ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ
PROJECT

<u>Θέμα: Το διαδίκτυο στη ζωή μας</u>

Α΄ ΛΥΚΕΙΟΥ
ΓΥΜΝΑΣΙΟ – ΛΤ. ΑΓΡΑΣ ΛΕΣΒΟΥ

ΣΧΟΛΙΚΟ ΕΤΟΣ 2013 - 2014

ΠΕΡΙΕΧΟΜΕΝΑ

Μέρος 1ο: Η ΙΣΤΟΡΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο αποτελεί σήμερα ένα από τα πλέον διαδεδομένα μέσα επικοινωνίας, ανταλλαγής και εύρεσης πληροφοριών, αλλά και χώρο εργασίας για αυτόνομες μονάδες ατόμων και επιχειρήσεις.Ο όρος διαδίκτυο και ευρέως γνωστός με την αγγλική λέξη **internet (inter-network)**, αναφέρεται για να περιγράψει ένα σύνολο διασυνδεμένων υπολογιστών, όπου επικοινωνούν μεταξύ τους παρέχοντας πληροφορίες και υπηρεσίες στους χρήστες. Ο όρος διαδίκτυο στην περισσότερο χρησιμοποιημένη του μορφή σήμερα, δηλώνει ένα παγκόσμιο δίκτυο υπολογιστών (Wikipedia, 2008).

Εικόνα 1: Υπολογιστής σαν αυτούς που συνδέονταν στο ARPANET

Η σημερινή και ευρέως γνωστή μορφή του διαδικτύου απέχει κατά πολύ από την αρχική, καθώς και από την αρχική ιδέα δημιουργίας του. Το διαδίκτυο ξεκίνησε ως ιδέα δημιουργίας ενός δικτύου στα μέσα της δεκαετίας του 1960. Δεδομένου ότι η εποχή εκείνη ήταν ψυχροπολεμική, το Υπουργείο Αμύνης των Η.Π.Α, προσπαθούσε να δώσει λύση στο πρόβλημα της κατασκευής ενός συστήματος τηλεπικοινωνιών , όπου θα ήταν ανθεκτικό στις ενδεχόμενες πολεμικές καταστροφές.

Κάτω από αυτές τις συνθήκες ξεκίνησαν οι μελέτες για ένα τηλεπικοινωνιακό σύστημα, το οποίο θα συνέχιζε να λειτουργεί σε περίπτωση καταστροφής κάποιου μέρους των κέντρων και των γραμμών επικοινωνίας (Τσιμπινός, 2008).

1. ARPANET

Στα πλαίσια της μελέτης αυτής δημιουργήθηκε η ομάδα ARPA (Advanced Research Project Agency), που αργότερα ονομάσθηκε **DAPRA** (Defense Advance Project Agency), η οποία κατασκεύασε το ARPANET το οποίο ήταν η πρώτη μορφή του σημερινού internet. (Wikipedia, 2008).

Εικόνα 2: Οι πρώτοι κόμβοι του ARPANET

Η βασική ιδέα της ομάδας των (J. C. R. Licklider, Bolt Beranek και Newman), (Wikipedia, 2008) ήταν η δημιουργία ενός δικτύου υπολογιστών όπου θα επικοινωνούσαν μεταξύ τους με την μέθοδο της μεταγωγής πακέτων (packet-switching). Κάθε μήνυμα κοβόταν σε μικρά πακέτα, που περιείχαν τα στοιχεία του παραλήπτη και του αποστολέα, έναν διαφορετικό τρόπο επικοινωνίας που βασιζόταν στο γεγονός ότι μία σύνδεση θα μπορεί να εξυπηρετεί παραπάνω από μία μηχανή. (webopedia, 2008) Η ιδέα για το μετέπειτα internet γίνεται πράξη το 1969, όταν τέθηκε σε εφαρμογή ο πρώτος διαδικτυακός κόμβος με την ονομασία ARPANET, ο οποίος μέχρι τα τέλη του ΄69 έφτασε να εξυπηρετεί τέσσερις κόμβους: UCLA (30 Αυγούστου), Stanford Research Institute (SRI) (1 Οκτωβρίου), University of California Santa Barbara (UCSB) (1 Νοεμβρίου), University of Utah (Δεκέμβριος).

Στα πρώτα στάδια του ARPANET συνδέονταν μεταξύ τους ερευνητές από το στρατό, τα πανεπιστήμια ή τις εταιρίες, που συμμετείχαν στις στρατιωτικές έρευνες. Ενώ βρισκόντουσαν σε απομακρυσμένα μεταξύ τους υπολογιστικά κέντρα, μπορούσαν μέσα από το δίκτυο να μοιράζονται προγράμματα, βάσεις δεδομένων, αλλά ακόμη και σκληρούς δίσκους υπολογιστών. Από το τέλος όμως της δεκαετίας το 1970, οι χρήσεις του δικτύου άνοιξαν σε μη στρατιωτικές εφαρμογές, οι οποίες γίνονταν σε πανεπιστήμια κι αργότερα σε επιχειρήσεις.

Μετά όμως από δέκα περίπου χρόνια, διαρκών πειραματισμών και εισαγωγής νέων καινοτομιών, το αρχικό πρόγραμμα του ARPANET διογκώθηκε τόσο πολύ, ώστε στις αρχές του 1980 έπρεπε να χωρισθεί σε δύο τμήματα, τα οποία επικοινωνούσαν αποκομμένα μεταξύ τους.

Το ένα τμήμα ήταν αποκλειστικά αφιερωμένο σε στρατιωτικές χρήσεις και ονομαζόταν **Milnet**. Το άλλο τμήμα, που περιλάμβανε όλες τις υπόλοιπες χρήσεις, αρχικά ονομάσθηκε **DARPA Internet**, για να επικρατήσει τελικά με την πάροδο του χρόνου η σύντομη ονομασία Internet (Τσιμπινός, 2008).

2. NSFNET

Μια από τις σημαντικότερες εξελίξεις στην ιστορία του Internet οφείλεται στην πρωτοβουλία του **NSF (National Science Foundation)**, κυβερνητικής υπηρεσίας των ΗΠΑ, να δημιουργηθούν στο μέσο της δεκαετίας του 1980 πέντε μεγάλα κέντρα υπολογιστών (super computer centers). Ουσιαστικά, ως τότε η πρόσβαση στους μεγαλύτερους υπολογιστές του κόσμου περιορίζετε στο στρατό και σε λίγους ακόμη συνεργαζόμενους με αυτόν ερευνητές. Το άνοιγμα των χρήσεων των υπερυπολογιστών στην ευρύτερη ακαδημαϊκή κοινότητα έγινε από το NSF μόνο σε πέντε κέντρα, γιατί τα σχετικά έξοδα ήταν τεράστια. Για το σκοπό αυτό, για την ικανοποίηση της ανάγκης κατανομής των πόρων στα πέντε κέντρα, το NSF έφτιαξε το 1986 το δίκτυο NSFNET, χρησιμοποιώντας την τεχνολογία του **ARPANET**. Το NSFNET επέτρεπε τη σύνδεση των πέντε κέντρων μεταξύ τους αλλά και τη σύνδεση με αυτά ερευνητών από διάφορα ιδρύματα των ΗΠΑ. Βαθμιαία έτσι, το NSFNET άρχισε να αντικαθιστά το ARPANET στις επιστημονικές διασυνδέσεις, μέχρι το Μάρτιο του 1990, οπότε το ARPANET διαλύθηκε επισήμως.

Από τα μέσα λοιπόν της δεκαετίας του 1980 το NSFNET αποτελούσε τη ραχοκοκαλιά του Internet. Από τότε κι έπειτα, οι ρυθμοί αύξησης του Internet πολλαπλασιάζονταν εκθετικά. Η είσοδος του NSF ακολουθήθηκε από τη συμμετοχή στο Internet μεγάλων κυβερνητικών υπηρεσιών των ΗΠΑ, όπως το Υπουργείο Ενεργείας (U.S. Department of Energy) και η NASA (National Aeronautics and Space Administration). Επίσης, τότε στα μέσα της δεκαετίας του 80 εισήλθαν στο Internet τα πρώτα μεγάλα διεθνή τοπικά δίκτυα χωρών εκτός των ΗΠΑ (Τσιμπινός, 2008, NSF,2008, Wikepedia,2008).

3. ΠΡΩΤΟΚΟΛΛΟ TCP/IP

Το κυριότερο πρωτόκολλο που χρησιμοποιεί το internet είναι το **TCP(Internet protocol suite)**. Πρωτόκολλο το οποίο αργότερα χωρίστηκε σε δύο τομείς το TCP και IP (Σουίτα Πρωτοκόλλων Διαδικτύου), μια συλλογή από πρωτόκολλα επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Λόγω επικράτησης των δύο κυριότερων πρωτοκόλλων, είναι γνωστό με την συντομογραφία **TCP/IP Transmission Control Protocol** (Πρωτόκολλο Ελέγχου Μετάδοσης) και το **IP** ή **Internet Protocol** (Πρωτόκολλο Διαδικτύου, World Wide Web) (Wikipedia, 2008).

Πολλοί πιστεύουν πως το **internet** και ο παγκόσμιος ιστός είναι ή ίδια έννοια με διαφορετικές λέξεις, όμως είναι δύο διαφορετικά πράγματα, αφού το internet αποτελεί το σύνολο όλων των δικτύων υπολογιστών. Ενώ ο παγκόσμιός ιστός είναι υποσύνολο του και εμφανίστηκε ως έννοια πολύ αργότερα (RAM 2007).

Ο πρώτος **web server** (1990) ! Το 1990 το internet μπαίνει σε μια νέα εποχή με τον σχεδιασμό του παγκόσμιου ιστού από τον Tim Berners Lee στο ερευνητικό κέντρο CERN στην Γενεύη (Τσιμπίνος, 2008).

Η πρόταση του αφορούσε την ανταλλαγή πληροφοριών για την συνεργασία μεταξύ φυσικών και άλλων ερευνητών στην ενεργειακή κοινότητα των φυσικών, μέσω του διαδικτύου σε πραγματικό χρόνο.

Η πρόταση έγινε πραγματικότητα μέσω τριών τεχνολογιών που ενσωματωθήκαν. Η **HTML (Hyper Text Markup Language)** για την εγγραφή web σελίδων, το HTTP (Hyper

Text Transfer Protocol) για την μετάδοση των σελίδων, ένας web browser και ένα λογισμικό πρόγραμμα για να ερμηνεύει και εμφανίζει τα δεδομένα.

Με αυτά τα μέσα γεννήθηκε το **WWW (World Wide Web)**. Με την πρώτη ανταλλαγή του κειμένου μεταξύ των επιστημόνων έχουμε και την πρώτη μορφή web design (Wikipedia, 2008, Innervisions, 2008).

Μέρος 2ο: ΚΑΤΗΓΟΡΙΕΣ ΙΣΤΟΣΕΛΙΔΩΝ ΠΟΥ ΥΠΑΡΧΟΥΝ ΣΗΜΕΡΑ ΔΙΑΘΕΣΙΜΕΣ ΓΙΑ ΤΟΥΣ ΧΡΗΣΤΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στο χώρο το internet υπάρχουν διάφορες κατηγορίες ιστοσελίδων για να ενημερωθείς, να ψυχαγωγηθείς, να επικοινωνήσεις να πάρεις μέρος σε παιχνίδια, σε δημοψηφίσματα κι άλλα. Επίσης μπορείς να κάνεις έξυπνες και οικονομικές αγορές ρούχων, αντικειμένων ή και μέσων μεταφοράς. Οι κατηγορίες κατατάσσονται ως εξής:

Αθλητισμός όπου μπορείς να βρεις πληροφορίες σχετικά με όλα τα αθλήματα, όπως ποδόσφαιρο, μπάσκετ, βόλεϊ κι άλλα. Επίσης, μπορείς να ενημερωθείς για τις βαθμολογίες ή και να διαβάσεις αθλητικές εφημερίδες. Κάποια site που βρήκαμε περί αθλητισμού είναι τα εξής: novasports.gr, redplanet.gr,olapaok.gr,gazzeta.gr, aek36.com, leoforos.gr.

Επόμενη κατηγορία είναι τα **μέσα μεταφοράς**: anytimeonline.gr όπου μπορείς να δεις διάφορα αυτοκίνητα, μηχανάκια, φορτηγά κι άλλα, σε κάποια site μπορείς να τα αγοράσεις. Επίσης μπορείς σε συγκεκριμένο site να κάνεις ασφάλεια αυτοκινήτου. Κάποια site είναι: car.gr,alfaromeo.gr,autoblog.gr,asfalistra.gr, drive.gr moto.gr anytimeonline.gr.

Διασκέδαση και ψυχαγωγία: gossiptv.gr Home,Lifestyle,Showbiz,G-sports,Media,G-fashion,Astrology,Celebrities. Σε αυτές τις κατηγορίες μπορείς να βρείς κυρίως κουτσομπολίστικα περιοδικά. Το κάθε περιοδικό έχει τη δική του σελίδα. κά, Σε διάφορες σελίδες βρίσκεις διάφορα τεστ: αισθηματικά, ερωτικά, συναισθηματικά και προσωπικότητας κι άλλα πολλά. Επίσης μπορείς να παίξεις παιχνίδια: περιπέτειας, σκέψης, δράσης, αθλητικά κι άλλα. Κάποια site είναι: games.gr, yupiii.gr, gameover.gr, zoo.gr, athinorama.gr.

Άλλη κατηγορία είναι οι **ειδήσεις** και **Μ.Μ.Ε**: alphatv,gr, εκπομπές, πρόγραμμα, web tv, Alpha News, Social Live, καιρός, Alpha 989 οπου διαβάζεις ολες τις εφημερίδες και

βλέπεις νέα από το χωριό σου,το νήσι σου,την πόλη σου,την χώρα σου και για όλο τον κόσμο.

Επίσης έχει online όλα τα **τηλεοπτικά κανάλια** και μπορείς να ενημερωθείς για το προγράμμα του καναλιού που σε ενδιαφέρει ή να παρακολουθήσεις τις εκπομπές που θέλεις ξανά. Κάποια site είναι: yahoo.com, Newsit, NewsBOMB.gr, Εθνος Online, Θέμα, in.gr zougla.gr, tovima.gr, tanea.gr, protothema.gr, tovima.gr alphatv.gr.

Επόμενη κατηγορία είναι **εργασία** και **εκπαίδευση**: Alfavita.gr, Εκπαίδευση, Πολιτική, Κοινωνία, Εργασία, Επιμόρφωση, Πανελλήνιες, Αρθρα, Επιστήμη, Χρήσιμα, Χρήστες οπου μπορεί κάποιος να ενημερωθεί για θέματα που αφορούν τους εκπαιδευτικούς, τους φοιτητές, τους μαθητές και γενικότερα να πληροφορηθεί για το εκπαιδευτικό σύστημα. Επιπλέον, θα μπορούσε κάποιος να γνωρίσει σχετικά με τον **επαγγελματικό προσανατολισμό** και την **αγορά εργασίας**. Επιπροσθέτως,θα μπορούσαν να βρεθούν μέσα από αυτές τις κατηγορίες τρόποι αντιμετώπισης της ανεργίας.Οι ιστοσελίδες της παραπάνω κατηγορίας είναι: alfavita.gr, kareira.gr, ipaideia.gr, uoi.gr, diorismos.gr, bookbook.gr, fititis.gr.

Επιστήμη και τεχνολογία είναι η κατηγορία όπου μας ενημερώνει για τον τρόπο με τον οποίο εξελλίσσεται η τεχνολογία στην σημερινή εποχή αλλά ακόμη, παρουσιάζονται και πολλά τεχνολογικά επιτεύγματα .Στην κατηγορία αυτή αναφέρεται το παρακάτω site: ftiaxno.gr. Επιπλέον, μια κατηγορία ακόμη είναι οι **επιχειρήσεις** και **οικονομία** που σχετίζονται με τις διαθέσιμες επιχειρήσεις για εργασία, για την οικονομία των κρατών γενικότερα αλλά και για την οικονομία της ίδιας της χώρας μας.

Ακόμη,υπάρχει μια κατηγορία που αναφέρεται στα **καταστήματα** και τις **αγορές**. Σε αυτή την κατηγορία μπορεί κάποιος να παραγγείλει μέσω του ηλεκτρονικού του υπολογιστή διάφορα αντικείμενα π.χ ρούχα είτε παπούτσια. Ακόμη διάφορα ηλεκτρικά είδη και σύμφωνα με τα τωρινά δεδομένα,θα μπορούσε κάποιος να διαλέξει από κάποιο super market κάποια προϊόντα τα οποία μάλιστα θα μεταφερθούν στο σπίτι του. Οι ηλεκτρονικές σελίδες για αυτή την κατηγορία είναι: e -shop.gr, ikea.gr, skroutz.gr, ntynomai.gr, e-bay.gr.

Κοινωνία είναι μια κατηγορία όπου αναφέρεται σε κοινωνικά δίκτυα και διάφορες ψυχαγωγικές σελίδες όπως σε όπως astrology.gr facebook.com.

Κράτος και οργανισμοί, μια κατηγορία όπου μπορείς να βρείς sites σχετικά με διάφορους οργανισμούς όπως: oaed.gr:,astynomia.gr: Υπηρεσίες, Τύπος και Μ.Μ.Ε,

Οδηγός του πολίτη, Στατιστικά στοιχεία, Δημόσια Δεδομένα, Αστυνομική Ακαδημία, Κοινωνικές δράσεις, Μετανάστευση, ,.diavgeia.gr, .minedu.gr: ika.gr minedu.gr:, ika.gr: Επίσης, **σπίτι και οικογένεια** ένα site που μπορείς να διαβάσεις περιοδικά και άρθρα σχετικά με την οικογένεια,την μητρότητα και την πατρότητα,μπορείς κιόλας να βρείς σελίδες μαγειρικής,μερικά site είναι:parents.gr, sintagoulis.gr.

Εργαλεία.Ταξίδια και τουρισμός μια κατηγορία που περιέχει χιλιάδες sites με τουριστικά αξιοθέατα διάφορες εκδηλώσεις και πολλές σχετικές πληροφορίες. Ακόμη, μπορείς να βρείς **τις τιμές των εισιτηρίων** για οποιαδήποτε διαδρομή και ακόμη να κλείσεις και εισητήρια.: aegeanair.com, airfasttickets.gr, skyscanner.gr, pamediakopes.gr καθώς και πληροφορίες για **ξενοδοχεία** και **ενοίκιαση αυτοκινήτου**,

Τέχνες και πολιτισμός, εδώ , μπορείς να βρείς θέματα σχετικά με την γλώσσα μας, τα έθιμα μας, την κουλτούρα μας ή και ακόμη **στίχους και ποιήματα**,κάποια sites είναι greek-language.gr stixoi.info.Τέλος, **υγεία και ομορφιά**. Σε αυτή τη κατηγορία υπάρχουν sites σχετικά με τον καλλωπισμό και την μόδα και επίσης σελίδες που μας ενημερώνουν για **ασθένειες** και πώς να προφυλαχτούμε από αυτές, κάποιες σελίδες είναι:vita.gr: Υγεία, Διατρόφη, Δίαιτα, Ομορφιά, Ψυχολογία, Fithess, Παιδί, Go Green, Body and Mind, marieclaire.gr.

Μέρος 3ο: ΚΙΝΔΥΝΟΙ ΠΟΥ ΕΓΚΥΜΟΝΟΥΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΓΙΑ ΤΟΥΣ ΧΡΗΣΤΕΣ

Ενημέρωση, ψυχαγωγία, διασκέδαση, παιχνίδια, φλέρτ, διαπροσωπικές σχέσεις, έχουν περάσει για τα καλά στη σφαίρα του διαδικτύου. Ποιος δεν ανοίγει τον ηλεκτρονικό του υπολογιστή για να ενημερωθεί από κάποιο διαδικτυακό μέσο, να ψυχαγωγηθεί ακούγοντας τραγούδια, ή βλέποντας ταινίες, να μιλήσει σε κάποιο φιλικό του πρόσωπο με **e-mail** και βιντεοκλήση, να κάνει “like” και “comment” στο **facebook**, ή “retweet” στο twitter; Η χρήση του internet διευρύνεται και διεσδύει σε όλες τις ηλικιακές ομάδες. Περισσότερο εξοικειωμένοι όμως είναι τα παιδιά και οι έφηβοι, όπου τα σημάδια εθισμού από την παράχρηση του διαδικτύου αρχίζουν και εμφανίζονται ανησυχώντας τους ειδικούς. Όπως επίσης τους ανησυχούν και οι κίνδυνοι που «παραμονεύουν» σε πολλές γωνιές του ψηφιακού «παράλληλου σύμπαντος». Το «μίτο» των κινδύνων του διαδικτύου

για τα παιδιά και τους εφήβους επιχειρεί να ξετυλίξει το πρόγραμμα «Αριάδνη» που υλοποιεί το Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών με την επιστημονική ευθύνη της Μονάδας Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής Πανεπιστημίου Αθηνών, του Νοσοκομείου Παίδων «Π. & Α. Κυριακού».

Η έρευνα του προγράμματος «Αριάδνη» για τον εθισμό από το διαδίκτυο διεξήχθη με τη σύμπραξη 7 Ευρωπαϊκών χωρών (Ελλάδα, Γερμανία, Ισπανία, Πολωνία, Ισλανδία, Ολλανδία, Ρουμανία) στο πλαίσιο του προγράμματος Safer Internet. Το αντιπροσωπευτικό δείγμα ήταν έφηβοι 15-16 ετών σε κάθε χώρα, συμπληρώθηκαν 2.000 ερωτηματολόγια σε κάθε χώρα (συνολικά 14000 ερωτηματολόγια) και πραγματοποιήθηκαν 20 συνεντεύξεις εφήβων με score διαδικτυακής εξάρτησης στο σχετικό εργαλείο ανά χώρα (140 συνεντεύξεις συνολικά). Την ανακοίνωση των στοιχείων που προέκυψαν από την έρευνα παρουσίασε επιστημονική ομάδα του προγράμματος «Αριάδνη. Βασική παράμετρος της έρευνας ήταν η διαπίστωση του βαθμού **εξάρτησης** των εφήβων από το διαδίκτυο. Ως συμπεριφορά εξάρτησης από το διαδίκτυο ορίζεται η συμπεριφορά που χαρακτηρίζεται από απώλεια ελέγχου σχετικά με τη χρήση του διαδικτύου με αποτέλεσμα την παραμέληση βασικών πτυχών της καθημερινότητας (σχολικές υποχρεώσεις, δραστηριότητες-χόμπι, φιλικές σχέσεις, φλερτ, σωματική φροντίδα και υγιεινή).

Εθισμός στο Διαδίκτυο

Ο εθισμός στο Διαδίκτυο (**internet addiction**) μια σχετικά νέα μορφή εξάρτησης, προτάθηκε ως όρος πρώτη φορά από τον Goldberg (1995) και έγινε δημοφιλής με την καινοτόμο έρευνα της Young (1996), αναφέρεται στην «καταναγκαστική, υπερβολική χρήση του διαδικτύου και τον εκνευρισμό ή δυσθυμική συμπεριφορά που παρουσιάζεται κατά τη στέρησή της» (Mitchell, 2000). Ο εθισμός στο Διαδίκτυο αν και δεν έχει επισήμως αναγνωρισθεί ως κλινική οντότητα παρά μόνο σε Κίνα, Ν.Κορέα και Ταιβάν, αποτελεί μια κατάσταση, που προκαλεί σημαντική έκπτωση στην κοινωνική και επαγγελματική ή ακαδημαϊκή λειτουργικότητα του ατόμου. Οι ειδικοί της ψυχικής υγείας όλο και συχνότερα καλούνται, να προσεγγίσουν θεραπευτικά άτομα με προβληματική χρήση του Διαδικτύου. Ήδη στην επόμενη έκδοση του διαγνωστικού εγχειριδίου της Αμερικανικής Ψυχιατρικής Εταιρείας, DSM-V, θα συμπεριληφθεί ως χρήζουσα περισσότερη έρευνα η οντότητα "**Internet Use Gaming Disorder**", ένας όρος που δεν έχει χρησιμοποιηθεί σε έρευνες ως σήμερα. Συνηθέστερη ορολογία πέρα από τον εθισμό στο Διαδίκτυο (**Internet Addiction Disorder - IAD**) είναι επίσης οι "Pathological Internet Use" (Παθολογική χρήση του

διαδικτύου)», "Problematic Internet Use" (Προβληματική χρήση του διαδικτύου), "Excessive Internet Use" (Υπερβολική χρήση του διαδικτύου) και "Compulsive Internet Use" (Καταναγκαστική χρήση του διαδικτύου) (Widyanto & Griffiths, 2006).

- 1.2% του συνολικού δείγματος παρουσιάζει συμπεριφορές εξάρτησης και 12,7% οριακή διαδικτυακή συμπεριφορά (13.9% δυσλειτουργική διαδικτυακή χρήση)
- Οι διαφορές μεταξύ των χωρών δεν είναι σημαντικές, ωστόσο μεγαλύτερα ποσοστά παρουσιάζονται σε Ρουμανία, Ελλάδα και Ισπανία ενώ τα μικρότερα σε Ισλανδία, Ολλανδία και Γερμανία
- Τα ποσοστά εξάρτησης παρουσίαζαν τάση ανόδου στα αγόρια, στις μεγαλύτερες ηλικίες και στο χαμηλότερο μορφωτικό επίπεδο γονέων
- Υπήρχαν ψυχοκοινωνικές δυσκολίες στην ομάδα των εξαρτημένων εφήβων (χαμηλή κοινωνικότητα, διάσπαση προσοχής, καταθλιπτικό συναίσθημα κ.α.)
- 63% των εφήβων επικοινωνούν με αγνώστους on-line
- 9,3% από αυτούς αναφέρουν ότι αυτό τους έβλαψε (5,4% του συνολικού δείγματος)
- 45,7% από αυτούς συνάντησαν στο φυσικό κόσμο κάποιον που γνώρισαν μέσω διαδικτύου (28.4% του συνολικού δείγματος)
- Οι χώρες με τα μεγαλύτερα ποσοστά κινδύνου διαδικτυακής αποπλάνησης ήταν οι Ρουμανία, Γερμανία και Πολωνία, ενώ η Ελλάδα είχε το μικρότερο ποσοστό
- 58.8% του δείγματος εκτέθηκαν σε πορνογραφικό υλικό (32,8% από αυτούς αναφέρουν ότι ενοχλήθηκαν από την έκθεση σε πορνογραφικό υλικό – 18,4% του δείγματος)
- Τα αγόρια παρουσίαζαν μεγαλύτερα ποσοστά έκθεσης σε πορνογραφικό υλικό, ενώ οι διαφορές των χωρών δεν ήταν σημαντικές
- 21.9% έχει δεχθεί διαδικτυακό εκφοβισμό (53.5% από αυτούς ανέφεραν ότι αυτό τους έβλαψε)
- Τα κορίτσια παρουσίαζαν μεγαλύτερα ποσοστά έκθεσης σε διαδικτυακό εκφοβισμό, ενώ οι χώρες με τα μεγαλύτερα ποσοστά ήταν οι Ρουμανία και Ελλάδα και τα μικρότερα οι Ισλανδία και Ισπανία

• 92% των εφήβων της μελέτης είναι μέλη σε κοινωνικά δίκτυα

• 39.4% κάνει χρήση των κοινωνικών δικτύων περισσότερο από 2 ώρες την καθημερινή ημέρα. Το ποσοστό αυτό ανεβαίνει στο 60,2% τα Σαββατοκύριακα και τις αργίες

• Το 25% των εφήβων που κάνουν χρήση κοινωνικών δικτύων περισσότερο από 2 ώρες ημερησίως, μπορεί να παρουσιάσουν συμπεριφορά εξάρτησης, ενώ το αντίστοιχο ποσοστό για χρήση κάτω των 2 ωρών είναι 8% ($p<0.001$)

• Περισσότεροι από 600 περίπου διαδικτυακοί φίλοι μπορεί να συσχετιστούν με συμπεριφορές εξάρτησης

• Η τάση αυτή αφορά και τα δύο φύλα, με μικρή υπεροχή των κοριτσιών

• 61,8% του δείγματος παίζουν Διαδικτυακά Παιχνίδια

• Οι έφηβοι που παίζουν διαδικτυακά παιχνίδια παρουσιάζουν διπλάσια πιθανότητα συμπεριφορών εξάρτησης

• Η ενασχόληση για περισσότερο από 2,6 ώρες την ημέρα συσχετίστηκε με εμφάνιση συμπεριφορών εξάρτησης

• Αυτή η τάση αφορά κυρίως στα αγόρια

• 10,6% των εφήβων του δείγματος ασχολούνται με τζόγο στο φυσικό κόσμο, ενώ το 5,9% ασχολείται με το τζόγο στο διαδίκτυο

• Οι έφηβοι που ασχολούνται με τον διαδικτυακό τζόγο έχουν τριπλάσια πιθανότητα εμφάνισης συμπεριφορών εξάρτησης

• Αυτή η τάση αφορά κυρίως στα αγόρια

• Η συμμετοχή σε Κοινωνικά Δίκτυα, Διαδικτυακά Παιχνίδια και Τζόγο είναι διαδικτυακές δραστηριότητες που σχετίζονται με συμπεριφορές εξάρτησης

• Η μεγαλύτερη πιθανότητα για συμπεριφορά εξάρτησης είναι στα παιδιά που ασχολούνται με τον τζόγο, ενώ ακολουθούν τα κοινωνικά δίκτυα και τα παιχνίδια.

Κίνδυνοι για εφήβους

Το διαδίκτυο έχει μπει πλέον για τα καλά στη ζωή μας σε σημείο που να μην είναι υπερβολή να μιλά κανείς για εθισμό, ιδιαίτερα των νέων σε ηλικία ανθρώπων. ΄Ομως πόσο χρήσιμη ή βλαβερή είναι αυτή η πρακτική; Το Πανεπιστήμιο Frederick, οργάνωσε σήμερα Τετάρτη, 2 Νοεμβρίου, επίκαιρη ημερίδα στην Αίθουσα Τελετών "Τάσσος Παπαδόπουλος" στις εγκαταστάσεις του στη Λευκωσία με θέμα "Εθισμός στο διαδίκτυο και άλλοι διαδικτυακοί κίνδυνοι". Το διαδίκτυο, είναι εφαρμογή που κάνει την πληροφορία προσβάσιμη. Με αυτή την έννοια, το διαδίκτυο αποτελεί μέσο εκδημοκρατισμού και παρέχει τη δυνατότητα στο σύνολο σχεδόν των χρηστών να έχουν πρόσβαση σε εξειδικευμένη γνώση και σε πολύ σύντομο χρονικό διάστημα να αξιοποιούν τεράστιο όγκο πληροφοριών, τόσο μεγάλο που συχνά δεν είναι εύκολο να τον διαχειριστεί κανείς. Παράλληλα το διαδίκτυο είναι μέσο επικοινωνίας ,διασκέδασης, εκπαίδευσης, ακόμα και συναλλαγής. Όλα αυτά επιτυγχάνονται με ταχύτητα και ελευθερία, αλλά αυτή η ελευθερία χρήσης και δημιουργίας κάνουν το διαδίκτυο τόπο πολλαπλού ενδιαφέροντος ακόμα και για κακόβουλη χρήση. Το ηλεκτρονικό έγκλημα , η υπεξαίρεση προσωπικών δεδομένων ,η διαβολή προσωπικοτήτων ,η διασπορά ψευδών πληροφοριών είναι φαινόμενα που ευδοκιμούν σε ένα τόσο ανοιχτό και διευρυμένο μέσο. Επιπλέον, η μεγάλη διεισδυτικότητά του στο κάθε νοικοκυριό πια, διαμορφώνει συνθήκες που μπορούν να εκθέσουν ευάλωτες ομάδες χρηστών σε νέους και άγνωστους κινδύνους. Από τον πρώτο εντυπωσιασμό στην κατάχρηση, για κάποιους η διαδρομή είναι ανησυχητικά σύντομη. Και έγκαιρα αυτή η ανησυχία στράφηκε στην κατανόηση των κινδύνων που ελλοχεύουν στην αλόγιστη χρήση του. Ήδη από τη μέση της δεκαετίας του 90 διαπιστώνεται πως υπάρχουν κίνδυνοι παθολογικής χρήσης του διαδικτύου. Σήμερα γνωρίζουμε πως ένα ποσοστό των χρηστών προσωπικού υπολογιστή με πρόσβαση στο διαδίκτυο θα θεωρηθούν εξαρτημένοι από αυτό. Νέα, ιδιότυπη εξάρτηση που συχνά εντοπίζεται δύσκολα, είναι όμως το ίδιο τραγική για τον εξαρτημένο. Η αιτιολογία της , η διάγνωσή της, η πρόληψή της, η αντιμετώπισή της, είναι πεδία που αποτελούν προτεραιότητες πρώτης γραμμής για όλους αυτούς που ασχολούνται με την κοινωνική φροντίδα ,την αγωγή υγείας, τη δημόσια ασφάλεια, τη δημόσια υγεία και την εκπαίδευση.

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψιάστου χρήστη είναι η μόλυνση του συστήματος με κάποιον **ιό.** Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο -φαινομενικά αθώο- αρχείο όπως ένα κείμενο ή μια φωτογραφία και όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση

επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστοτόπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη.

Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται **worm (=σκουλήκι)**. Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης.

Άλλος κίνδυνος είναι **ο Δούρειος Ίππος**, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

Οι κίνδυνοι βαθαίνουν στις περιπτώσεις επικοινωνίας με ανθρώπους άγνωστων προθέσεων. Οι κίνδυνοι αυτοί μπορεί να αποδειχθούν άμεσα ή έμμεσα επιβλαβείς, αλλά και να περιλαμβάνουν τους ίδιους τους νέους ως πρωταγωνιστές σε παράνομες και ανάρμοστες πράξεις. Σχεδόν κάθε μορφή κινδύνου που διατρέχει ένα παιδί στο φυσικό κόσμο, όπως ο εκφοβισμός, η σεξουαλική παρενόχληση και η αποπλάνηση, μεταφέρεται με παλαιούς και νέους όρους στο Διαδίκτυο.

Εξέλιξη αυτής της νέας δυνατότητας

Πολλά λέγονται για τον εθισμό που μπορεί κανείς να αποκτήσει, την εξάρτηση από το διαδίκτυο. Οι χρήστες καταναλώνουν όλο και περισσότερες ώρες μπροστά στον υπολογιστή τους και ίσως αυτός ο χρόνος να είναι εις βάρος της κλασικής επικοινωνίας που έχουμε συνηθίσει οι άνθρωποι.

Αν η τάση του ανθρώπου είναι αυτή, αν θέλει δηλαδή να επικοινωνεί με όλο τον κόσμο, χωρίς παράλληλα να σηκώνεται από την καρέκλα του, τότε είναι φανερό προς τα πού πηγαίνουν τα πράγματα. Κάποια στιγμή στο μέλλον όλοι οι άνθρωποι πλην των πρωτόγονων θα είναι συνδεδεμένοι διαδικτυακά και η σκέψη τους θα διασχίζει αστραπιαία τις ηπείρους και θα διαμορφώνει καταστάσεις και ιστορία.

Δεν μπορούμε φυσικά να φανταστούμε τίποτε πιο πέρα από αυτό, μόνο υποθέσεις μπορούμε να κάνουμε που βρίσκονται στη σφαίρα της επιστημονικής φαντασίας. Όπως

ότι ίσως κάποτε, στο μακρινό μέλλον, θα εγκαταλειφθεί ο φυσικός κόσμος στην πανίδα του και στη χλωρίδα του και ο άνθρωπος θα κλειστεί στο σπίτι του και θα επικοινωνεί με τους συνανθρώπους του διαδικτυακά. (Ο Ασίμωφ είχε γράψει κάτι παρόμοιο εδώ και πολλά χρόνια).

Αν στον πυρήνα του πολιτισμού που παράγει ο άνθρωπος υπάρχει ως «τέλος» (ως τελικός σκοπός) η απαλλαγή του από τα σωματικά δεσμά και η απελευθέρωση του πνεύματός του από την ύλη, τότε το διαδίκτυο είναι η πιο επιτυχημένη μέχρι στιγμής υλική εφεύρεση που προσφέρεται να μας εξαϋλώσει. Ας μην ξεχνάμε άλλωστε ότι οι ωραιότεροι και οι σημαντικότεροι μύθοι της ανθρωπότητας τόσο στη θρησκεία όσο και στη λογοτεχνία δείχνουν προς αυτή την κατεύθυνση.

Ψηφιακή Εποχή

Στην εποχή της ψηφιακής επανάστασης το Διαδίκτυο παίζει σημαντικό ρόλο στη ζωή του ανθρώπου, καθώς αποτελεί τον μεγαλύτερο παγκόσμιο κόμβο ως αναπόσπαστο κομμάτι της σύγχρονης κοινωνικής ζωής, μέσα από τον οποίο ενημερωνόμαστε, ψυχαγωγούμαστε, δραστηριοποιούμαστε, εργαζόμαστε, διευρύνουμε τους πνευματικούς ορίζοντές μας και καθετί άλλο στο σύνολο των καθημερινών ενασχολήσεων μας. Αναμφισβήτητα, υπάρχουν αναρίθμητα οφέλη από τη χρήση των νέων ψηφιακών μέσων. Είναι ένας ευχάριστος χώρος που παρέχει δυνατότητες διασκέδασης, πλούσια πληροφόρηση, άμεση και οικονομική επικοινωνία, είναι βολικό, εύκολα προσβάσιμο και επινοητικό και αποτελεί αναπόσπαστο κομμάτι της εκπαιδευτικής κοινότητας.

Παρόλα αυτά, το Διαδίκτυο ως υπερλεωφόρος πληροφοριών, ελέγχεται από τους χρήστες του. Οι πληροφορίες για θύματα και θύτες στον κόσμο του διαδικτύου κατακλύζουν καθημερινά την ειδησεογραφία. Και το χειρότερο είναι ότι θύτης και θύμα ταυτίζονται. Αυτό δεν αποτελεί λεκτική υπερβολή, καθώς στο Διαδίκτυο δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αρχή που να ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί, γιατί σύμφωνα με πολλούς χρήστες θα αποτελούσε είδος λογοκρισίας, καθώς επίσης οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες σε κάθε χώρα. Μέσω της δυναμικής εισβολής της ψηφιακής τεχνολογίας αναπτύσσονται τεράστιες δυνατότητες χρήσης και κατάχρησης. Παρά τις δυσκολίες όμως, νομικά, δεοντολογικά και ηθικά ζητήματα οδηγούν κρατικές υπηρεσίες, κρατικούς μηχανισμούς και αστυνομικές αρχές κάθε χώρας με αντίστοιχες

νομοθετικές ρυθμίσεις, στο να παρεμβαίνουν με σκοπό την δίωξη του ηλεκτρονικού εγκλήματος και αξιόποινων πράξεων που διαπράττονται μέσω διαδικτύου ή στο να παρεμβαίνουν στους παρόχους υπηρεσιών Διαδικτύου, υποχρεώνοντας τους να βάλουν φραγή σε επιλεγμένους διαδικτυακούς χώρους. Είναι λοιπόν μεγάλη η ευθύνη της πολιτείας δημιουργώντας μηχανισμούς ελέγχου και θεσπίζοντας σύγχρονες και αποτελεσματικές νομοθετικές ρυθμίσεις, να διασφαλίσει τη νόμιμη και ορθολογική λειτουργία του Διαδικτύου, χωρίς να θιχθεί η ελευθερία, αλλά παράλληλα είναι ευθύνη των πολιτών και ιδιαίτερα των γονέων με παιδιά να τα προστατεύσουν από την άλογη και παράνομη χρήση του Διαδικτύου.

Είναι κοινός τόπος πως υπάρχει η δυνατότητα αμφίδρομης επίδρασης στο Διαδίκτυο με το χρήστη. Αυτό οδηγεί στη δυνατότητα πρόκλησης ζημιών από κακόβουλους χρήστες τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο. Οι κίνδυνοι που καραδοκούν μικρούς και μεγάλους στο Διαδίκτυο προσδιορίζονται από την ανθρώπινη συμπεριφορά και αφορούν θέματα όπως παραβίαση προσωπικών πληροφοριών και δικαιωμάτων, καταπάτηση της ιδιωτικής ζωής, ψευδοπροσωπία, πρόκληση ζημιών ιδιωτικής φύσεως με υφαρπαγή προσωπικών δεδομένων, βλάβη από κακόβουλο λογισμικό, ιούς και hackers, έκθεση σε ανάρμοστο περιεχόμενο με υλικό πορνογραφίας, βία, εχθρότητα και εξτρεμιστικές ομάδες, θυματοποίηση από online απάτες, παραπλάνηση τύπου Hoax, εθισμό στο Διαδίκτυο (αποκτώντας προβλήματα κοινωνικότητας, σχολική αποτυχία, διαταραχές ύπνου, μειωμένη αυτοεκτίμηση, μειωμένη φυσική δραστηριότητα, χαμηλή ποιότητα ζωής), εμπλοκή του ατόμου σε μορφές ηλεκτρονικού εγκλήματος με παράνομες online ενέργειες, κακή μη ελεγχόμενη επιρροή που έχει κατηγορηθεί ακόμα και ως παράγοντας που οδήγησε σε θανάτους και άλλους πολλούς κινδύνους.

Φυσικά οι διαδικτυακοί κίνδυνοι δεν είναι μόνο αυτοί. Σοβαρές είναι οι προκλήσεις ζημιών στο υπολογιστικό σύστημα ενός χρήστη με μόλυνση από ιό που αναλαμβάνει δράση επιμολύνοντας το σύστημα και καταστρέφει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος εκμεταλλευόμενος κενά ασφαλείας στο λογισμικό του χρήστη. Παρόμοιας δράσης είναι ένα πρόγραμμα που αποκαλείται σκουλήκι (worm) με τη διαφορά ότι δεν απαιτεί την προσκόλλησή του σε ένα αρχείο, έχοντας έτσι αυτονομία, προκαλώντας βλάβη κυρίως στο δίκτυο σύνδεσης επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth). Άλλος κίνδυνος είναι ο Δούρειος Ίππος (trojan), ένα πρόγραμμα που ξεγελά το χρήστη του και εγκαθιστά κακόβουλα προγράμματα. Τέλος τα διαδικτυακά ρομπότ (bots) ευθύνονται

για την αποστολή των περισσοτέρων ανεπιθύμητων ηλεκτρονικών μηνυμάτων, δημιουργώντας ένα botnet, δηλαδή ένα δίκτυο υπολογιστών που έχουν το ίδιο bot, παραδίνοντας τον έλεγχο των υπολογιστών σε ένα κεντρικό άτομο.

Σαφέστατα η χρήση του διαδικτύου μπορεί να γίνει ασφαλέστερη με την υιοθέτηση πρακτικών τρόπων προστασίας που θα χρησιμοποιούνται σε συνδυασμό. Σημαντική θεωρείται η χρήση τείχους προστασίας (Firewall) που αποτελεί ένα λογισμικό πρόγραμμα το οποίο ελέγχει τις κινήσεις του χρήστη και επιτρέπει ή απαγορεύει τη μεταφορά πληροφοριών που μπορεί να είναι επικίνδυνες για το σύστημα του υπολογιστή. Επιπλέον, πολύτιμη είναι η εγκατάσταση ενός λογισμικού προστασίας και η συχνή ενημέρωση προγράμματος αναγνώρισης ιών (antivirus) και προγραμμάτων κατασκοπείας (spyware), τα οποία αναγνωρίζουν και αποτρέπουν την εγκατάσταση ενός ιού, worm ή άλλου κακόβουλου προγράμματος στον υπολογιστή. Ακόμα χρήσιμη είναι η ενημέρωση του λειτουργικού και των λογισμικών προγραμμάτων ενός υπολογιστή με τις πιο πρόσφατες ενημερώσεις ασφαλείας, ώστε να μην δοθεί η δυνατότητα σε ιούς να εκμεταλλευτούν αδυναμίες των προγραμμάτων. Επίσης, οι χρήστες δεν πρέπει να ανοίγουν επισυνάψεις ηλεκτρονικών μηνυμάτων που δεν εμπιστεύονται. Συνοψίζοντας, ο κάθε χρήστης διαδικτύου οφείλει να προσέχει και να φυλάει τα προσωπικά του δεδομένα ώστε να μην είναι δυνατό οι κίνδυνοι του διαδικτύου, οι απατεώνες και τα τεχνάσματα να τον εξαπατήσουν και να τον βλάψουν.

Αναπόσπαστο κομμάτι στην ασφάλεια από τους κινδύνους του Διαδικτύου αποτελούν η ενημέρωση, η επαγρύπνηση και οι κανόνες ασφάλειας σε ιδιωτικό επίπεδο, ώστε να επιτευχθεί μια σχετικά ασφαλής χρήση των τεχνολογιών του ψηφιακού κόσμου αποφεύγοντας τους κινδύνους που ελλοχεύουν. Συγκεκριμένα, η ανάγνωση και αποδοχή των όρων και των προϋποθέσεων χρήσης μιας ιστοσελίδας, ο σεβασμός στα δικαιώματα αλλά και τα συναισθήματα των άλλων με προσεκτική σκέψη για τις μακροπρόθεσμες συνέπειες, η προσοχή μας στο τι αναρτούμε με προσπάθεια διατήρησης της ιδιωτικότητας των προσωπικών μας πληροφοριών, αποτελούν τα βασικό πλαίσιο που πρέπει να κινούμαστε. Τέλος πολύ σημαντικό είναι να προστατεύουμε τα μέλη της οικογένειάς μας από τους πολύ σοβαρούς διαδικτυακούς κινδύνους που διατρέχουν, ώστε να γίνει ασφαλής και υπεύθυνη η πλοήγηση στο Διαδίκτυο, θωρακίζοντας τον υπολογιστή μας με ρυθμίσεις ασφαλείας, αποκλεισμό ακατάλληλου περιεχομένου, αύξηση ασφάλειας και προστασίας του απορρήτου, χρήση υπηρεσιών ελεγχόμενης πρόσβασης (Web-Filtering) και άλλες σημαντικές ρυθμίσεις σε συνδυασμό με την ουσιαστική συζήτηση και

επικοινωνία με τα παιδιά, κάνοντας αδύνατον το να παραπλανηθούν η να κινδυνεύσουν από οτιδήποτε επιβλαβές. Συμπερασματικά, η καλύτερη προστασία από καθετί είναι η γνώση, η εξοικείωση με τα διαδραστικά μέσα, η προσοχή και η εφαρμογή μέτρων προφύλαξης.

Αποτελέσματα

Ξυπνάτε και κοιμόσαστε έχοντας διαρκώς το μυαλό σας στο διαδίκτυο; Προτιμάτε την «παρέα» του ηλεκτρονικού σας υπολογιστή, από την παρέα των αγαπημένων σας φίλων; Νιώθετε άγχος και νευρικότητα κάθε φορά που βρίσκεστε offline; Ε, τότε πιθανότατα, να είστε κι εσείς ένας από τους πολλούς ανθρώπους στη χώρα μας που βρίσκονται στον «προθάλαμο» του διαδικτυακού εθισμού, γεγονός που σημαίνει ότι το παρόν άρθρο σας αφορά απόλυτα!

Σύμφωνα με τα τελευταία στοιχεία της Μονάδας Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών, του Νοσοκομείο Παίδων «Π. & Α. Κυριακού», ολοένα και μεγαλύτερος αριθμός εφήβων, τα τελευταία χρόνια, παρουσιάζει διαδικτυακές συμπεριφορές υψηλού κινδύνου!

Και ενώ θα περίμενε κανείς ότι την «πρωτιά» στον διαδικτυακό εθισμό κρατάει η Αττική, τα περισσότερα κρούσματα -σύμφωνα πάντα με την έρευνα της Μ.Ε.Υ-, εντοπίζονται στην επαρχία, όπου τα παιδιά φαίνεται να έχουν πιο περιορισμένες επιλογές και μια αυξημένη ροπή στην απομόνωση.

Τα στοιχεία που είδαν πρόσφατα το φως της δημοσιότητας και αφορούν στον εθισμό στο διαδίκτυο είναι αποκαρδιωτικά και φανερώνουν μια κακώς εννοούμενη «άνεση» των Ελληνόπουλων με το ίντερνετ:

- Το 2,4% των εφήβων 15-16 ετών στη χώρα μας, παρουσιάζουν διαδικτυακή εξάρτηση και το 19,1% οριακή χρήση, που δυνητικά στο μέλλον μπορεί να οδηγήσει σε συμπεριφορές εξάρτησης.

- Το ποσοστό των εφήβων με συμπεριφορές εξάρτησης ήταν μεγαλύτερο στις επαρχιακές πόλεις σε σύγκριση με την Αττική (3,4% έναντι 1,3%).

- Δεν διαπιστώθηκε διαφοροποίηση που να σχετίζεται με το φύλο. Τα δίκτυα κοινωνικής δικτύωσης αποτελούν πλέον τον πρώτο σε συχνότητα λόγο που οι εξαρτημένοι έφηβοι χρησιμοποιούν το Διαδίκτυο, ενώ ακολουθούν τα online παιχνίδια.

- Από το σύνολο των εφήβων, το 63,7% θα δημοσιοποιούσαν προσωπικά τους δεδομένα (το 100% των εφήβων με εξάρτηση), ενώ το 18,5% θα συναντούσαν κάποιον διαδικτυακό φίλο στο φυσικό κόσμο (έναντι 74% των εφήβων με εξάρτηση).

- Το 95,2% των εφήβων με εθισμό στο Διαδίκτυο προέρχονταν από έγγαμες οικογένειες.

- Το 44,4% των εφήβων με εθισμό έχουν συχνή πρόσβαση στο Διαδίκτυο από το κινητό τηλέφωνο, έναντι 15% όσων δεν κάνουν συχνή χρήση του Διαδικτύου.

Αξίζει να σημειωθεί ότι από το καλοκαίρι του 2007, η Μονάδα Υγείας Εφήβων έχει δεχθεί περισσότερους από 100 εφήβους, γεγονός που φανερώνει ότι το πρόβλημα πλέον στη χώρα μας λαμβάνει ανεξέλεγκτες διαστάσεις.

Στη χώρα μας το πρόβλημα της διαδικτυακής εξάρτησης είναι μεγαλύτερο απ' ό, τι σε άλλες χώρες του εξωτερικού. Δυστυχώς, το διαδίκτυο στην Ελλάδα ήρθε απότομα, χωρίς να υπάρχει καμιά οργανωμένη προώθηση του ζητήματος, ώστε να μάθουν τα παιδιά να προφυλάσσονται από τους κινδύνους του. Δεν υπάρχει οργάνωση, δεν υπάρχει παιδεία.

Τα παιδιά πλέον στις επαρχιακές πόλεις μη έχοντας εναλλακτικές λύσεις για διασκέδαση, κλείνονται όλο και περισσότερο στον εαυτό τους. Για τα σημερινά παιδιά λοιπόν, αποτελεί εύκολη λύση να μπαίνουν στο διαδίκτυο και να καλύπτουν τις επικοινωνιακές τους ανάγκες μέσα απ' αυτό.

Εκτός από τους συναισθηματικούς λόγους που ωθούν τα σημερινά παιδιά στο διαδίκτυο, με αποτέλεσμα πολλές φορές να εθίζονται σ' αυτό, όλο αυτό είναι και κάτι που προωθείται απ' όλο το κοινωνικό σύνολο, απ' όλη την κοινωνική κατάσταση την οποία βιώνουμε. Έχει αλλάξει η νοοτροπία πια της σκέψης, τα δεδομένα, οι απαιτήσεις που

έχουμε από έναν έφηβο, άρα είναι δύσκολο να διαχειριστείς όλη αυτή την απότομη αλλαγή.

Το πιο ανησυχητικό απ' όλα είναι το γεγονός ότι η ηλικία όσων αναπτύσσουν επικίνδυνες διαδικτυακές συμπεριφορές κατεβαίνει και ενώ μέχρι πρόσφατα μιλούσαμε για παιδιά με προσκόλληση στο διαδίκτυο, ηλικίας από 12 έως 18, σήμερα μιλάμε για παιδιά από 10 έως 18 ετών!

Οι επιπτώσεις τόσο στην ψυχολογία, όσο και στο σώμα του ατόμου που έχει εθιστεί στο διαδίκτυο είναι πολλές και ενίοτε σοβαρές. Το κυρίαρχο αίσθημα, το οποίο έχει το άτομο με διαδικτυακή εξάρτηση είναι αυτό τη ευφορίας, όση ώρα βρίσκεται μπροστά στην οθόνη του υπολογιστή, ενώ προσπαθεί με κάθε τρόπο να παραμείνει online. Πολύ συχνά δε, παραμελεί οικογένεια και φίλους, στους οποίους φθάνει στο σημείο να λέει ψέματα για την πολύωρη ενασχόλησή του με το διαδίκτυο. Έντονο μέσα του είναι και το αίσθημα του κενού και της θλίψης, ενώ όταν δεν βρίσκεται στον υπολογιστή γίνεται οξύθυμο. Από την άλλη πλευρά, τα άτομα με διαδικτυακή εξάρτηση παρουσιάζουν προβλήματα προσαρμογής στη δουλειά τους ή το σχολείο, αν πρόκειται για μαθητές.

Σοβαρά είναι και τα σωματικά προβλήματα που προκύπτουν από την άνευ ορίων χρήση του ίντερνετ. Τα προβλήματα αυτά σχετίζονται -όπως μας ενημερώνει η ειδικός- με διατροφικές διαταραχές, διαταραχές ύπνου, μυοσκελετικές παθήσεις, μειωμένη αθλητική δραστηριότητα, οφθαλμολογικές παθήσεις, ακόμη και ημικρανίες. Συχνά μάλιστα, παρατηρείται και παραμέληση της προσωπικής υγιεινής.

Είναι γεγονός ότι ο διαδικτυακός εθισμός μπορεί να προκαλέσει ακόμη και κατάθλιψη. Πρόκειται για μια αμφίδρομη σχέση διαδικτύου-κατάθλιψης, μια που και η ίδια η κατάθλιψη από μόνη της μπορεί να οδηγήσει σε εξάρτηση από το διαδίκτυο.

Μπορεί ο εθισμός στο διαδίκτυο να συγκριθεί με άλλες μορφές εθισμού, όπως είναι το αλκοόλ και τα ναρκωτικά. Ο εθισμός στο διαδίκτυο ανήκει στην ίδια κατηγορία με τις άλλες μορφές εθισμού, με τη μόνη διαφορά ότι η αντιμετώπιση του συγκεκριμένου, όπως και του εθισμού στα τυχερά παιχνίδια, είναι πολύ πιο δύσκολη! Στην Ελλάδα, τα τελευταία χρόνια, όλο και μεγαλύτερος αριθμός εφήβων και γονιών απευθύνεται στα υπάρχοντα οργανωμένα κέντρα της χώρας μας, προκειμένου να λάβουν ενημέρωση, αλλά και βοήθεια σε θέματα εξάρτησης από το διαδίκτυο.

Μέρος 4ο: E- BULLYING

Η διαφορά της Διαδικτυακής παρακολούθησης και παρενόχλησης από τον Διαδικτυακό εκφοβισμό

Στον Διαδικτυακό εκφοβισμό παρατηρείται η συμμετοχή συνομήλικων και από τις δυο πλευρές, ή τουλάχιστον η συμμετοχή ενός ενήλικα υποκινούμενη από κάποιον ανήλικο εναντίον άλλου ανηλίκου. Στην περίπτωση που παρατηρηθεί εμπλοκή ενηλίκου χρησιμοποιούνται οι οροί Διαδικτυακή παρενόχληση (Cyber-Harassement) είτε η Διαδικτυακή παρακολούθηση (Cyber-Stalking). Ο όρος Διαδικτυακός εκφοβισμός, εν αντιθέσει με την σεξουαλική παρενόχληση, δεν χρησιμοποιείται σε περιπτώσεις, κατά τις οποίες ένας ενήλικας προσπαθεί να οδηγήσει ανηλίκους σε μη διαδικτυακές συναντήσεις δελεάζοντάς τους. Ωστόσο, συχνά παρατηρείται στον Διαδικτυακό εκφοβισμό η ανάμειξη ενός η περισσότερων ενηλίκων, οι οποίοι ικανοποιούνται μέσα από την διαδικτυακή **σεξουαλική παρενόχληση** των ανήλικων θυμάτων.

Αίτια

Συχνά οι νέοι οδηγούνται στον Διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων όπως θυμός, απόγνωση είτε πάλι και εκδίκηση, που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργικότητας που παρουσιάζει το άτομο. Σε μερικές περιπτώσεις ο Διαδικτυακός εκφοβισμός αποτελεί μορφή ψυχαγωγίας στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποίηση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου. Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου.

Μορφές Διαδικτυακού εκφοβισμού

- Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- Παρέμβαση και παρενόχληση οποιασδήποτε διαδικτυακής δραστηριότητας του ατόμου
- Δημιουργία ψεύτικων διαδικτυακών προφίλ
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή αλλού είδους μαγνητοσκοπημένου υλικού
- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες

- Αποστολή απειλητικών μηνυμάτων σε αλλά άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

Η συχνότητα των απειλών

1. Η επικοινωνία πραγματοποιείται μόνο μια φορά
2. Η επικοινωνία επαναλαμβάνεται με ίδιο ή διαφορετικό τρόπο
3. Η επικοινωνιακή δραστηριότητα αυξάνεται
4. Τρίτα άτομα εμπλέκονται στην επικοινωνία με αποτέλεσμα το άτομο να λαμβάνει μηνύματα από διαφορετικούς παραλήπτες

Αντιμετώπιση του Διαδικτυακού εκφοβισμού

- Αγνόηση ενοχλητικών μηνυμάτων, σε περίπτωση ωστόσο απειλών συνιστάται αναφορά των μηνυμάτων και λήψη προληπτικών μέτρων .
- Αποκλεισμός του αποστολέα που στέλνει απειλητικά ή ενοχλητικά μηνύματα
- Προειδοποίηση του αποστολέα
- Αναφορά του περιστατικού στην **Αστυνομία** είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού εγκλήματος

Στατιστικά στοιχεία

1. Περίπου 15-35% των νέων έχει πέσει θύμα Διαδικτυακού εκφοβισμού
2. 10-20% των νέων παραδέχεται την ανάμειξή του σε Διαδικτυακό εκφοβισμό
3. Τα κορίτσια ενδέχεται να εμπλακούν συχνότερα από ότι τα αγόρια σε περιστατικά Διαδικτυακού εκφοβισμού
4. Η πλειοψηφία των ατόμων που υφίστανται είτε ασκεί Διαδικτυακό εκφοβισμό είναι ηλικίας 12-16 ετών

Είδη παρατηρητών στον Διαδικτυακό εκφοβισμό

Όπως ακριβώς και στον **Σχολικό εκφοβισμό,** έτσι και στον Διαδικτυακό εκφοβισμό - που μπορεί να αποτελέσει προέκταση του πρώτου - καταγράφονται κυρίως δύο είδη παρατηρητών (bystanders):

- Στην πρώτη κατηγορία ανήκουν οι επιβλαβείς για το θύμα παρατηρητές, καθώς επιδοκιμάζουν την συμπεριφορά του θύτη ενισχύοντας έτσι την ένταση του εκφοβιστικού γεγονότος ή άλλοτε παρατηρούν το περιστατικό με απάθεια δίχως να σημειώνουν κάποια αντίδραση ή παρέμβαση για την καταστολή του εκφοβισμού.
- Σε αντίθεση με την πρώτη κατηγορία, οι βοηθοί παρατηρητές αντιδρούν άμεσα και ενεργά στο συμβάν του Διαδικτυακού εκφοβισμού. Παράλληλα, στοχεύουν στην κινητοποίηση περισσότερων ατόμων για την καταπολέμηση του Διαδικτυακού εκφοβισμού.

Συνέπειες

Το φαινόμενο του Διαδικτυακού εκφοβισμού εγκυμονεί σοβαρές επιπτώσεις για την ψυχική υγεία του θύματος, αλλά και του θύτη. Η αυτοεκτίμηση του ατόμου που υφίσταται Διαδικτυακό εκφοβισμό πλήττεται έντονα τόσο ώστε σε μερικές περιπτώσεις συνδέεται με το αίσθημα της ενοχής. Το άτομο αρχίζει να αναπαράγει αρνητικές σκέψεις και η επίδοση των κοινωνικών του ικανοτήτων μειώνεται σημαντικά. Κάποιες φορές, κυρίως κατά την εφηβική ηλικία η αποχή από το σχολείο και από τις παρέες των συνομηλίκων αποτελεί προσωρινό καταφύγιο, ενώ ταυτόχρονα η **αυτοκτονία** θεωρείται ως η μοναδική λύση στο πρόβλημα. Άτομα που δέχτηκαν έντονα Διαδικτυακό εκφοβισμό ενδέχεται στο μέλλον να παρουσιάσουν μεγαλύτερη αστάθεια στις διαπροσωπικές τους σχέσεις συνοδευόμενη από την κοινωνική απομόνωση. Από την άλλη, οι εκφοβιστές τείνουν να είναι άτομα με έντονη αντικοινωνική συμπεριφορά, επιρρεπή στο αλκοόλ και απομονωμένα από τους συνομηλίκους. Μακροπρόθεσμα αντιλαμβάνονται ότι ο εκφοβισμός δεν αποτελεί μορφή ικανοποίησης και αναγνώρισης, βιώνοντας έτσι έντονη προσωπική απογοήτευση.

Μέρος 5^{ο}: ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ – ΠΩΣ ΜΠΟΡΟΥΜΕ ΝΑ ΔΙΑΦΥΛΑΞΟΥΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΜΑΣ

Κατά την πλοήγηση στους χώρους του Διαδικτύου είναι καλό να έχουμε υπόψη μας τα παρακάτω:

1. Το Διαδίκτυο είναι κυρίως μια κοινωνία ανθρώπων και κρύβει τους ίδιους κινδύνους που κρύβει κάθε κοινωνία, ιδιαίτερα όταν διευκολύνεται στο έπακρο ο τρόπος επικοινωνίας των ανθρώπων μεταξύ τους.

2. Οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες.

3. Η κοινοποίηση των προσωπικών στοιχείων του χρήστη (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικοί πρόσβασης, αριθμός πιστωτικών καρτών, e-mail κ.λπ.) είναι καλό να αποφεύγεται.

4. Η τοποθέτηση του υπολογιστή (εάν είναι δυνατόν) σε κοινόχρηστο χώρο και όχι αποκλειστικά στο παιδικό δωμάτιο ενθαρρύνει τη χρήση του Διαδικτύου σε οικογενειακό περιβάλλον και βοηθά στην επίβλεψη των ιστοσελίδων τις οποίες επισκέπτονται τα παιδιά.

5. Η καλή επικοινωνία με τα παιδιά είναι απαραίτητη ώστε να ενθαρρύνονται να μιλάνε για αυτούς με τους οποίους επικοινωνούν, ανταλλάσσουν μηνύματα και να ενημερώνουν εάν ποτέ γίνονται θύματα απειλών, εκφοβισμού ή παρενόχλησης οποιασδήποτε μορφής.

6. Η χρήση του υπολογιστή ως μέσου απασχόλησης του παιδιού χωρίς την παρουσία ενηλίκου είναι καλό να αποφεύγεται. Ο υπολογιστής δεν πρέπει να χρησιμοποιείται ως ηλεκτρονική babysitter !!!

7. Η δημιουργία ενός συνόλου από κανόνες χρήσης του Η/Υ αποδεκτών από όλους και η ανάρτηση τους σε εμφανές σημείο δίπλα στον υπολογιστή συντελεί στην προστασία όλων των χρηστών.

8. Στη διεύθυνση http://www.safeline.gr/ έχουμε ίσως τη μοναδική ελληνική ανοικτή γραμμή για καταγγελία παράνομου περιεχομένου στο διαδίκτυο. Μη διστάσετε να τη χρησιμοποιήσετε.

Ο Παγκόσμιος Ιστός (World Wide Web) είναι μια από τις σημαντικότερες υπηρεσίες του Internet και προσφέρει στους χρήστες του τη δυνατότητα πρόσβασης στη μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο. Πρόκειται για μια τεράστια συλλογή εγγράφων, τα οποία είναι αποθηκευμένα σε εκατομμύρια υπολογιστές στον κόσμο και η οποία εμπλουτίζεται συνεχώς από όλους τους χρήστες οι οποίοι αποφασίζουν να ανεβάσουν στο χώρο του τις σελίδες τους.

Η πλοήγηση στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ειδικών προγραμμάτων πλοήγησης -browsers- (π.χ. Internet Explorer, Mozilla Firefox κ.λπ.) και απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς κινδύνους, τόσο για την ασφάλεια του υπολογιστή του, όσο και για την ασφάλεια των προσωπικών του δεδομένων.

Τα μέτρα τα οποία μπορεί να ληφθούν για να εξασφαλίσουν κατά το δυνατόν ασφαλή πλοήγηση στις σελίδες του παγκοσμίου ιστού εξαρτώνται α) από τις υπηρεσίες που μπορεί να προσφέρει ο παροχέας σύνδεσης (**internet provider**) και β) από τις ενέργειες που κάνει ο ίδιος ο χρήστης.

Υπηρεσίες παρόχου σύνδεσης

Τα μέτρα για την ασφαλή πλοήγηση έχουν ως αφετηρία τις υπηρεσίες του παροχέα (provider) πρόσβασης στο διαδίκτυο. Ένας καλός παροχέας μπορεί να προσφέρει φιλτράρισμα των ιστοσελίδων που επισκέπτεται ο χρήστης-πελάτης και των mails που δέχεται.

Για παράδειγμα, η πρόσβαση που προσφέρει το Πανελλήνιο Σχολικό Δίκτυο εποπτεύεται από πρόγραμμα φιλτραρίσματος το οποίο δρα με δύο τρόπους:

- ψάχνει στις ιστοσελίδες που ζητά να δει ο χρήστης και αναζητά συγκεκριμένες λέξεις που είναι ύποπτες για ακατάλληλο υλικό π.χ. sex

- ψάχνει να δει αν η ιστοσελίδα έχει καταχωρηθεί στην μαύρη λίστα που διατηρεί στη βάση δεδομένων του.

Σε κάθε μια από τις παραπάνω περιπτώσεις απαγορεύει την πρόσβαση στην ιστοσελίδα, εμφανίζοντας προειδοποιητικό μήνυμα.

Στην περίπτωση των εισερχόμενων μηνυμάτων ηλεκτρονικής αλληλογραφίας, ερευνά για την ύπαρξη ιών στα επισυναπτόμενα αρχεία, ενώ παρέχει και υπηρεσία προστασίας από τα **spam-mails** (ενοχλητική αλληλογραφία) με την ενεργοποίηση, από τον χρήστη, των κατάλληλων φίλτρων στο web mail του.

Είναι ωστόσο συχνές οι περιπτώσεις κατά τις οποίες σελίδες που περιέχουν ακατάλληλο υλικό δεν περιέχουν τις λέξεις που φιλτράρουν τα προγράμματα αυτά ή δεν έχουν καταχωρηθεί στην μαύρη λίστα. Αντιθέτως, υπάρχουν και ιστοσελίδες που δεν περιέχουν ακατάλληλο υλικό αλλά μπορεί να απαγορεύονται, επειδή περιέχουν λέξεις που φιλτράρει το πρόγραμμα. Σε αυτές τις περιπτώσεις είναι καλό ο χρήστης να ενημερώνει τον διαχειριστή του προγράμματος (**cachemaster**), προκειμένου αυτός να προβεί στις κατάλληλες ενέργειες.

Ενέργειες του ίδιου του χρήστη

Ακόμα και οι καλύτερες υπηρεσίες ενός παροχέα σύνδεσης δεν εξασφαλίζουν τον χρήστη από τους κινδύνους που ελλοχεύουν κατά την πλοήγηση, αν ο ίδιος δεν λάβει τα κατάλληλα μέτρα προστασίας και δεν υιοθετήσει μια πολύ προσεκτική συμπεριφορά.

Ο βασικότερος κανόνας είναι η προσεκτική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στην οθόνη του υπολογιστή. Ο χρήστης δε θα πρέπει σε καμία περίπτωση να κάνει κλικ στο «Ναι» ή το «Όχι» των παραθύρων χωρίς να διαβάζει το περιεχόμενό τους, ενώ θα πρέπει να κλείνει το παράθυρο χωρίς να κάνει κλικ, όταν δεν το καταλαβαίνει.

Pop-up windows

Πολλές φορές κατά την πλοήγηση ανοίγουν, χωρίς να το προκαλέσει ο χρήστης, παράθυρα (pop up windows) των οποίων το περιεχόμενο ποικίλει. Αυτό μπορεί να είναι:

-->Διαφημίσεις

-->Προειδοποιητικά μηνύματα που καλούν τον χρήστη να προβεί σε ενέργειες (αποδεχόμενος συγκεκριμένες προσφορές) με άγνωστες ή επικίνδυνες για αυτόν συνέπειες.

-->Κάλεσμα για παιγνίδια είτε κανονικά είτε τυχερά.

-->Δωρεές

-->Δεσμοί σε σελίδες πορνογραφικού περιεχομένου και γενικά ποικιλία δελεαστικών προτάσεων.

Η ενδεδειγμένη ενέργεια είναι να κλείνουν άμεσα αυτά τα παράθυρα. Σε περίπτωση που αυτό δεν είναι δυνατόν από το Χ στο πάνω δεξιά μέρος του παραθύρου, εναλλακτικοί τρόποι είναι:

--> Δεξί κλικ στην γραμμή κατάστασης, στο αντίστοιχο εικονίδιο και επιλογή «κλείσιμο»,

--> Πατώντας ταυτόχρονα Alt + F4 (επιλογή από το πληκτρολόγιο που κλείνει το ενεργό παράθυρο).

Η εμφάνιση τέτοιων παραθύρων μπορεί να αποφευχθεί χρησιμοποιώντας

κατάλληλα προγράμματα (**pop up blockers/ killers**), τα οποία προσφέρονται στο διαδίκτυο. Επισημαίνεται ότι η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την πρόσβαση σε κάποιες, χρήσιμες κατά τα άλλα, ιστοσελίδες. Μία τέτοια περίπτωση είναι αυτή κατά την οποία έγκυρες εταιρείες προσφέρουν μέσω pop up παραθύρων προγράμματα εφαρμογών απαραίτητα για τη σωστή εμφάνιση ενός πλήθους ιστοσελίδων (π.χ. Flash Player από την Macromedia, mwpluggin από την LCSI για το Microworlds κ.λπ). Σε αυτή την περίπτωση μπορούμε προσωρινά να απενεργοποιήσουμε τον blocker.

Τοπική αποθήκευση (download)

Η διαδικασία της τοπικής αποθήκευσης στον υπολογιστή προγραμμάτων τα οποία διατίθενται στο Διαδίκτυο (**download**) πρέπει να γίνεται με πολλή προσοχή, διότι ενδέχεται τα προγράμματα αυτά να είναι μολυσμένα με ιούς, ή να αποτελούν τα ίδια ιούς που μπορεί να καταστρέψουν τα αρχεία του υπολογιστή. Σε αυτήν την περίπτωση πρέπει να βεβαιωνόμαστε για την εγκυρότητα της ιστοσελίδας η οποία μας προτείνει το συγκεκριμένο πρόγραμμα. Τέτοιες ιστοσελίδες συνήθως εμφανίζουν μήνυμα στο οποίο ενημερώνουν ότι η λήψη δεδομένων από αυτές πληροί τις προϋποθέσεις ασφαλείας.

Ρύθμιση ασφαλείας φυλλομετρητών

Οι σύγχρονες εκδόσεις των φυλλομετρητών **(internet explorer/mozilla firefox**) προσφέρουν δυνατότητα ρύθμισης των επιπέδων ασφαλείας κατά την πλοήγηση στο διαδίκτυο. Οι ρυθμίσεις αυτές είναι καλύτερο να γίνουν με τη βοήθεια ενός τεχνικού, αν ο χρήστης δεν έχει την κατάλληλη εμπειρία ή γνώσεις.

Εγκατάσταση προγραμμάτων ασφαλείας

Οι πιο προχωρημένοι χρήστες μπορούν να εγκαταστήσουν προγράμματα φιλτραρίσματος (**filtering software**) ή τειχών προστασίας του υπολογιστή (firewalls) από εξωτερικούς εισβολείς (φυσικά πρόσωπα, ιοί, spyware), κάνοντας τις κατάλληλες ρυθμίσεις. Οι νεότερες εκδόσεις των Windows προσφέρουν ενσωματωμένο πρόγραμμα firewall.

Η τεράστια δεξαμενή πληροφοριών και εργαλείων του Διαδικτύου είναι διάσπαρτη σε δισεκατομμύρια ιστοσελίδες που πρακτικά είναι αδύνατον να ερευνηθούν από τον χρήστη χωρίς τη βοήθεια εξειδικευμένων προγραμμάτων, όπως οι μηχανές αναζήτησης. Οι μηχανές αναζήτησης χρησιμοποιούν ειδικά προγράμματα, τις λεγόμενες αράχνες

(spiders), τα οποία «χτενίζουν» τις ιστοσελίδες αναζητώντας τα κείμενα και τις διευθύνσεις τους. Τα κείμενα και οι διευθύνσεις τους συγκεντρώνονται και καταγράφονται. Με άλλα προγράμματα συγκεντρώνονται πληροφορίες από τα κείμενα, το είδος των οποίων ποικίλει από μηχανή σε μηχανή, και αποθηκεύονται σε βάσεις δεδομένων, ώστε να είναι εύκολο να ανακτηθούν.

Όταν διενεργείται μια αναζήτηση, με την χρήση ενός συνόλου από λέξεις-κλειδιά, ερευνάται πρώτα η βάση δεδομένων και ακολούθως συγκεντρώνονται όλες οι διευθύνσεις που περιέχουν αυτές τις λέξεις. Τα αποτελέσματα αναζήτησης, έτσι όπως εμφανίζονται στον χρήστη, συνήθως περιέχουν την διεύθυνση της ιστοσελίδας, ένα δείγμα του κειμένου μέσα στο οποίο υπάρχουν οι λέξεις που αναζητήθηκαν, μια σύντομη περιγραφή και την κατηγορία στην οποία έχει καταγραφεί η ιστοσελίδα στην δεδομένη μηχανή αναζήτησης.

Ο τρόπος σωστής αναζήτησης μέσα από τις μηχανές αναζήτησης, τους θεματικούς καταλόγους και τις μεταμηχανές αναζήτησης είναι από τις πλέον βασικές δεξιότητες που πρέπει να διαθέτει ο χρήστης, τόσο για να μη χαθεί στις λεωφόρους των πληροφοριών του Διαδικτύου, όσο και για να βρίσκει ταχύτερα τις πληροφορίες που αναζητά. Είναι επομένως βασικός στόχος της εκπαίδευσης των νέων ανθρώπων, πολιτών της κοινωνίας της πληροφορίας. Λέγεται ότι ένας δωδεκάχρονος μαθητής μπορεί να συγκεντρώσει σήμερα σε πολύ μικρό χρόνο τόσες πληροφορίες, όσες θα συγκέντρωνε ένας ερευνητής του μεσαίωνα σε όλη του την ζωή.

Βασικοί κανόνες

Υπάρχουν τρεις βασικοί κανόνες οι οποίοι καθορίζουν έναν συγκεκριμένο τρόπο συμπεριφοράς του χρήστη και συμβάλλουν στη σωστή αναζήτηση, έτσι ώστε να αποφεύγεται η προσπέλαση σε ακατάλληλο υλικό ή να ελαχιστοποιούνται οι συνέπειες όταν αυτό έχει συμβεί. Κάθε κανόνας αναφέρεται σε γνώση και δεξιότητες:

α. Διάβασε, σκέψου και μετά κάνε κλικ.

Θα πρέπει οι χρήστες να γνωρίζουν ότι, όταν ερευνούν στο Διαδίκτυο για μια καθ' όλα αποδεκτή λέξη, τα αποτελέσματα μπορεί να τους οδηγήσουν σε εντελώς ακατάλληλες ιστοσελίδες. Ακόμη και ελάχιστη εμπειρία είναι αρκετή για να πείσει για αυτό.

Οι χρήστες συχνά κάνουν κλικ στα αποτελέσματα της αναζήτησης χωρίς να διαβάσουν την περιγραφή. Αυτή η συμπεριφορά ενέχει κινδύνους. Πρέπει να ξέρουν ότι,

πριν κάνουν κλικ σε ένα από τα αποτελέσματα της αναζήτησης, πρέπει να διαβάσουν προσεκτικά την περιγραφή του λήμματος. Αν η περιγραφή αυτή δεν ανταποκρίνεται σε αυτό που αναζητούν ή αν δεν είναι σίγουροι που θα τους οδηγήσει ο δεσμός, τότε δεν πρέπει να κάνουν κλικ. Για εξάσκηση, μπορούν να δοθούν σε μαθητές παραδείγματα με αποτελέσματα αναζήτησης και να τους ζητηθεί να δείξουν για κάθε ένα από τα λήμματα αν ο δεσμός θα τους οδηγήσει σε αποτελέσματα σχετικά με αυτά που αναζητούν ή όχι. κατά τρόπο ανεπίστρεπτο, που δεν έχει προηγούμενο.

β. Πληκτρολόγησε, έλεγξε και μετά κάνε κλικ.

Μερικές φορές χρησιμοποιούνται διευθύνσεις του Διαδικτύου οι οποίες είναι σχεδόν όμοιες με νόμιμες και χρήσιμες, ελπίζοντας να ξεγελάσουν ανθρώπους και να επισκεφτούν πορνογραφικές ιστοσελίδες. Οι χρήστες συχνά πληκτρολογούν μια διεύθυνση και μετά κάνουν κλικ για να την επισκεφτούν, χωρίς να ελέγξουν αν πληκτρολογήθηκε σωστά. Θα πρέπει να αποκτήσουν την καλή συνήθεια να πληκτρολογούν τη διεύθυνση, ύστερα να ελέγχουν για να σιγουρευτούν αν την έγραψαν σωστά, και μετά να κάνουν κλικ. Θα πρέπει επίσης να γνωρίζουν ότι δεν είναι σωστό να προσπαθούν να μαντέψουν μια διεύθυνση. Αν δεν την γνωρίζουν με ακρίβεια, ας χρησιμοποιήσουν μια μηχανή αναζήτησης.

γ. Κλείσε και συζήτησε.

Οι χρήστες θα πρέπει να γνωρίζουν ότι, παρά τις προσπάθειές τους, μπορεί να βρεθούν σε λάθος ιστοσελίδα. Επίσης, θα πρέπει να γνωρίζουν ότι μερικές φορές αυτών των ειδών οι δικτυακοί τόποι χρησιμοποιούν αυτό που λέμε ποντικοπαγίδα. Δηλαδή απενεργοποιούν το κουμπί «πίσω», ανοίγουν πολλαπλά παράθυρα ή χρησιμοποιούν άλλες τεχνικές για να «παγιδεύσουν» τους χρήστες στον χώρο τους. Αν ένα παιδί βρεθεί σε έναν τέτοιο χώρο, η πρώτη του αντίδραση είναι το σοκ, γιατί δε θα μπορεί να φύγει από εκεί. Αν δεν το προετοιμάσουμε γι αυτή την πιθανότητα, η δεύτερη αντίδραση θα είναι ο φόβος ή ακόμα και η περιέργεια και αυτή η αντίδραση είναι και η πιο επικίνδυνη.

Για να αποφύγουμε τα χειρότερα, οφείλουμε να πληροφορήσουμε τα παιδιά για το τι πρέπει να κάνουν αν βρεθούν σε λάθος δικτυακό τόπο. Να ξέρουν ότι θα πρέπει να κλείσουν αμέσως τον φυλλομετρητή. Και αν δεν μπορούν να το κάνουν, να κλείσουν τον υπολογιστή και να αναφέρουν αμέσως σε κάποιον μεγαλύτερο αυτήν την αθέλητη προσπέλαση. Το αρχείο με τα cookies του φυλλομετρητή, που έχει προσπελάσει ακατάλληλη ιστοσελίδα, θα πρέπει να ελεγχθεί για να βεβαιωθεί ότι δεν έχουν τοποθετηθεί

ανεπιθύμητα cookies στον υπολογιστή.

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

Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι σημαντικό να διαχειριζόμαστε τη διεύθυνση της ηλεκτρονικής μας αλληλογραφίας με την ίδια προσοχή που διαχειριζόμαστε τον αριθμό του τηλεφώνου μας.

Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

1. Ιοί: Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς. Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο.

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.

Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»). Σε κάθε περίπτωση επιβάλλεται ο έλεγχος

της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

2. Ενοχλητική αλληλογραφία (spam mail): Είναι το λεγόμενο spam ή junk mail, δηλαδή μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος.

Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

3. Μηνύματα απατηλού περιεχομένου (hoaxes): Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

α. «Προειδοποιητικά»: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα

β. «Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου

(συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται

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

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

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

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

4.Μηνύματα οικονομικής εξαπάτησης (phishing): Το phishing (αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπαιρεώσουν μία συναλλαγή. Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης

όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές javascript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

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

Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mail που λαμβάνει, προκειμένου να διαπιστώσουν αν πρόκειται για phishing, ενώ αποκαλύπτουν και το πραγματικό όνομα του ιστοχώρου που επισκέπτεται ο χρήστης. Τέλος, τα γνωστά προγράμματα anti-spam μπορούν να μειώσουν τον αριθμό των απατηλών μηνυμάτων που λαμβάνει ο χρήστης.

Προστασία προσωπικών δεδομένων

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email.

Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail, οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας

προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται «δωμάτιο επικοινωνίας» (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους απ όλον τον κόσμο.

Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό (όπως στην περίπτωση του δημοφιλούς IRC, ή των διαφόρων τύπων messengers). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους.

Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός ιντερνετ-καφέ, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από

τους εκπαιδευτικούς.

Και μόνο η συμμετοχή σε τέτοιου είδους χώρους αποτελεί από μόνη της μια επικίνδυνη πρακτική. Σε περίπτωση όμως που δε μπορούν οι γονείς να αποτρέψουν ή να ελέγξουν τα παιδιά τους, οφείλουν τουλάχιστον να τους επιστήσουν την προσοχή, γιατί αυτά συχνά ξεγελιούνται και αποκαλύπτουν πολλά προσωπικά τους στοιχεία σε αγνώστους, οι οποίοι καταφέρνουν να κερδίσουν την εμπιστοσύνη τους.

Οι συμμετέχοντες σε τέτοιου είδους συνομιλίες δε θα πρέπει με κανέναν τρόπο να αποκαλύπτουν την ταυτότητά τους, ούτε τα προσωπικά τους στοιχεία (διεύθυνση, αριθμό τηλεφώνου, e-mail, όνομα σχολείου, πόλη), να μη δέχονται ποτέ να στείλουν τη φωτογραφία τους σε αγνώστους, ούτε να τους συναντούν σε πραγματικό χώρο. Επίσης, οφείλουν να γνωρίζουν πως σε καμιά περίπτωση δεν είναι ασφαλείς λόγω της ανωνυμίας τους. Ένας καλός χρήστης του Διαδικτύου είναι σε θέση να εντοπίσει την IP διεύθυνση του υπολογιστή τους, να αποκτήσει πρόσβαση σε προσωπικά τους αρχεία, να μολύνει τον υπολογιστή τους με ιούς ή σκουλήκια, τα οποία συχνότατα κυκλοφορούν σε τέτοιου είδους χώρους.

Τα παιδιά θα πρέπει να ενθαρρύνονται να συζητούν με τους γονείς τους για τις συνομιλίες τις οποίες παρακολουθούν μέσα σε chat-rooms, να μιλάνε για τους νέους φίλους τους, όπως θα έκαναν και για τους φίλους που γνωρίζουν στην πραγματική τους ζωή, να αναφέρουν κάθε περίπτωση κατά την οποία έχουν υποστεί παρενόχληση, οποιουδήποτε είδους. Οι γονείς, με τη σειρά τους, θα πρέπει να προτρέπουν τα παιδιά τους να χρησιμοποιούν αυτή τη δυνατότητα του Διαδικτύου για να επικοινωνήσουν με φίλους τους που βρίσκονται μακριά και τους οποίους τα παιδιά ήδη γνωρίζουν, και όχι ως μέσο νέων γνωριμιών.

Είναι η δυνατότητα, που προσφέρει το Διαδίκτυο στους χρήστες του, να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται μέσω διαφόρων προγραμμάτων (που διατίθενται στο διαδίκτυο ελεύθερα ή με πληρωμή).

Καθένα από τα προγράμματα αυτά λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή του χρήστη, σε όλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως, κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα

αρχεία, στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας, σύγχρονη επικοινωνία μεταξύ υπολογιστών, γι αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης (peer-to-peer) προγράμματα.

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

Οι κίνδυνοι, από την χρήση προγραμμάτων διαμοιρασμού αρχείων στο Διαδίκτυο, αφορούν κυρίως στα εξής:

Ασφάλεια

Η χρήση των προγραμμάτων διαμοιρασμού αρχείων παραβιάζει τους κανόνες «υγιεινής» του υπολογιστή μας. Μοιραζόμαστε «πράγματα» με χρήστες που δεν τους γνωρίζουμε και δεν τους εμπιστευόμαστε. Η «υγεία» του υπολογιστή μας κινδυνεύει από ιούς και άλλα καταστροφικά προγράμματα που διαχέονται στον υπολογιστή μας και τον μολύνουν. Οι ιοί μπορούν να καταστρέψουν τον υπολογιστή μας. Άλλα προγράμματα (π.χ. spyware) μπορούν να καταγράψουν τις δραστηριότητες μας στο Διαδίκτυο και να στείλουν αυτή την πληροφορία σε τρίτους ή να προκαλούν εμφάνιση διαφημιστικών μηνυμάτων ακόμη και όταν δεν είμαστε συνδεδεμένοι στο Διαδίκτυο.

Πρόσβαση των παιδιών σε πορνογραφικό υλικό

Τα περισσότερα από τα προγράμματα διαμοιρασμού αρχείων στο Διαδίκτυο επιτρέπουν την πρόσβαση ανήλικων σε ακατάλληλα βίντεο ή εικόνες. Καθώς τα παιδιά αναζητούν την αγαπημένη τους μουσική μπορεί αθέλητα να γίνουν παραλήπτες πορνογραφικού υλικού, απλά επειδή αυτό περιέχει τις ίδιες λέξεις-κλειδιά με τις οποίες γίνεται η αναζήτηση. Πολλά από τα προγράμματα ελέγχου της πλοήγησης, συμπεριλαμβανομένου και αυτού του σχολικού δικτύου, δεν είναι καθόλου αποτελεσματικά όταν η διακίνηση του ακατάλληλου υλικού γίνεται μέσα από προγράμματα διαμοιρασμού.

Νομικά προβλήματα

Τα περισσότερα αρχεία, που είναι διαθέσιμα μέσα από τα προγράμματα διαμοιρασμού (βίντεο, μουσική, τραγούδια, βιντεοπαιχνίδια), έχουν προστατευμένα δικαιώματα. Αυτό σημαίνει ότι ο νόμος προστατεύει το δικαίωμα του ιδιοκτήτη να επιβάλλει περιορισμούς στην αντιγραφή και την διακίνηση του προϊόντος. Η απόκτηση (download) και η διάθεση (upload) προϊόντων χωρίς την άδεια του ιδιοκτήτη μπορεί να προκαλέσει νομικά προβλήματα. Η ανωνυμία δεν είναι ποτέ απόλυτα δεδομένη στο Διαδίκτυο. Σε αρκετές περιπτώσεις υπήρξαν διώξεις «πειρατών», που διακινούσαν παράνομα αρχεία μουσικής.

Προσωπικά δεδομένα

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

Μέρος 6ο: ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΑ

Και οι πέντε ομάδες συνέβαλλαν στην σύνταξη ερωτηματολογίου σχετικά με τη χρήση του διαδικτύου από τους έφηβους μαθητές και μαθήτριες του γυμνασίου με Λυκειακές τάξεις Άγρας, και τους κινδύνους που επιφυλάσσει για αυτούς . Το εν λόγω ερωτηματολόγιο διανεμήθηκε σε παιδιά του γυμνασίου και των Λυκειακών τάξεων και των δύο φύλων τα οποία το απάντησαν ανώνυμα.

==========

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Απαντήστε βάζοντας στο κουτάκι στα δεξιά ένα ✓

Αγόρι ☐ Κορίτσι ☐

Α’ γυμνασίου ☐ Β’ γυμνασίου ☐ Γ’ γυμνασίου ☐

Α’ λυκείου ☐ Β’ λυκείου ☐ Γ’ λυκείου ☐

Γνώσεις ηλεκτρονικού υπολογιστή

α) Δεν έχω καθόλου ☐ β) Λίγο ☐ γ) Μέτρια ☐

δ) Πολύ καλά ☐ ε) Είμαι κάτοχος πτυχίου ☐

Διαδίκτυο

Χρησιμοποιείς το διαδίκτυο; Ναι ☐ Όχι ☐

Αν ναι, πόσες ώρες την ημέρα; …....

Ποιες ώρες της ημέρας; Πρωί ☐ Μεσημέρι ☐ Βράδυ ☐

Σερφάρεις στο διαδίκτυο α) Τις καθημερινές ☐ β) Σαβ/κο ☐

Ποιες κατηγορίες ιστοσελίδων επισκέπτεσαι περισσότερο;

α) Κοινωνικής Δικτύωσης (Facebook κτλ.) ☐

β) Για εύρεση πληροφοριών (Google/Wikipedia) ☐

γ) Online shopping (Ricardo/ebay κτλ) ☐

δ) Διασκέδαση (Youtube/sports κτλ) ☐

Χρησιμοποιείς το διαδίκτυο για τις σχολικές εργασίες;

Ναι ☐ Όχι ☐
Αν ναι , πόσες ώρες ημερησίως; ……..

E-bullying

Έχετε κάνει γνωριμίες μέσω Διαδικτύου; Ναι ☐ Όχι ☐

Αν ναι, πιστεύετε ότι η ταυτότητα που σας παρουσίασαν είναι αληθινή;

Ναι ☐ Όχι ☐

Έχετε πέσει θύματα ηλεκτρονικού εκφοβισμού;

Ναι ☐ Όχι ☐

Αν ναι, με ποιο τρόπο;
……
.....
.....

Πως το αντιμετωπίσατε;

Μόνος/Μόνη ☐ Ενημέρωσα γονείς ☐ Ενημέρωσα αδέλφια ☐ Φίλους ☐ Καθηγητές ☐

Ποια ήταν η έκβαση;…….....

<u>Online παιχνίδια</u>

Παίζεις online παιχνίδια; Ναι ☐ Όχι ☐

Αν, ναι πόσο χρόνο ημερησίως αφιερώνεις; ……

Τα online παιχνίδια που παίζεις έχουν όριο ηλικίας; Ναι ☐ Όχι ☐

Είσαι μέσα στο όριο ηλικίας; Ναι ☐ Όχι ☐

Οι ενήλικες στο σπίτι σου γνωρίζουν ότι παίζεις; Ναι ☐ Όχι ☐

Παίζεις με χρήματα; Ναι ☐ Όχι ☐

Η ενασχόληση σου με το Διαδίκτυο έχει επηρεάσει την απόδοση σου;

Όχι ☐ Ναι, προς το καλύτερο ☐ Ναι, προς το χειρότερο ☐

Θεωρείς ότι η ενασχόληση σου σε έχει απομακρύνει από τις κοινωνικές συναναστροφές;
Ναι ☐ Όχι ☐

ONLINE SHOPPING

Χρησιμοποιείς το Διαδίκτυο για αγορές; Ναι ☐ Όχι ☐

Αν ναι, τι προϊόντα αγοράζεις;

Ένδυση-Υπόδηση ☐ Ηλεκτρικές συσκευές ☐ Software/παιχνίδια ☐

Ποιους τρόπους πληρωμής επιλέγετε;

Με αντικαταβολή ☐ Μέσω τράπεζας ☐ Πιστωτική κάρτα ☐

Οι πληροφορίες που σας δόθηκαν για το προϊόν ήταν αληθείς; Ναι ☐ Όχι ☐

Έχετε πέσει θύμα εξαπάτησης από ιστοσελίδα αγοραπωλησιών; Ναι ☐ Όχι ☐

Μπορείτε να διακρίνετε τις ασφαλείς ιστοσελίδες στις οποίες χρησιμοποιείτε πιστωτική κάρτα για τις συναλλαγές σας; Ναι ☐ Όχι ☐

==========

Από την επεξεργασία του ερωτηματολόγιου αυτού από τις ομάδες, προέκυψαν τα εξής συμπεράσματα :

Α. Όσον αφορά στην ηλικιακή ομάδα 12-15 ετών , σε παιδιά και των δύο φύλων , τα αποτελέσματα που προέκυψαν είναι τα παρακάτω :

Σε αυτή την ηλικία το επίπεδο των γνώσεων του ηλεκτρονικού υπολογιστή είναι **μέτριο** . Χρησιμοποιούν το διαδίκτυο **καθημερινώς** , περίπου **3 ώρες ημερησίως** και μάλιστα κατά προτίμηση **τις καθημερινές ,τις μεσημβρινές και βραδινές ώρες .**

Οι έφηβοι επισκέπτονται ιστοσελίδες, α) κοινωνικής δικτύωσης (facebook) κτλ β) ιστοσελίδες για εύρεση πληροφοριών (Google Wikipedia) γ) για ηλεκτρονικές αγορές (online shopping), δ) για διασκέδαση (YouTube, online games) . Οι μαθητές και μαθήτριες αυτών των ηλικιών χρησιμοποιούν το διαδίκτυο σαν πηγή πληροφοριών για της σχολικές τους εργασίες , περίπου μια ώρα ημερησίως.

Σύμφωνα με το ερωτηματολόγιο, τα παιδιά δεν έχουν πέσει θύματα ηλεκτρονικού εκφοβισμού (e- bulling).

Τα παιδιά παίζουν online παιχνίδια στον ελεύθερο τους χρόνο και αφιερώνουν **μισή με μια ώρα περίπου ημερησίως** . Τα online παιχνίδια που παίζουν δεν απευθύνονται σε ενήλικες. Οι γονείς/κηδεμόνες τους γνωρίζουν για την ενασχόλησή τους με τα online παιχνίδια. Οι έφηβοι δεν παίζουν με χρήματα. Δεν θεωρούν ότι η ενασχόλησή τους με το internet έχει επηρεάσει την απόδοση τους, αντίθετα θεωρούν ότι το διαδίκτυο έχει συμβάλλει σημαντικά στην πρόοδο τους. Επιπλέον, πιστεύουν ότι ο χρόνος που αφιερώνουν στο διαδίκτυο δεν τους έχει απομακρύνει από τις κοινωνικές συναναστροφές.

Όσον αφορά στις ηλεκτρονικές αγορές, τα παιδιά χρησιμοποιούν το διαδίκτυο κυρίως για να αγοράσουν προϊόντα ένδυσης και υπόδησης . Επιλέγουν την αντικαταβολή ως τρόπο πληρωμής. Οι πληροφορίες που λαμβάνουν για τα προϊόντα που αγοράζουν από ιστοσελίδες , είναι αληθείς , κατά συνέπεια δεν έχουν πέσει θύματα εξαπάτησης. Ωστόσο, θεωρούν ότι δεν είναι σε θέση να διακρίνουν εάν μια ιστοσελίδα με την οποία συναλλάσσονται, είναι ασφαλής ή όχι.

Β. Όσον αφορά στην ηλικιακή ομάδα 15 με 17, τα αποτελέσματα είναι τα εξής: Οι έφηβοι αυτή της ηλικίας έχουν **μέτρια** γνώση υπολογιστών. Περίπου **1 ώρα την ημέρα** επισκέπτονται το διαδίκτυο προκείμενου να αναζητήσουν πληροφορίες για τις σχολικές τους εργασίες.

Παρ'όλα αυτά, χρησιμοποιούν το διαδίκτυο και μάλιστα **4 με 5 ώρες ημερησίως,** κατά προτίμηση **τις βραδινές ώρες, τις καθημερινές.** Κυρίως, επισκέπτονται ιστοσελίδες κοινωνικής δικτύωσης π.χ Facebook, και ιστοσελίδες διασκέδασης π.χ Youtube.

Οι έφηβοι αυτής της ηλικίας **έχουν** κάνει γνωριμίες μέσω internet και μάλιστα θεωρούν ότι η ταυτότητα που τους παρουσίασαν είναι αληθινή. Δήλωσαν ότι **δεν έχουν** πέσει θύματα ηλεκτρονικού εκφοβισμού (e-bulling).

Στον ελεύθερο χρόνο τους παίζουν παιχνίδια online τα οποία δεν έχουν όριο ηλικίας. Ασχολούνται περίπου **μιάμιση ώρα την ημέρα**. Οι γονείς-κηδεμόνες γνωρίζουν γι'αυτή την ενασχόλησή τους. Τα παιδιά δεν παίζουν με χρήματα, ενώ θεωρούν ότι αυτή η ενασχόλησή τους **δεν** έχει επηρεάσει τη σχολική τους απόδοση ωστόσο, πιστεύουν ότι τους έχει απομακρύνει από τους φίλους τους.

Οι έφηβοι χρησιμοποιούν το διαδίκτυο για τις αγορές τους (online shopping) και κατά κύριο λόγο αγοράζουν προϊόντα ένδυσης και υπόδησης. Επιλέγουν να πληρώνουν με αντικαταβολή. Οι πληροφορίες που λαμβάνουν από τις ιστοσελίδες για τα προϊόντα που αγοράζουν, είναι αληθείς. Δεν έχουν πέσει θύματα εξαπάτησης από ιστοσελίδες αγοραπωλησιών, βέβαια δηλώσανε ότι δεν είναι σε θέση να διακρίνουν τις ασφαλείς ιστοσελίδες με τις οποίες συναλάσσονται.

Πηγές

- http://mblog.lib.umich.edu/cyberbulling/archives/2007/03/what_are_the_so.html
- http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf
- http://www.stopcyberbullying.org/why_do_kids_cyberbully_each_other.html
- http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html
- http://www.stopcyberbullying.org/parents/guide.html
- http://www.stopcyberbullying.org/lawenforcement/telling_the_difference.html
- http://www.pi.ac.cy/InternetSafety/sec_kindinoi_ekfobismos.html

Στην παρούσα ερευνητική εργασία συμμετείχαν οι μαθητές και μαθήτριες της Α΄ τάξης των Λυκειακών Τάξεων Άγρας Λέσβου.

Επιβλέποντες καθηγητές ήταν οι Δουβαλέτα Δέσποινα (ΠΕ06) Αγγλικής Φιλολογίας και Τσακίρογλου Γεώργιος (ΠΕ20) Πληροφορικής.