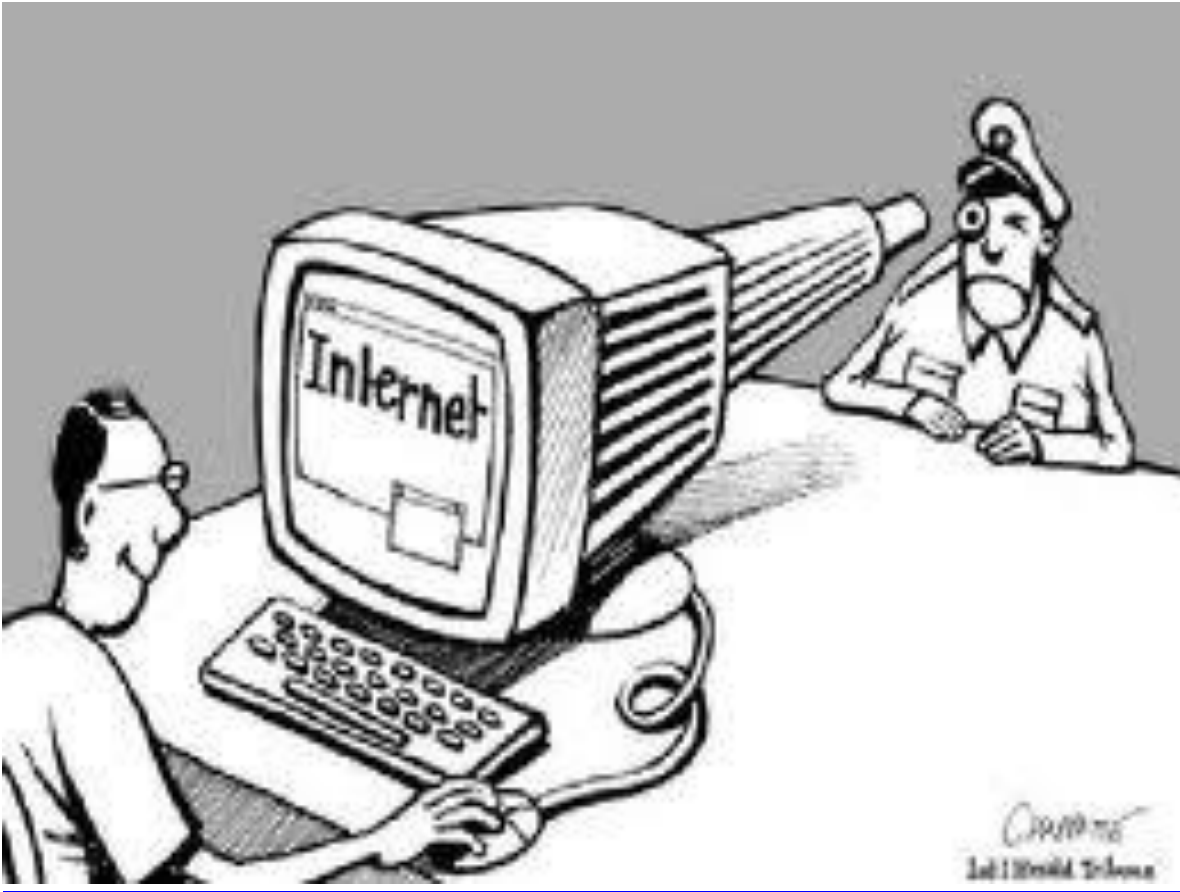


«Ερευνητική εργασία»
«Ασφάλεια στο Διαδίκτυο»
«Κίνδυνοι στο διαδίκτυο»



Διδάσκων : Γιάννης Δετοράκης

ΟΜΑΔΑ 3

- Αργυροπούλου Στυλιανή - Νικολέτα
- Ανδρουλάκης Γιώργος
- Βεισάκη Δήμητρα
- Ρινακάκη Παναγιώτα

Τάξη : Β΄ Γενικού Λυκείου Μοιρών

Σχολικό Έτος: 2013-2014

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος	Σελ.3
1. Κίνδυνοι στο Διαδίκτυο	
1.1 Υιοί υπολογιστών	Σελ.5
1.2 Ακατάλληλο περιεχόμενο	Σελ.6
1.3 Ακατάλληλα μηνύματα	Σελ.7
1.4 Αποξένωση από τον πραγματικό κόσμο	Σελ.7
1.5 Αποπλάνηση	Σελ.8
1.6 Βίαια παιχνίδια	Σελ.8
1.7 Εθισμός	Σελ.9
1.8 Εκφοβισμός	Σελ.10
1.9 Επιβλαβείς συμπεριφορές	Σελ.10
1.10 Ηλεκτρονικός τζόγος	Σελ.10
1.11 Παιδική πορνογραφία	Σελ.11
1.12 Παραβίαση ιδιωτικότητας	Σελ.12
1.13 Παραπληροφόρηση	Σελ.13
1.14 Παραποίηση γλώσσας	Σελ.13
1.15 Υποκλοπή προσωπικών στοιχείων	Σελ.14
1.16 Φυσικές παθήσεις	Σελ.14
2. Τρόποι αντιμετώπισης	Σελ.15
Επίλογος	Σελ.16
Βιβλιογραφία	Σελ.17

ΠΡΟΛΟΓΟΣ

Η ερευνητική εργασία μας είχε θέμα «Ασφάλεια στο Διαδίκτυο». Η ομάδα μας ασχολήθηκε με τους κινδύνους που μπορεί να αντιμετωπίσει κανείς στο διαδίκτυο.

Με την εξέλιξη της τεχνολογίας, το διαδίκτυο απέκτησε σημαντικό ρόλο στην καθημερινότητα του ατόμου. Πλέον το άτομο πληροφορείται και ψυχαγωγείται μέσω διαδικτύου, συνομιλεί με γνωστούς και αγνώστους, έχει τη δυνατότητα να αγοράζει και να πουλάει, να σχολιάζει και να εκθέτει τις απόψεις του χωρίς να δέχεται κριτική. Παρ' όλα αυτά εγκυμονούν πολλοί κίνδυνοι. Το άτομο μπορεί να εθιστεί στο διαδίκτυο μέσω ηλεκτρονικών παιχνιδιών ή των Μέσων Κοινωνικής Δικτύωσης. Ο ηλεκτρονικός τζόγος και τα βίαια παιχνίδια επηρεάζουν την ψυχολογία του ατόμου και ιδίως των μικρών παιδιών, τα οποία δεν έχουν διαμορφώσει ακόμα τον χαρακτήρα τους και μπορεί να οδηγηθούν ακόμα και σε αντικοινωνική συμπεριφορά. Η υποκλοπή προσωπικών δεδομένων είναι ακόμα ένας κίνδυνος που απασχολεί τους χρήστες του διαδικτύου και πιο συγκεκριμένα όσους ασχολιούνται με αγοροπωλησίες. Εκτός από την υποκλοπή, από τις αγοροπωλησίες και όχι μόνο, κινδυνεύουμε και από τους ιούς. Επίσης, η παραπληροφόρηση επιτυγχάνεται πολύ εύκολα εφόσον το άτομο έρχεται αντιμέτωπο με ένα μεγάλο πλήθος πληροφοριών που οδηγείται ακόμα και σε σύγχυση. Παράλληλα, αλλοιώνεται η γλώσσα χαρακτηριστικό παράδειγμα αποτελούν τα greeklish. Τελευταίος κίνδυνος αλλά εξίσου σημαντικός είναι η αποπλάνηση, η παιδική πορνογραφία και ο εκφοβισμός. Γεγονότα που έχουν απασχολήσει την ελληνική κοινωνία πολλές φορές τα τελευταία χρόνια.

Με βάση άρθρων της εφημερίδας «ΚΑΘΗΜΕΡΙΝΗ» :

- Ποινικοποιείται η παιδική πορνογραφία 17 Apr, 2002
- Ιντερνετ: ανεξέλεγκτα κυκλώματα παιδικής πορνείας ΕΛΛΑΔΑ 23 Mar, 2002
- Επιλοχίας με... ιστοσελίδα παιδικής πορνογραφίας ΕΛΛΑΔΑ 25 Sep, 2002
- Η πρόκληση του Ιντερνετ κρυφή απειλή για τα παιδιά - ΕΛΛΑΔΑ 28 Sep, 2002
- Κατέστρεφαν λογισμικό υλικό - ΕΛΛΑΔΑ 24 Oct, 2002
- Παγκόσμια κόντρα για τα πνευματικά δικαιώματα και το μέλλον του PC - ΟΙΚΟΝΟΜΙΑ & ΑΓΟΡΕΣ 26 Jan, 2002
- Τα ραντεβού της διαφθοράς μέσω Ιντερνετ - ΕΛΛΑΔΑ 25 Feb, 2003
- Από το «κουνελάκι» «Christmas tree» στον «I love you Virus» - ΚΟΣΜΟΣ 31 Aug, 2003
- Καθηγητής - εξαγωγέας παιδικής πορνογραφίας - ΕΛΛΑΔΑ 6 Nov, 2003
- Κύκλωμα νεαρών σατανιστών μέσω του Διαδικτύου - ΕΛΛΑΔΑ 17 Dec, 2003
- Στόχος κυβερνοαπατεώνων οι τραπεζικοί λογαριασμοί πελατών της Citibank - ΟΙΚΟΝΟΜΙΑ & ΑΓΟΡΕΣ 3 Oct, 2004

- Το 2ο Συνέδριο Τα... «εγχειρίδια» των απατεώνων του Διαδικτύου - ΕΛΛΑΔΑ 10 Aug, 2005
- Προσωπικά μυστικά στο Διαδίκτυο - ΕΛΛΑΔΑ 12 Jan, 2005
- Πάνω από 6 δισ. δολάρια ο τζίρος από πορνό - ΕΛΛΑΔΑ 9 Feb, 2005
- «Κράκερ» διεθνής εκβιαστής - ΕΛΛΑΔΑ 10 Aug, 2005
- Χιλιάδες e-mails εποφθαλμιούν απόρρητους κωδικούς και προσωπικά δεδομένα 6 Apr, 2008
- Χάκερ στην ιστοσελίδα του CERN - ΕΛΛΑΔΑ 16 Sep, 2008
- Αναμένεται η ταυτοποίηση των χάκερ μέσω ΗΠΑ - ΕΛΛΑΔΑ 30 Sep, 2009
- Προσοχή στους κωδικούς ασφαλείας στο Διαδίκτυο - ΟΙΚΟΝΟΜΙΑ & ΑΓΟΡΕΣ 23 Jan, 2010
- Συνομιλία πρόδωσε τον χάκερ - ΕΛΛΑΔΑ 11 Jun, 2011
- Θύμα ηλεκτρονικής επίθεσης η ιστοσελίδα του υπ. Δικαιοσύνης - ΠΟΛΙΤΙΚΗ 4 Feb, 2012
- Μυστήριο με την υποκλοπή εγγράφων - ΠΟΛΙΤΙΚΗ 30 Oct, 2012
- Η αστυνομία λέει ότι τα υπεξαίρεσαν υπάλληλοι του ΓΛΚ,
ενώ οι Anonymous ανέλαβαν την ευθύνη
- Τρεις υποθέσεις υποκλοπών από τον Ιούλιο μέχρι σήμερα - ΕΛΛΑΔΑ 9 Jan, 2013

Ιοί Υπολογιστών

Οι ιοί των υπολογιστών είναι μικρά προγράμματα λογισμικού, τα οποία εγκαθίστανται στον υπολογιστή μας εν αγνοία του χρήστη και ενεργοποιούνται είτε σε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια. Είναι σχεδιασμένα να εξαπλώνονται από τον έναν υπολογιστή στον άλλον και να παρεμβαίνουν στη λειτουργία του υπολογιστή. Ένας ιός μπορεί να αλλοιώσει ή να διαγράψει δεδομένα από τον υπολογιστή σας, να χρησιμοποιήσει το πρόγραμμα ηλεκτρονικού ταχυδρομείου σας για να εξαπλωθεί σε άλλους υπολογιστές ή ακόμα και να διαγράψει τα πάντα από το σκληρό σας δίσκο.



Οι ιοί εξαπλώνονται πιο εύκολα μέσω των συνημμένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου ή των άμεσων μηνυμάτων. Γι' αυτό είναι απαραίτητο να μην ανοίγετε ποτέ συνημμένα ηλεκτρονικού ταχυδρομείου, εκτός εάν γνωρίζετε από ποιόν είναι και τα περιμένετε. Οι ιοί μεταμφιέζονται σε συνημμένα με αστείες φωτογραφίες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο. Επίσης, εξαπλώνονται μέσω λήψεων από το Internet. Μπορούν να κρυφτούν σε νόμιμο λογισμικό ή άλλα αρχεία ή προγράμματα των οποίων ενδεχομένως να κάνετε λήψη.

Υπάρχουν πολλοί τύποι υπολογιστικών ιών, όπως [ιοί αρχείων](#), [ιοί της περιοχής εκκίνησης](#) (boot sector), [ιοί σκουλήκια](#) και προγράμματα [δούρειοι ίπποι](#) (Trojan Horse).

➤ **Ιοί περιοχής εκκίνησης** - Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν.

➤ **Ιοί αρχείων** – Σ' αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

➤ **Ιοί σκουλήκια (Worms):** Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων. Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία. Στη συνέχεια γίνεται αναφορά σε δύο ιούς σκουλήκια τον Blaster και τον Sobig.

Η έκρηξη του Blaster έγινε την 11η Αυγούστου 2003. Το μεσημέρι της ίδιας μέρας είχαν μολυνθεί 7.000 υπολογιστές και το βράδυ 330.000. Ο ιός ήταν προγραμματισμένος να επιτεθεί

στο δικτυακό τόπο της Microsoft στις 16 Αυγούστου. Οι τεχνικοί της Microsoft πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών της εταιρίας και η επίθεση απέτυχε.

Μια εβδομάδα αργότερα έκανε την εμφάνισή του η έκτη έκδοση ενός ακόμα ιού του Sobig. Ο ιός αυτός μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας. Ο Sobig ήταν πολυμορφικός ιός. Όταν οι χρήστες άνοιγαν το μολυσμένο μήνυμα ο κώδικας του ιού ξεκινούσε την αναπαραγωγή του. Έβρισκε τις διευθύνσεις αλληλογραφίας του χρήστη και έστελνε μολυσμένα μηνύματα. Οι μολυσμένοι υπολογιστές θα επιχειρούσαν να συνδεθούν στο διαδίκτυο και Παρασκευή και Κυριακή από τις 0:00 έως τις 3:00. Τότε επικοινωνούσαν με 20 διακομιστές και θα κατέβαζαν επιπλέον λογισμικό.

Η εξάπλωση του ιού ήταν τεράστια. Οι διακομιστές αλληλογραφίας κατακλύστηκαν από μηνύματα που μετέφεραν τον ιό. Η America On Line (παροχέας διαδικτύου στις ΗΠΑ) έλαβε σε μία μέρα 31 εκατομμύρια μηνύματα (τρεις φορές περισσότερα από το κανονικό). Τα 11,5 εκατομμύρια ήταν μολυσμένα μηνύματα με τον Sobig. Μέσα σε μία εβδομάδα στάλθηκαν 200 εκατομμύρια μολυσμένα μηνύματα. Η όλη δραστηριότητα του ιού σταμάτησε στις 10 Σεπτεμβρίου καθώς έτσι είχε προγραμματιστεί ο ιός.

➤ **Δούρειος ίππος** - Αυτοί οι ιοί δρουν αθόρυβα. Μολύνουν τον υπολογιστή και αναμένουν κάποιο γεγονός ανάλογα με το προγραμματισμό τους. Συνήθως δεν πολλαπλασιάζοντας και δεν εξαπλώνονται σε άλλους υπολογιστές. Για να μολυνθεί ένας υπολογιστής ο χρήστης του πρέπει να κατεβάσει και να εκτελέσει τον ιό. Αυτό γίνεται συνήθως με ένα ηλεκτρονικό μήνυμα όπου ο ιός είναι συνημμένος και ο χρήστης πείθεται να τον εκτελέσει. Όταν ο ιός δούρειος ίππος εγκατασταθεί στέλνει μέσω διαδικτύου τις κατάλληλες πληροφορίες στο δημιουργό του ώστε αυτός να πάρει τον έλεγχο του υπολογιστή και να χρησιμοποιηθεί σε διάφορες παράνομες και επιβλαβείς ενέργειες.

Ακατάλληλο Περιεχόμενο

Ο όρος ακατάλληλο περιεχόμενο είναι υποκειμενικός σε σχέση με την ηλικία ή και την ψυχική κατάσταση του κάθε ατόμου. Για παράδειγμα ένα περιεχόμενο μπορεί να θεωρηθεί μη αποδεκτό για ένα μικρό παιδί εάν αυτό περιέχει ακατάλληλο υλικό, το οποίο μπορεί να προκαλέσει ψυχικές διαταραχές, να σοκάρει ή ακόμα να προωθήσει λάθος συμπεριφορές. Το ίδιο περιεχόμενο μπορεί όμως να θεωρηθεί κατάλληλο για ένα μεγαλύτερο σε ηλικία άτομο.

Συνήθως με τον όρο ακατάλληλο περιεχόμενο, αναφερόμαστε σε περιεχόμενο, το οποίο μπορεί να περιλαμβάνει ρατσιστικό ή ξενοφοβικό περιεχόμενο, προώθηση επιβλαβών συμπεριφορών, προώθηση τυχερών παιχνιδιών, παρουσίαση πορνογραφικού υλικού, προώθηση βίας κ.λ.π.

Ανεπιθύμητα Μηνύματα (Spam)

Ανεπιθύμητα Μηνύματα θεωρούνται τα μηνύματα εκείνα που υπό κανονικές συνθήκες οι χρήστες δεν θα επέλεγαν να δουν και τα οποία διανέμονται σε μεγάλο αριθμό παραληπτών. Παραδείγματα ανεπιθύμητων μηνυμάτων είναι μηνύματα που περιέχουν διαφημιστικά για αμφίβολα προϊόντα, μηνύματα με περιεχόμενο που συσχετίζεται με ψευδοτυχερά παιχνίδια, ψευδονομικές υπηρεσίες, πορνογραφικό υλικό κτλ. Πολύ συχνό φαινόμενο είναι και η λήψη αλυσιδωτών μηνυμάτων (chain e-mails). Τα μηνύματα αυτά είναι, συνήθως, ανεπιθύμητα και ο αποστολέας ζητά από τον παραλήπτη να προωθήσει το μήνυμα σε άλλα άτομα, τα οποία γνωρίζει. Ο κίνδυνος εδώ, είναι ότι κάθε φορά που προωθούμε ένα μήνυμα, αν δεν είμαστε προσεχτικοί, μαζί με αυτό εμφανίζεται και η ηλεκτρονική διεύθυνση όλων των προηγούμενων ατόμων που προώθησαν το ίδιο μήνυμα. Έτσι δεν γνωρίζουμε ποιος θα παραλάβει το μήνυμα και τι θα κάνει με τις ηλεκτρονικές διευθύνσεις, οι οποίες θα εμφανίζονται σε αυτό.

Αποξένωση από τον Πραγματικό Κόσμο

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



Αρκετοί είναι αυτοί οι οποίοι ξοδεύουν άπειρες ώρες μπροστά στον υπολογιστή παίζοντας διαδικτυακά παιχνίδια, σερφάροντας στο Διαδίκτυο ή ακόμα και επικοινωνώντας με φίλους τους μέσω του Διαδικτύου. Η πολύωρη

ενασχόληση με τα πιο πάνω, οδηγεί πολλές φορές στην Αποξένωση από τον Πραγματικό Κόσμο εφόσον επιτρέπει στους ανθρώπους να ψυχαγωγούνται ή να επικοινωνούν χωρίς τα πλεονεκτήματα και τα μειονεκτήματα της προσωπικής επαφής. Αρκετοί είναι αυτοί για παράδειγμα οι οποίοι αναπτύσσουν Διαδικτυακές (on-line) σχέσεις χωρίς να εγκαταλείπουν τα σπίτια τους.

Όλα αυτά γίνονται σε βάρος του χρόνου που διαφορετικά μπορούν να έχουν διαθέσιμο για τη συμμετοχή σε άλλες δραστηριότητες με φίλους, γείτονες ή ομάδες ανθρώπων με κοινά ενδιαφέροντα. Ως αποτέλεσμα, κάποιοι άνθρωποι δεν μπορούν να ταυτιστούν με τους άλλους νιώθοντας αποκλεισμένοι στην εντός του Διαδικτύου κοινωνική τους ζωή.

Αποπλάνηση (Grooming)

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

Στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι ποιος είναι ο συνομιλητής μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε κάμερα. Έτσι, πολλοί επιτήδριοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (κυρίως για την ηλικία τους) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική με αυτά σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ. τόπο διαμονής, τα ενδιαφέροντά τους, τα χόμπι τους, τις σεξουαλικές τους εμπειρίες κ.λ.π.).



Τα δωμάτια επικοινωνίας (chat rooms) είναι ένας δημοφιλής τρόπος επικοινωνίας μεταξύ των νέων αλλά και δημοφιλές μέσο αποπλάνησης (Shannon, 2008). Αυτά είναι εικονικά μέρη όπου άνθρωποι από όλο τον κόσμο μπορούν να «συναντηθούν» και να «συνομιλήσουν» μέσω μηνυμάτων. Πρέπει να γνωρίζουμε όμως ότι οποιοσδήποτε μπορεί, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις μας. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όπου κάποιος από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλίας, έχουν δεχτεί προτροπές από αγνώστους για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίστηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από κακόβουλους αγνώστους, τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας (Craven, et al, 2006).

Βία Παιχνίδια

Σύμφωνα με έρευνες, εκατομμύρια άτομα αφιερώνουν χρόνο σε καθημερινή βάση σε ηλεκτρονικά παιχνίδια (<http://www.appdata.com>). Όπως στην αγορά έτσι και στο Διαδίκτυο υπάρχουν διάφορες κατηγορίες παιχνιδιών. Η πιο δημοφιλής κατηγορία παιχνιδιών είναι η κατηγορία παιχνιδιών δράσης η οποία χωρίζεται σε άλλες υποκατηγορίες, όπως παιχνίδια πολεμικών τεχνών (Beat'em up), λαβυρίνθων (maze), πλατφόρμας (platform), βολών (shooters) κ.ά.

Η κατηγορία βολών θεωρείται η πλέον βίαια κατηγορία παιχνιδιών και έχει κατακριθεί ιδιαίτερα για τα κακά πρότυπα και τις αρνητικές επιδράσεις που πιθανότατα να έχει, ειδικά σε νεαρά άτομα. Όπως λέει και το όνομα, σκοπός είναι να χρησιμοποιήσουμε όπλα, ώστε να εξοντώσουμε τους αντιπάλους και να ολοκληρώσουμε τις αποστολές του παιχνιδιού. Βία όμως που εκφράζουμε στα παιχνίδια μπορεί να την εμφανίσουμε και στην κανονική μας ζωή. Ανησυχητικά είναι τα συμπεράσματα που προκύπτουν από τις έρευνες των Πανεπιστημίων της Καλιφόρνια και του Σαν Φρανσίσκο στις ΗΠΑ. Οι μελετητές βρήκαν ότι η βία στα ηλεκτρονικά παιχνίδια προκαλεί

αντικοινωνική και πολεμοχαρή συμπεριφορά στην καθημερινότητα των παιδιών ηλικίας 18 έως 21 (Ferguson, 2007).

Αυτό το ενισχύει και ο οργανισμός ISFE (Interactive Software Federation of Europe), όπου σύμφωνα με έρευνές του, υψηλά επίπεδα έκθεσης σε βίαια ηλεκτρονικά παιχνίδια σχετίζονται έντονα με αυξανόμενη επιθετική συμπεριφορά στο σχολείο και στο ελεύθερο παιχνίδι και οδηγούν στην εγκληματικότητα. Εδώ υπάρχει το ζήτημα του ενδεχομένως ακατάλληλου για την ηλικία του παιδιού περιεχόμενο. Για το σκοπό αυτό η βιομηχανία παιχνιδιών εφαρμόζει κώδικες σήμανσης των παιχνιδιών όπως π.χ. Πανευρωπαϊκού Συστήματος Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (Pan European Game Information - PEGI). Στη σήμανσή του, το PEGI αναφέρει τόσο την ηλικιακή ομάδα στην οποία απευθύνεται ο κάθε τίτλος, καθώς και τα στοιχεία που περιλαμβάνει (π.χ. βία, ρατσιστικά στοιχεία, κ.ά.).

Εθισμός (Internet Addiction)

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

Ένα άτομο είναι εθισμένο όταν χαρακτηρίζεται από τουλάχιστο τρία από τα πιο κάτω:

- Χρήση του Διαδικτύου για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο
- Κατανάλωση υπερβολικού χρόνου ή και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο
- Συμπτώματα Συνδρόμου Απόσυρσης, όπως για παράδειγμα άγχος, έμμονη σκέψη για το Διαδίκτυο, όνειρα για το Διαδίκτυο
- Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης
- Μείωση λειτουργικότητας του ατόμου. Συνήθως παραμελούν την προσωπική τους υγεία, γευματίζουν ανθυγιεινά, σταματούν τα αγαπημένα τους ενδιαφέροντα, εγκαταλείπουν το σχολείο, συγκρούονται έντονα στο σπίτι με τους γονείς τους, έχουν μεγάλη ένταση και θυμό που οδηγεί ακόμα και στη βία (Chakraborty, 2010)
- Συνέχιση χρήσης του Διαδικτύου παρά τη γνώση της παραπάνω δυσλειτουργίας

Σύμφωνα με στατιστικά στοιχεία της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) στην Ελλάδα, το φαινόμενο είναι συχνότερο σε αγόρια, σε δυσλειτουργικές οικογένειες και σε παιδιά με καταθλιπτικά συναισθήματα ή σύνδρομο υπερκινητικότητας.



Εκφοβισμός (Cyberbullying)

Εκφοβισμός είναι δυνατό να συμβεί μέσω του Διαδικτύου και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης.

Ο Διαδικτυακός Εκφοβισμός συνήθως έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού, προσβλητικού ή πρόστυχου ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο. Κάποιες φορές ο εκφοβισμός μπορεί να οδηγήσει στο να περιθωριοποιηθούν και να αποκλειστούν άτομο ή άτομα από άλλους.

Ο Διαδικτυακός Εκφοβισμός διαφέρει από τα άλλα είδη εκφοβισμού αφού επεμβαίνει στον προσωπικό χώρο του παραλήπτη. Ο εκφοβισμός αυτός είναι δύσκολο να περιοριστεί, αφού δεν υπάρχει περιορισμός ούτε των μηνυμάτων που διανέμονται ηλεκτρονικά, ούτε του αριθμού των παραληπτών που μπορούν να γίνουν δέκτες αυτών των μηνυμάτων. Η σύγχρονη έρευνα έχει δείξει ότι το σχολείο, όταν υπάρχει πληροφόρηση και ενημέρωση του προσωπικού, μπορεί να αντιμετωπίσει το πρόβλημα (Bhat, 2008).



Επιβλαβείς Συμπεριφορές

Το γεγονός ότι το Διαδίκτυο δεν είναι υπό τη δικαιοδοσία οποιουδήποτε καθιστά αδύνατο τον έλεγχο του περιεχομένου του. Ιστοσελίδες για βουλιμία, ανορεξία, αυτοκτονία, σατανισμό και τυχερά παιχνίδια υπάρχουν πολλές και παρακινούν σε επιβλαβείς συμπεριφορές. Για παράδειγμα, σύμφωνα με το Eating Disorders Review (2003), άρχισαν να εμφανίζονται ιστοσελίδες υπέρ των διατροφικών διαταραχών και, παρά τις προσπάθειες που κατέβαλαν ομάδες εναντίον της ανορεξίας και της βουλιμίας, αυτές οι ιστοσελίδες παραμένουν προσβάσιμες. Σύμφωνα με έρευνα από την British Medical Journal, οι άνθρωποι που ψάχνουν πληροφορίες για τρόπους αυτοκτονίας είναι πιθανότερο να βρουν σελίδες που την ενθαρρύνουν παρά σελίδες που προσφέρουν βοήθεια και στήριξη. Από 240 ιστοσελίδες που βρέθηκαν το 2008 να αναφέρουν την αυτοκτονία οι 45 περίπου την ενθάρρυναν, την προωθούσαν ή την διευκόλυναν.

Ηλεκτρονικός Τζόγος

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

Ένα από τα βασικότερα προβλήματα του τζόγου είναι η απώλεια χρημάτων. Κάποιος μπορεί να χάσει τις οικονομίες του, το σπίτι του, την περιουσία του ακόμη και το/τη σύζυγό της/του. Πολλοί είναι αυτοί που εθίζονται και δεν μπορούν να σταματήσουν πιστεύοντας πως στον επόμενο γύρο θα πάρουν τα λεφτά τους πίσω. Έτσι εκτός από την σπατάλη πολλών χρημάτων

οδηγούνται παράλληλα στη σπατάλη πολλού χρόνου, παραμέληση των υποχρεώσεών τους με όλες τις επακόλουθες συνέπειες του εθισμού. Είναι γνωστό ότι ακόμα και η ενασχόληση με περιβάλλοντα τζόγου, στα όπου δεν γίνεται χρήση πραγματικών χρημάτων, μπορεί να προκαλέσει τον εθισμό (Hyder et al, 2008).

Η ευκολία πρόσβασης σε ιστοσελίδες ηλεκτρονικού τζόγου αυξάνει τους κινδύνους εμπλοκής παιδιών και εφήβων σε τέτοιες δραστηριότητες.

Παιδική Πορνογραφία

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

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές:

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

Σύμφωνα με ανακοίνωση στην ιστοσελίδα του φορέα για την ασφάλεια του Διαδικτύου στην Κύπρο (www.cyberethics.info) τον Αύγουστο του 2009, η 14η ιστοσελίδα προτίμησης των Κυπρίων είναι πορνογραφικού περιεχομένου. Η 14η θέση είναι η ψηλότερη θέση προτίμησης για πορνογραφική ιστοσελίδα ανάμεσα σε ευρωπαϊκές χώρες. Αυτές οι πληροφορίες είναι ανησυχητικές, γιατί σύμφωνα με ειδικούς κλινικούς σεξολόγους, οι άνθρωποι που εθίζονται στην πορνογραφία τείνουν να έχουν διαταραγμένη αντίληψη για τις ανθρώπινες σχέσεις, κάτι που μπορεί να τους αποξενώσει από τους συντρόφους τους. Επίσης, επισημαίνουν ότι οι ανήλικοι είναι πιο επιρρεπείς σε αυτό γιατί τους λείπει η συναισθηματική ωριμότητα.



Η εξάπλωση των κυκλωμάτων παιδοφιλίας είναι ανησυχητική. Τα κυκλώματα αυτά είναι ομάδες ατόμων, τα οποία εργάζονται μαζί μέσω του Διαδικτύου με στόχο τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Τέτοιες ενέργειες αποτελούν έγκλημα και υπόκεινται στο νόμο.



Παραβίαση Ιδιωτικότητας

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο “προσφέρουμε” προσωπικές πληροφορίες. Αυτές οι πληροφορίες είναι σαν ένα γρίφος που πρέπει να συμπληρωθεί για να αποκαλυφθεί η εικόνα μας. Η περιήγηση μας στο Διαδίκτυο έχει πολλά κοινά με τη ζωή μας στο φυσικό κόσμο. Έτσι τίθενται κάποια πολύ σοβαρά ζητήματα: της προστασίας των προσωπικών μας δεδομένων, της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας και το γεγονός πως ό,τι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη.

Όταν στέλνουμε ηλεκτρονικά μηνύματα σίγουρα δίνουμε πληροφορίες στο άτομο με το οποίο επικοινωνούμε. Εάν δεν είμαστε προσεχτικοί, μπορεί επίσης να δώσουμε πληροφορίες σε ένα μεγάλο αριθμό ατόμων, συμπεριλαμβανομένου του εργοδότη μας, της κυβέρνησης, του παροχέα ηλεκτρονικού ταχυδρομείου και οποιουδήποτε βρίσκεται στη διαδρομή του μηνυματός μας προς τον παραλήπτη. Προσεχτικοί πρέπει να είμαστε και όταν συμμετέχουμε σε ομάδες συζητήσεων (groups ή listserves) του Διαδικτύου όπου είμαστε μέλη και δίνουμε προσωπικές πληροφορίες σε όλα τα μέλη της ομάδας (π.χ. διεύθυνση του ηλεκτρονικού μας ταχυδρομείου). Δεν απαγορεύεται σε μέλος να πάρει και να διανέμει τη διεύθυνσή μας.

Σημαντικό είναι να γνωρίζουμε ότι κατά την πλοήγησή μας στο Διαδίκτυο με χρήση οποιουδήποτε φυλλομετρητή αφήνουμε ίχνη. Όταν απλά κοιτάζουμε πληροφορίες στο Διαδίκτυο πολύ πιθανόν ο φυλλομετρητής μας να δίνει τον αριθμό του υπολογιστή και τις σελίδες που επισκεφθήκαμε στον παροχέα Διαδικτύου. Αν ο φυλλομετρητής χειρίζεται και το ηλεκτρονικό μας ταχυδρομείο, τότε πολύ πιθανόν να παρέχει την ηλεκτρονική διεύθυνση και το τηλέφωνό μας.



Επίσης πολλές από τις ιστοσελίδες που επισκεπτόμαστε, φυλάνε στον υπολογιστή μας δεδομένα για την επίσκεψη μας, τα λεγόμενα “Cookies”. Τα Cookies είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, πληροφορίες της εγγραφής μας σε μια σελίδα, προτιμήσεις, διαδικτυακά «καλάθια με ψώνια» και λοιπά. Οι νόμιμες εταιρείες χρησιμοποιούν τα Cookies για να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Παράνομες εταιρείες χρησιμοποιούν Cookies για να πάρουν πληροφορίες για τους χρήστες και να τις πουλήσουν σε εταιρείες Marketing.

Προσεχτικοί πρέπει να είμαστε και όταν στέλνουμε Μηνύματα της Στιγμής (Instant Messages) π.χ. με Google Talk ή με Microsoft Live Messenger. Πρέπει να γνωρίζουμε ότι πολλές από αυτές τις εταιρείες αυτόματα αποθηκεύουν τα μηνυματά μας, εκτός και εάν έχουμε κάνει τις ανάλογες ρυθμίσεις. Κοινωνικά Δίκτυα όπως το Facebook και MySpace επιτρέπουν την αποστολή φωτογραφιών και την αποθήκευση προσωπικών σημειώσεων. Προσωπικές πληροφορίες που ανταλλάσσονται σε τέτοια δίκτυα μπορεί να προκαλέσουν προβλήματα του χρήστη με το σχολείο, τον εργοδότη του και όχι μόνο. Τέτοιες ιστοσελίδες δέχονται συχνά και με ευκολία επισκέψεις από παιδοφίλους που ενδιαφέρονται είτε να παραπλανήσουν ανήλικους σε πραγματικές συναντήσεις ή να κλέψουν φωτογραφίες και πληροφορίες που ανταλλάσσονται από άτομα που χρησιμοποιούν αυτά τα δίκτυα.

Ίχνη στο Διαδίκτυο είναι δυνατό να αφήσουμε και κατά τη χρήση ιστολογίων (Blog). Πολλοί νεαροί που χρησιμοποιούν το Διαδίκτυο, έχουν δημιουργήσει το δικό τους ιστολόγιο (Blog), κάτι σαν ενημερωτικό φυλλάδιο ή εφημερίδα, το οποίο ανανεώνεται συχνά και είναι για ελεύθερη πρόσβαση. Οι χρήστες των ιστολογίων μπορούν να καταθέσουν σχόλια. Σε κάποια από τα ιστολόγια χρειάζεται να κάνει κάποιος εγγραφή για να μπορεί να σχολιάσει, δίνοντας έτσι πληροφορίες όπως ηλεκτρονική διεύθυνση, όνομα κ.λπ.

Παραπληροφόρηση (Misinformation)

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

Παραποίηση Γλώσσας

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

Αυτό ξεκίνησε, επειδή η χρήση του ελληνικού αλφαβήτου στην τεχνολογία ήταν είτε αδύνατη είτε δύσκολη. Παρόλο που τα τελευταία χρόνια πολλοί υπολογιστές και προγράμματα χρησιμοποιούν την ελληνική γλώσσα, πάρα πολλοί δεν επικοινωνούν στα ελληνικά αλλά σε greeklish όταν στέλνουν μηνύματα στο κινητό ή όταν χρησιμοποιούν το Διαδίκτυο. Υπάρχουν επίσης ιστοσελίδες όπου η γλώσσα που χρησιμοποιείται δεν είναι τα Ελληνικά αλλά τα greeklish και σε σελίδες του Διαδικτύου διατίθενται greeklish converters, προγράμματα που μετατρέπουν greeklish σε Ελληνικά και το αντίστροφο. Όλα αυτά μπορούν να οδηγήσουν όχι μόνο στη παραποίηση της γλώσσας μας αλλά, όπως κάποιοι υποστηρίζουν και στην αλλοίωση της ταυτότητας των Ελλήνων.

Επίσης είναι πολύ συχνό φαινόμενο οι νεαροί να χρησιμοποιούν εικόνες ή διάφορα άλλα ακρώνυμα για να επικοινωνήσουν γρήγορα και άμεσα. Αυτά συμπεριλαμβάνουν τα εικονίδια συναισθημάτων (emotions) και τα ακρώνυμα. Τα Emotions είναι εικονίδια τα οποία στόχο έχουν να εκφράσουν κάποια συναισθήματα. Μπορούμε να δημιουργήσουμε ένα emotion πληκτρολογώντας τον κατάλληλο συνδυασμό χαρακτήρων (π.χ. ο συνδυασμός :-) σημαίνει «χαμόγελο»). Τα Ακρώνυμα είναι συνδυασμοί πλήκτρων για συντομογραφία λέξεων ή ακόμα και προτάσεων (π.χ. ο συνδυασμός POS σημαίνει «Parent Over Shoulder»).

Υποκλοπή Προσωπικών στοιχείων(Phishing)

Υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών,ης κ.λπ). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα (cracker) να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς, κ.λπ.

Κάποιοι θεωρούν τις Απάτες (Scams) ως ένα είδος υποκλοπής, μόνο που οι Απάτες συνήθως δεν ενδιαφέρονται για τις προσωπικές μας πληροφορίες, αλλά προσπαθούν να προκαλέσουν τον οίκτο μας για τον ανθρώπινο πόνο ώστε να προσφέρουμε λεφτά για να βοηθήσουμε ένα δήθεν καλό σκοπό. Για παράδειγμα, σχεδόν κάθε μεγάλη καταστροφή (σεισμός, πλημμύρες, πείνα, πόλεμος) έχει προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες να προσφέρουν λεφτά για να βοηθήσουν για κάποιο καλό σκοπό. Πολλοί άνθρωποι έχουν χάσει πολλά λεφτά για τέτοιους “καλούς” σκοπούς. Κάποιοι έχουν χάσει ακόμα και τη ζωή τους, καθώς έχουν ταξιδέψει σε άλλες χώρες για να γνωρίσουν αυτούς που επωφελούνταν των προσφορών τους.

Φυσικές Παθήσεις

Με την εισαγωγή του Διαδικτύου στη ζωή μας, οι ώρες χρήσης του υπολογιστή έχουν αυξηθεί κατακόρυφα. Η πολύωρη χρήση του Διαδικτύου είτε είναι για έρευνα είτε για παιχνίδι είτε για κοινωνικοποίηση εγκυμονεί κινδύνους για την υγεία μας. Πέρα από τις διαταραχές στην όραση και τις υποψίες για ενδεχόμενα προβλήματα εξαιτίας της έκθεσης σε ακτινοβολία, κυρίως από τις οθόνες, εκείνοι που ασχολούνται για ώρες μπροστά στον υπολογιστή χωρίς διάλειμμα ή εναλλαγή δραστηριοτήτων κάνουντας μεγάλο αριθμό επαναλαμβανόμενων κινήσεων μπορεί να προσβληθούν από διάφορες μυοσκελετικές παθήσεις. Κακώσεις όπως ο ευθυσισμός του αυχένα, ο πόνος του αγκώνα (tennis elbow), τενοντίτιδα, πηχαιοκαρπική άρθρωση και άλλες παθήσεις έχουν συνδέσει το όνομά τους με την υπερβολική χρήση του υπολογιστή.

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Υπάρχουν πολλοί τρόποι για την αντιμετώπιση των κινδύνων του Διαδικτύου. Μερικοί είναι και οι παρακάτω:

- Ποτέ δε δίνουμε προσωπικά μας στοιχεία μέσα από το Διαδίκτυο, όπως τον αριθμό του τηλεφώνου μας, τη διεύθυνση του σχολείου μας ή του σπιτιού μας, αριθμούς πιστωτικών καρτών κ.τ.λ.
- Κλείνουμε τον υπολογιστή μας όταν δούμε ότι κάτι μας ενόχλησε.
- Δε πρέπει να απαντάμε σε ανώνυμα ή προσβλητικά ηλεκτρονικά μηνύματα. Το καλύτερο που έχουμε να κάνουμε, όταν παίρνουμε τέτοιου είδους μηνύματα, είναι να τα σβήνουμε αμέσως από τον υπολογιστή μας, χωρίς βέβαια να απαντήσουμε σε αυτά. Αν κάνουμε το λάθος και απαντήσουμε, τότε δίνουμε το δικαίωμα σε αυτούς που τα στέλνουν να συνεχίσουν να μας ενοχλούν.
- Ποτέ δε μένουμε για πολλή ώρα συνδεδεμένοι στο Διαδίκτυο χωρίς να υπάρχει πραγματικός λόγος. Σερφάροντας άσκοπα στο Διαδίκτυο, αναπόφευκτα θα επισκεφτούμε σελίδες αισχρού περιεχομένου, σελίδες που θα μας προτρέψουν να δοκιμάσουμε τυχικά παιχνίδια και πολλά άλλα.
- Ποτέ δε συναντάμε κάποιον που έχουμε γνωρίσει μέσω Διαδικτύου. Θα πρέπει να θυμόμαστε ότι σχεδόν πάντα όλοι όσοι επικοινωνούν μέσω αυτού, δίνουν ψεύτικα στοιχεία, τις περισσότερες φορές. Αν για οποιονδήποτε λόγο πρέπει να συναντήσουμε κάποιον, τότε θα πρέπει οπωσδήποτε να συνοδευόμαστε από άλλα άτομα.
- Αν θέλουμε να χρησιμοποιήσουμε το Διαδίκτυο για αγορές, τότε καλό θα είναι να απευθυνθούμε στις εμπορικές τράπεζες για να αποκτήσουμε τις πιστωτικές κάρτες που έχουν σχεδιαστεί ειδικά για ηλεκτρονικό εμπόριο. Έτσι μειώνετε ο κίνδυνος ηλεκτρονικής κλοπής.
- Τέλος, πρέπει να διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο με άλλες πηγές, γιατί υπάρχει περίπτωση να είναι λανθασμένες.

ΕΠΙΛΟΓΟΣ

Η ερευνητική εργασία «Ασφάλεια στο Διαδίκτυο», έφτασε στο τέλος της. Όλα τα μέλη της ομάδας δουλέψαμε γι' αυτήν την εργασία και αποκτήσαμε μια ωραία εμπειρία.

Όλη η διαδικασία μας φάνηκε λίγο κουραστική, αλλά άξιζε τον κόπο γιατί αποκομίσαμε αρκετές γνώσεις και ομαδικό πνεύμα.

Επί τη ευκαιρία, ας ευχαριστήσουμε τον καθηγητή μας, κ. Γιάννη Δετοράκη, ο οποίος συνέβαλε στην προσπάθειά μας για την διεξαγωγή της ερευνητικής εργασίας μας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

<http://www.cyberethics.info/cyethics1/index.php?lang=el>

<http://www.police.gov.cy/police/police.nsf/All/42956AEC03E802http://www.youthboard.org.cy/5DC22578A900271F4A?OpenDocument>

<http://www.cytanet.com.cy/>

<http://www.pccpwc.org/>

<http://www.kathimerini.gr/>