτ. 2014; www.imerisia.gr/article.asp?catid=27200&subid=2&pubid=113372985 [Προσπελάστηκε 08/12/2014]

[112] Ασφάλεια στο Διαδίκτυο, "Σκέψου πριν δημοσιεύσεις: 20+1 ερωταπαντήσεις από το webinar", *Ασφάλεια στο Διαδίκτυο-Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου,* 03 Ιουν. 2014*;* http://internet-safety.sch.gr/index.php/articles/teach/item/292-21 [Προσπελάστηκε 08/12/2014]

[113] "Ενημερωτικό Υλικό/ Webinars", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?objId=Category260&parentobjId=Page15 [Προσπελάστηκε 08/12/2014]

[114] Cyber Crime Unit Greece, "1^{ο} Συνέδριο: Ασφαλής πλοήγηση στο Διαδίκτυο-Αίθουσα 1", *YouTube*, 2 Σεπτ. 2012; https://www.youtube.com/watch?v=KqMeYhqrM6w [Προσπελάστηκε 08/12/2014]

[115] "Παιδί και Κίνδυνοι στο Διαδίκτυο: Δείτε live το 2^{ο} συνέδριο ασφαλούς πλοήγησης στο Διαδίκτυο", *mama 365: μικροί-μεγάλοι,* 07 Febr. 2013; http://mikroimegaloi.gr/content/παιδί-και-κίνδυνοι-στο-διαδίκτυο-δείτε-live-το-2ο-συνέδριο-ασφαλούς-πλοήγησης [Προσπελάστηκε 09/12/2014]

[116] "Συνέδριο Διεθνούς Πανεπιστημίου με θέμα την «Ασφάλεια του Διαδικτύου και Ασφάλεια στο Διαδίκτυο", *Η Καθημερινή,* 14 Νοε. 2013; www.kathimerini.gr/59717/article/epikairothta/ellada/synedrio-die8noys-panepisthmioy-me-8ema-thn-asfaleia-toy-diadiktyoy-kai-asfaleia-sto-diadiktyo [Προσπελάστηκε 09/12/2014]

[117] "Ασφάλεια στις Τηλεπικοινωνίες", *Υπουργείο Υποδομών, Μεταφορών και Δικτύων*; www.yme.gr/index.php?tid=1581 [Προσπελάστηκε 09/12/2014]

[118] "Σεμινάριο για την ασφαλή πλοήγηση και εξάρτηση των εφήβων από το Διαδίκτυο στο Βόλο", *ΚΕΘΕΑ ΣΤΡΟΦΗ*; www.kethea-strofi.gr/article.php?id=816 [Προσπελάστηκε 09/12/2014]

[119] "Ασφαλής πλοήγηση και εξάρτηση των νέων από το Διαδίκτυο", *ΚΕΘΕΑ ΣΤΡΟΦΗ*; www.kethea-strofi.gr/article.php?id=863 [Προσπελάστηκε 09/12/2014]

[120] "Δημαρχείο Κορωπίου: Ημερίδα με θέμα την Ασφάλεια στο Διαδίκτυο", *newsbomb,* 29 Σεπτ. 2014; www.newsbomb.gr/ellada/news/story/500660/dimarheio-koropioy-imerida-me-thema-tin-asfaleia-sto-diadiktyo [Προσπελάστηκε 09/12/2014]

[121] "*Ημερίδα για την Ασφάλεια στο Διαδίκτυο*", Ιερά Μητρόπολις Αλεξανδρουπόλεως, 10 Οκτ. 2014; www.imalex.gr/A70D1DC3.el.aspx [Προσπελάστηκε 09/12/2014]

[122] Ημερίδα με θέμα την Ασφάλεια στο Διαδίκτυο και την καλή χρήση της Τεχνολογίας", *trikalanews;* www.trikalanews.gr/biz/event/asfaleia-diadiktio.html [Προσπελάστηκε 10/12/2014]

[123] Κ. Μαχαίρας, *"Εθισμός στο Διαδίκτυο"*, ΝΕΡΙΤ; http://195.211.203.105/details.asp?pid=3414973&chid=9 [Προσπελάστηκε 11/12/2014]

[124] Νέοι Φάκελοι, "Οι κίνδυνοι στο Internet", *YouTube,* 4 Φεβρ. 2009; https://www.youtube.com/watch?v=ZNp1iC38WL0 [Προσπελάστηκε 11/12/2014]

[125] Ελληνική Αστυνομία, "Ασφάλεια στο Διαδίκτυο – Cyber Bulling", *YouTube,* 8 Ιουλ. 2011; https://www.youtube.com/watch?v=gEPUGRiP7IM [Προσπελάστηκε 11/12/2014]

[126] Μονάδα Εφηβικής υγείας (Μ.Ε.Υ.), "Νέο τηλεοπτικό σποτ για την ασφάλεια στο Διαδίκτυο", *YouTube, 18 Σεπτ. 2014;* https://www.youtube.com/watch?v=hwU-3h-Vvpg [Προσπελάστηκε 11/12/2014]

[127] Κοινωνικό Σχολείο; http://socialschool.gr/page/about [Προσπελάστηκε 20/12/2014]

[128] "Countries: Greece", *Ins@fe: Safer Internet;* www.saferinternet.org/greece [Προσπελάστηκε 14/12/2014]

[129] "About Ins@fe", *Ins@fe: Safer Internet;* www.saferinternet.org/about [Προσπελάστηκε 13/12/2014]

[130] "Ποιοι είμαστε", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?parentobjId=Page74 [Προσπελάστηκε 13/12/2014]

[131] "Ποιοί είμαστε-Σκοπός μας", *Ελληνική Γραμμή για το Παράνομο Περιεχόμενο στο Διαδίκτυο;* www.safeline.gr/poioi-eimaste/skopos-mas [Προσπελάστηκε 13/12/2014]

[132] "Countries: Greece", *Ins@fe: Safer Internet;* www.saferinternet.org/greece [Προσπελάστηκε 14/12/2014]

[133] "At A Glance", *International Association Of Internet Hotlines (INHOPE);* www.inhope.org/gns/who-we-are/at-a-glance.aspx [Προσπελάστηκε 14/12/2014]

[134] "Γραμμή Βοηθείας Ελληνικού Κέντρου Ασφαλούς Διαδικτύου", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/helpline [Προσπελάστηκε 15/12/2014]

[135] Μονάδα Εφηβικής υγείας (Μ.Ε.Υ.): Γραμμή Βοηθείας ΥποΣΤΗΡΙΖΩ; http://youth-health.gr/drastiriotites/grammi-boitheias-upostirizo/grammi-boitheias-upostirizo.1#.VJIkbWcYv6Y [Προσπελάστηκε 15/12/2014]

[136] "Countries: Greece", *Ins@fe: Safer Internet;* www.saferinternet.org/greece [Προσπελάστηκε 14/12/2014]

[137] Ασφάλεια στο Διαδίκτυο: Ενημερωτικός Κόμβος πανελλήνιου Σχολικού Δικτύου; http://internet-safety.sch.gr/ [Προσπελάστηκε 15/12/2014]

[138] Ασφάλεια στο Διαδίκτυο, "Όροι χρήσης", *Ασφάλεια στο Διαδίκτυο: Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου*, 28 Σεπτ. 2012; http://internet-safety.sch.gr/index.php/inform/terms [Προσπελάστηκε 16/12/2014]

[139] Ασφάλεια στο Διαδίκτυο: Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου; http://blogs.sch.gr/internet-safety [Προσπελάστηκε 16/12/2014]

[140] Πανελλήνιο Σχολικό Δίκτυο; www.sch.gr/ [Προσπελάστηκε 18/12/2014]

[141] "Aims of the Hellenic Association for the Study of Internet Addiction Disorder", *Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο: hasiad;* www.hasiad.gr/ [Προσπελάστηκε 18/12/2014]

[142] "Ποιοι είμαστε", *Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο: hasiad;* www.hasiad.gr/index.php?option=com_content&view=article&id=2&Itemid=2&lang=el [Προσπελάστηκε 18/12/2014]

[143] International Association of CyberPsychology, Training, and Rehabilitation (iACToR); http://iactor.ning.com/page/affiliated-societies [Προσπελάστηκε 18/12/2014]

[144] Μονάδα Εφηβικής υγείας (Μ.Ε.Υ.): Τμήμα Ασφαλούς Διαδικτύου (ΤΑΔ); http://youth-health.gr/drastiriotites/ekpaideusi/tmima-asfalous-diadiktuou-tad#.VIoXz8ln_ls [Προσπελάστηκε 19/12/2014]

[145] "Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος", *Ελληνική Αστυνομία: Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης*; www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang [Προσπελάστηκε 19/12/2014]

[146] Cyberkid; www.cyberkid.gov.gr/about.html [Προσπελάστηκε 19/12/2014]

[147] "Συμβουλές για τους Γονείς", *Ελληνική Αστυνομία: Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης;* www.astynomia.gr/index.php?option=ozo_content&perform=view&id=322&Itemid=86&lang [Προσπελάστηκε 21/12/2014]

[148] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για Μπαμπάδες και Μαμάδες, για Παππούδες και Γιαγιάδες", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File483 [Προσπελάστηκε 21/12/2014]

[149] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για τους Μαθητές", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File382 [Προσπελάστηκε 21/12/2014]

[150] "Έρευνα: Προώθηση της Ασφαλούς Χρήσης του Διαδικτύου στο Σχολείο - Η Άποψη των Εκπαιδευτικών", Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, 15 Σεπτ, 2009; www.saferinternet.gr/index.php?action=download&objId=File342 [Προσπελάστηκε 21/12/2014]

[151] "Ασφαλής Χρήση του Διαδικτύου: Συνοπτικός Οδηγός για τους Εκπαιδευτικούς", *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*, 2012*;* www.saferinternet.gr/index.php?action=download&objId=File379 [Προσπελάστηκε 21/12/2014]