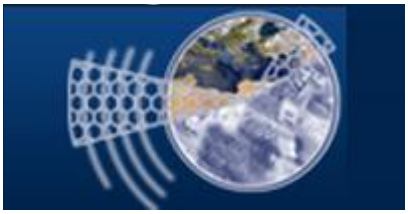
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων



Πτυχιακή Εργασία

Τίτλος:

Πληροφοριακό σύστημα για μελέτη Cyberbullying στο Νομό Ηρακλείου

Περτσελή Ζαφειρένια ΑΜ:2311

Περγιανάκη Ιωάννα ΑΜ:2310

Επιβλέπων Καθηγητής: Νίκος Παπαδάκης

ΗΡΑΚΛΕΙΟ 2015

SUMMARY

The subject of this thesis is the theoretical research on Internet Addiction. The purpose of this project is to present the penetration of the new technologies and the Internet in the daily lives of young people of today□s society and to approach from a theoretical perspective the question of online addiction. With regard to all these, cybercrime is certainly dominant in this thesis.

For the preparation of the thesis, a lengthy bibliographical research took place initially. Then, the general objectives were set up. Subsequently, the separation of the objectives, which consist the main body of the work, took place. The appendix, where relevant pictures and research results in tabular format are included, is part of the writing.

The lengthy study of the issue led to some important main conclusions. The young people of this era come very early in contact with the computer and the Internet via online games or social network. This early contact should bring the user only positive effects. However, the excessive use of the Internet causes addiction with all that this entails. The most important tool at the society□s disposal in order to prevent and tackle this addiction is to inform all users. The Internet does not have bad intentions by itself. Misuse causes serious impacts on its user.

Summarizing, the computer and the Internet are the most powerful media and means of communication of the modern era, provided that they are properly used and not abused.

Key words

Addiction, Internet, Cybercrime, Prevention, Computer, Information

ΠΕΡΙΛΗΨΗ

Το θέμα της παρούσας πτυχιακής εργασίας είναι η θεωρητική έρευνα για τον Εθισμό στο Διαδίκτυο. Σκοπός της εργασίας είναι να παρουσιάσει τη διείσδυση των νέων τεχνολογιών και του διαδικτύου στην καθημερινότητα των νέων της σημερινής κοινωνίας και να προσεγγίζει από τη θεωρητική σκοπιά το ζήτημα του διαδικτυακού εθισμού. Με αφορμή όλων αυτών φυσικά, το ηλεκτρονικό έγκλημα κατέχει δεσπόζουσα θέση στην παρούσα πτυχιακή εργασία.

Για την εκπόνηση της πτυχιακής εργασίας σε πρώτη φάση έλαβε χώρα μια μακροσκελής βιβλιογραφική έρευνα. Έπειτα καθορίστηκαν οι γενικοί στόχοι. Στη συνέχεια έγινε ο διαχωρισμός των κεφαλαίων, τα οποία αποτέλεσαν τον κυρίως κορμό της εργασίας. Μέρος του συγγράμματος αποτελεί το παράρτημα, στο οποίο περιλαμβάνονται σχετικές εικόνες και αποτελέσματα ερευνών σε μορφή πινάκων.

Η μακροσκελής μελέτη του θέματος οδήγησε σε κάποια σημαντικά κύρια συμπεράσματα. Οι νέοι της σημερινής εποχής έρχονται από πολύ νωρίς σε επαφή με τον ηλεκτρονικό υπολογιστή και με το διαδίκτυο, μέσω online παιχνιδιών ή μέσω σελίδων κοινωνικής δικτύωσης. Αυτή η πρόωρη επαφή θα έπρεπε μόνο θετικά αποτελέσματα να επιφέρει στον χρήστη. Ωστόσο, η αλόγιστη χρήση του διαδικτύου προκαλεί τον εθισμό με ότι αυτός συνεπάγεται. Το σημαντικότερο εργαλείο, που διαθέτει η κοινωνία, για την πρόληψη και την αντιμετώπιση αυτού του εθισμού είναι η ενημέρωση όλων των χρηστών. Το διαδίκτυο δεν έχει από μόνο του κακές προθέσεις. Η κακή χρήση είναι αυτή που προκαλεί σοβαρές επιπτώσεις στο άτομο που το χρησιμοποιεί.

Συνοψίζοντας, ο ηλεκτρονικός υπολογιστής και το διαδίκτυο είναι τα πιο ισχυρά μέσα ενημέρωσης και επικοινωνίας της σύγχρονης εποχής, με την προϋπόθεση ότι γίνεται σωστή χρήση τους και όχι κατάχρηση.

Λέξεις – Κλειδιά
Εθισμός, Διαδίκτυο, Ηλεκτρονικό Έγκλημα, Πρόληψη, Ηλεκτρονικός Υπολογιστής, Ενημέρωση

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Η παρούσα μελέτη πραγματοποιήθηκε στο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης, στα πλαίσια εκπόνησης της πτυχιακής μου εργασίας για την απόκτηση του πτυχίου μου, στο τμήμα Μηχανικών Πληροφορικής της Σχολής Τεχνολογικών Εφαρμογών. Στόχος της παρούσας εργασίας είναι η μελέτη των όρων ηλεκτρονικό έγκλημα και εθισμός στο διαδίκτυο, καθώς και η επίδραση τους στο κοινωνικό σύνολο.

ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψης του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα ζωής, εισέρχονται και παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εθισμού αλλά και εγκληματικότητας. Αυτές οι μορφές εγκληματικότητας προσδιορίζονται με τον όρο ηλεκτρονικό έγκλημα και εθισμός στο διαδίκτυο.

Όλα τα παραπάνω αποτέλεσαν το έναυσμα για την επιλογή της πτυχιακής και τη διεξοδική μελέτη των προβλημάτων αυτών. Μέσα από θεωρητική έρευνα των φαινομένων που προαναφέρθηκαν, καθορίστηκαν οι στόχοι της εργασίας.

Στόχοι της πτυχιακής εργασίας είναι:

- Ανάλυση του όρου Διαδίκτυο σαν πρώτο βήμα για τη βαθύτερη κατανόηση των προβλημάτων που προκύπτουν από την υπερβολική χρήση.
- Ανάπτυξη του όρου Εθισμός στο Διαδίκτυο σαν κοινωνικό πρόβλημα της σύγχρονης εποχής.
- Εντοπισμός των γνώσεων του κοινωνικού συνόλου για το πρόβλημα όπως παρουσιάζεται.
- Παράθεση των εργαλείων επίλυσης του προβλήματος.
- Παρουσίαση του όρου Ηλεκτρονικό Έγκλημα σαν απόρροια του εθισμού στο διαδίκτυο.
- Ανάλυση των μορφών του Ηλεκτρονικού Εγκλήματος.
- Παρουσίαση των μέτρων πρόληψης και προστασίας των χρηστών του διαδικτύου από το Ηλεκτρονικό Έγκλημα.
- Εντοπισμός των τρόπων που μπορούν να ωφεληθούν συγκεκριμένες ομάδες ατόμων-χρηστών του διαδικτύου (ανήλικοι και ενήλικες που χρησιμοποιούν το διαδίκτυο για εργασίες, διασκέδαση, παιχνίδια, επικοινωνία και πληροφόρηση)

Στη συνέχεια, έγιναν, όπως φαίνεται και στον κορμό της εργασίας, προσπάθειες προσέγγισης των όρων Εθισμός στο Διαδίκτυο και Ηλεκτρονικό Έγκλημα. Οι δύο αυτοί ορισμοί αποτελούν σημαντικό κομμάτι της έρευνας.

«Η πληροφορική ως επιστήμη κατέστησε δυνατό εκτός από τη θετική εξέλιξη που έχει επίδραση και στη ζωή μας, φυσικά να υπάρχει και η αρνητική εξέλιξη με την έννοια της κακής και ανεξέλεγκτης χρήσης της, η χρήση από ανθρώπους οι οποίοι κινούνται στο φάσμα της παραβατικότητας, της εγκληματικότητας και του εθισμού. Ως Ηλεκτρονικό Έγκλημα ορίζουμε λοιπόν, αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται από συγκεκριμένες ποινές και από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με χρήση ηλεκτρονικού υπολογιστή και σε εγκλήματα που τελούνται μέσω διαδικτύου, τα Κυβερνοεγκλήματα.»
(http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN).

«Ως εθισμός ορίζεται μια κατάσταση κατά την οποία το άτομο λαμβάνει μια ουσία ή συμμετέχει σε μια δραστηριότητα, η οποία μπορεί να είναι ευχάριστη, αλλά της οποίας η χρήση γίνεται καταναγκαστική και επηρεάζει σημαντικά την λειτουργικότητα του (εργασία, διαπροσωπικές σχέσεις, υγεία). Όπως λοιπόν είναι κατανοητό υπάρχουν δυο τύποι εθισμού, ο εθισμός σε ουσίες (ναρκωτικά, αλκοόλ ,νικοτίνη) και ο εθισμός σε δραστηριότητες (τυχερά παιχνίδια, σεξουαλική δραστηριότητα, διαδίκτυο, αγορές, φαγητό). Ο εθισμός είναι μια επίπονη κατάσταση, καθώς οι πάσχοντες από αυτόν μη έχοντας επίγνωση του προβλήματος και έλεγχο της συμπεριφοράς τους

δημιουργούν δυσλειτουργικές καταστάσεις με επιπτώσεις τόσο στο εαυτό τους όσο και στους άλλους»
(http://www.inpsyche.gr/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B5%CE%B8%CE%B9%CF%83%CE%BC%CF%8C%CF%82)

Η ενασχόληση με το Διαδίκτυο γίνεται ιδιαίτερα ελκυστική εφόσον το άτομο παρουσιάζει κάποιες ανάγκες που βρίσκουν προσωρινή ικανοποίηση μέσα από αυτήν. Οι λόγοι μπορεί να σχετίζονται με στοιχεία της προσωπικότητας του, υποκείμενες ψυχικές διαταραχές (άγχος, κατάθλιψη, κοινωνική φοβία, κ.α.) ή να είναι μία μαθημένη συμπεριφορά που ενισχύθηκε από τον περίγυρο (π.χ. η τάση των γονέων να χρησιμοποιούν τον Η/Υ και το Διαδίκτυο για να αποσπάσουν τη προσοχή των παιδιών τους όπως με την τηλεόραση, το γεγονός ότι όλος κοινωνικός περίγυρος του ατόμου έχει λογαριασμό σε κάποιο μέσο κοινωνικής δικτύωσης κ.α.). Αυτές οι ανάγκες δεν ικανοποιούνται με άλλο τρόπο ή ικανοποιούνται σαφώς ευκολότερα με τη βοήθεια του Διαδικτύου. Το Διαδίκτυο προσφέρει ανωνυμία, εύκολη προσβασιμότητα, μικρό κόστος, απομονώνει από τον περίγυρο και είναι γενικά αποδεκτό ως μέσο. Αυτά τα στοιχεία του μπορεί να βοηθήσουν την έκφραση ψυχικών δυσκολιών μέσω της χρήσης του.

Όσο αφορά τη δομή της πτυχιακής εργασίας, τα κεφάλαια χωρίστηκαν με βάση τις ανάγκες για πιο λεπτομερή έρευνα του αντικειμένου.
Αναλυτικότερα, η εργασία εκτείνεται σε 6 κεφάλαια.

Στο 1ο κεφάλαιο (Διαδίκτυο) προσεγγίζεται η έννοια του Διαδικτύου και πραγματοποιείται μία ιστορική αναδρομή, αναφορικά με την εμφάνιση του διαδικτύου και την παρουσία των νέων τεχνολογιών στη ζωή του ατόμου (ενήλικα και ανηλίκου). Εν συνεχεία, γίνεται αναφορά στις δύο βασικές χρήσεις του Διαδικτύου, δηλαδή στις Πληροφορίες που αναζητά ο χρήστης και στην Επικοινωνία που προσφέρει το Διαδίκτυο ανάμεσα στους χρήστες.

Στο 2ο κεφάλαιο (Εθισμός στο Διαδίκτυο) γίνεται μια προσπάθεια προσέγγισης του όρου Εθισμός, καθώς σύμφωνα με τους ειδικούς, τα όρια ανάμεσα στην υπερβολική χρήση και τον εθισμό είναι ασαφή. Άλλωστε, ο εθισμός στο Διαδίκτυο ανήκει στη κατηγορία των συμπεριφορικών εθισμών – δηλαδή τα προβλήματα που ανακύπτουν όταν μία συγκεκριμένη συμπεριφορά ξεφύγει από τον έλεγχο του ατόμου. Ο συμπεριφορικός εθισμός συχνά συγχέεται με τον υψηλό βαθμό εμπλοκής με τη συγκεκριμένη δραστηριότητα.

Έπειτα, αναλύονται τα αίτια του Εθισμού, τα συμπτώματα που παρουσιάζει ο εθισμένος χρήστης καθώς και οι επιπτώσεις του Εθισμού στο άτομο αλλά και στον κοινωνικό του περίγυρο. Τέλος, γίνεται διαχωρισμός του Εθισμού στις διάφορες Μορφές του, όπως αυτές παρατηρούνται από τους ειδικούς και καταγράφονται από τη σχετική βιβλιογραφία.

Στο 3ο κεφάλαιο (Πρόληψη και Αντιμετώπιση του Εθισμού), δίνεται ιδιαίτερη έμφαση στους τρόπους πρόληψης και προστασίας του ατόμου από τον Εθισμό στο Διαδίκτυο. Συγκεκριμένα, προτείνονται όλα εκείνα τα μέτρα που πρέπει να πάρουν οι γονείς, τα παιδιά, οι εκπαιδευτικοί και οι ειδικοί σε θέματα Εθισμών ώστε να βοηθήσουν τα άτομα που έχουν εθιστεί, ή να προστατευτούν οι ίδιοι από τους κινδύνους του Εθισμού στο Διαδίκτυο. Πρέπει να λαμβάνεται υπόψη, άλλωστε, ότι ο εθισμός στο διαδικτυακό παιχνίδι, ιδιαίτερα συχνό πρόβλημα στον μαθητικό, εφηβικό και φοιτητικό πληθυσμό, μπορεί να είναι η πρώτη παρουσίαση προβληματικής συμπεριφοράς σε αυτές τις ηλικιακές ομάδες . Πολύ συχνά η πρώτη γνωριμία του ατόμου με τον υπολογιστή γίνεται μέσω του ηλεκτρονικού παιχνιδιού όπως και η πρώτη γνωριμία με το διαδίκτυο μέσω του διαδικτυακού παιχνιδιού από τις πολύ μικρές ηλικίες.

Στο 4ο κεφάλαιο (Ηλεκτρονικό Έγκλημα) γίνεται προσέγγιση του όρου Ηλεκτρονικό Έγκλημα. Στη συνέχεια, κατηγοριοποιούνται και αναλύονται οι Μορφές του «Κυβερνοεγκλήματος».

Συγκεκριμένα, παρατηρούνται οι εξής μορφές:

α. Οικονομικό Έγκλημα, Απάτες μέσω διαδικτύου

β. Πορνογραφία, Οι συχνότερες μορφές εθισμού σε ενήλικες είναι σε διαδικτυακό σεξ (cybersex) και θέαση διαδικτυακού πορνογραφικού υλικού (cyberporn). Η επέκταση των σεξουαλικών

διαστροφών και μέσω του διαδικτύου (παιδοφιλία, σεξουαλική παρενόχληση) συνιστά ένα νέο κοινωνικό πρόβλημα της σύγχρονης εποχής.

γ. Κλοπή Προσωπικών Δεδομένων, Cracking και Hacking, Πειρατεία- Διακίνηση Λογισμικού

δ. Απάτη στα ATM – Πιστωτικές Κάρτες,

ε. Έγκλημα στα Social Media (chat rooms). Εφαρμογές όπως τα chat rooms και το instant messaging μπορεί να αποκτήσουν επίσης καταναγκαστικά στοιχεία.

ζ. Διακίνηση Ναρκωτικών, Ξέπλυμα χρήματος

Στο 5^{ο} κεφάλαιο (Πρόληψη – Προστασία Προσωπικών Δεδομένων) αναφέρονται όλα τα εργαλεία προστασίας και πρόληψης από το Ηλεκτρονικό Έγκλημα, σε όλες τις μορφές του, όπως παρουσιάστηκε παραπάνω.

Στο 6^{ο} κεφάλαιο (Έρευνα, Αποτελέσματα Έρευνας) παρατίθενται τα στοιχεία που προέκυψαν από σχετική έρευνα 85 ατόμων καθώς και τα αποτελέσματα αυτής της έρευνας. Επίσης, στο κεφάλαιο αυτό περιλαμβάνεται και ένας σχολιασμός σε μορφή συμπερασμάτων των δεδομένων της έρευνας.

Στο 7^{ο} κεφάλαιο (Συμπεράσματα - Αξιολόγηση) καταγράφονται τα γενικά συμπεράσματα που προέκυψαν από τη θεωρητική έρευνα, καθώς και λαμβάνοντας υπόψη τις σχετικές έρευνες. Τέλος, επιχειρείται μια συνολική αξιολόγηση της πτυχιακής εργασίας.

Στο Παράρτημα παραθέτονται πίνακες, οι οποίοι παρουσιάζουν αποτελέσματα ερευνών που έχουν πραγματοποιηθεί για το παραπάνω αντικείμενο, καθώς και σχετικές εικόνες.

ΚΕΦΑΛΑΙΟ 1ο: ΔΙΑΔΙΚΤΥΟ

1.1. ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ Η ΙΣΤΟΡΙΑ ΤΟΥ

Το διαδίκτυο (Internet) είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων ηλεκτρονικών υπολογιστών, οι οποίοι χρησιμοποιούν συγκεκριμένη ομάδα πρωτοκόλλων, εξυπηρετώντας έτσι καθημερινά εκατομμύρια χρήστες σε ολόκληρο τον κόσμο. Αυτοί οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας. Μέσω αυτού ανταλλάσσουν πακέτα με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας). Το κοινό αυτό δίκτυο ονομάζεται διαδίκτυο.

Σύμφωνα με ειδικούς, το διαδίκτυο καθώς και η ψηφιακή τεχνολογία γενικά, έχουν τη μοναδική ικανότητα να δημιουργούν "εικονικούς χώρους", στους οποίους σταματούν να ισχύουν τα κοινωνικά και πολιτιστικά διαχωριστικά όρια που υπάρχουν στον πραγματικό κόσμο. Σημαντικό είναι επίσης, ότι τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν εύκολα τέτοιου είδους τεχνολογίες. Η επικοινωνία μέσω του διαδικτύου είναι πλέον όχι μόνο άμεση αλλά και αμφίδρομη. Δίνεται έτσι η δυνατότητα σε κάθε χρήστη του διαδικτύου, να ανταλλάξει πληροφορίες και απόψεις μέσω ενός πιο συμμετοχικού και όχι τόσο ελεγχομένου διαύλου επικοινωνίας. Οι χρήστες με αυτόν τον τρόπο, αρχίζουν όλο και πιο ενεργά να είναι «παγκόσμιοι πολίτες».

Υπάρχει γενικά η τάση, από την εμφάνιση του διαδικτύου, να θεωρείται από πολλούς ένα πολύ δημοκρατικό μέσο μαζικής επικοινωνίας και ενημέρωσης. Το διαδίκτυο έχει την ικανότητα να αφαιρεί κάθε είδους διαμεσολαβητή στην επικοινωνία και έτσι, καθιστά ισχυρότερο τον μέσο χρήστη. Επιπλέον, του επιτρέπει να έχει πρόσβαση σε μεγάλο όγκο πληροφοριών καθώς και τη δυνατότητα της προσωπικής επιλογής των πληροφοριών αυτών. Επομένως, προσεγγίζοντας το θέμα από αυτή τη σκοπιά, συμπεραίνεται από πολλούς ότι το διαδίκτυο θα καταστήσει την κοινωνία πιο δημοκρατική καταργώντας την ανάγκη για διαμεσολάβηση στην επικοινωνία των χρηστών.

Το διαδίκτυο, μαζί με την εξελισσόμενη ψηφιακή τεχνολογία, είναι υπεύθυνα για τη δημιουργία μιας τεράστιας αγοράς γνώσεων και πληροφοριών. Χαρακτηριστικό φαινόμενο είναι ότι παραδοσιακές μορφές τέχνης (κινηματογράφος, μουσική και άλλα) μέσω της ψηφιακής τεχνολογίας παίρνουν την μορφή αρχείων δεδομένων όπως συνέβαινε με αντικείμενα που φαίνονταν εντελώς διαφορετικά ως τώρα, όπως για παράδειγμα η ιατρική επιστήμη. Παρατηρείται, επομένως, μία συγκέντρωση γνώσεων και πληροφοριών που συνδέεται άμεσα με το ίντερνετ. Βέβαια, εδώ τίθεται το ζήτημα του ποιος θα είναι υπεύθυνος για τη διοίκηση αυτού του όγκου γνώσεων.

Εφόσον το διαδίκτυο είναι ένα δίκτυο συνδεδεμένων ηλεκτρονικών υπολογιστών, κάθε χρήστης μπορεί να μοιράζεται πληροφορίες με άλλους χρήστες. Πληροφορίες, τις οποίες μπορεί να δημιουργεί και ο ίδιος ή απλά να τις κοινοποιεί. Δυστυχώς για κάποιους και ευτυχώς για κάποιους άλλους, δεν υπάρχει άμεσος έλεγχος των πληροφοριών που κοινοποιούνται στο διαδίκτυο από κάποιον ανώτερο χρήστη ή οργανισμό. Αυτή η διαφωνία έγκειται στο ότι ο όγκος των πληροφοριών στο διαδίκτυο είναι πράγματι πολύ μεγάλος, όπως προαναφέρθηκε. Ωστόσο, οι πληροφορίες μπορούν να χωριστούν σε εκείνες στις οποίες ο χρήστης έχει εύκολη πρόσβαση και σε εκείνες που θα δυσκολευτεί να εντοπίσει.

Η πρώτη προσπάθεια για τη δημιουργία ενός διαδικτύου ξεκίνησε στην Αμερική την περίοδο του ψυχρού πολέμου. Η κυβέρνηση της Ρωσίας είχε στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1. Αυτό έκανε τους Αμερικανούς να ανησυχήσουν για την εθνική τους ασφάλεια. Προσπαθώντας, λοιπόν, να προστατευτούν από την πιθανότητα πυρηνικής επίθεσης από την πλευρά των Ρώσων δημιούργησαν μια αμυντική υπηρεσία. Πρόκειται για μια υπηρεσία προηγμένων αμυντικών ερευνών ή οποία ονομάστηκε *ARPA* (Advanced Research Project Agency) και είναι πλέον γνωστή στις μέρες μας ως DARPA (Defense Advanced Research Projects Agency). Σκοπός της υπηρεσίας αυτής ήταν να συμβάλλει στην τεχνολογική ανάπτυξη των στρατιωτικών δυνάμεων των ΗΠΑ και να δημιουργηθεί, έτσι, ένα κοινό δίκτυο επικοινωνίας, το οποίο θα ήταν ικανό να αντέξει από μια πυρηνική επίθεση των Ρώσων.

Οι αναφορές για «γαλαξιακό δίκτυο» στα συγγράμματα του J.C.R. Licklider, αποτέλεσαν τα πρώτα βήματα της θεωρητικής προσέγγισης του σκοπού. Η ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα αντάλλαζαν πληροφορίες και μηνύματα αποτέλεσε τη θεωρητική βάση των προσπαθειών. Βέβαια, σ' αυτό το σημείο, υπήρχε κι ένα μεγάλο ζήτημα που απασχόλησε τους ειδικούς. Οι ηλεκτρονικοί υπολογιστές έπρεπε μεν να βρίσκονται συνδεδεμένοι σε

ένα δίκτυο, ωστόσο, το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο. Κι αυτό γιατί έτσι θα εξασφαλιζόταν ότι ακόμη κι αν κάποιος κόμβος του δικτύου δεχόταν οποιαδήποτε επίθεση θα υπήρχε δυνατότητα επικοινωνίας για τους υπόλοιπους υπολογιστές. Η λύση σ' αυτό δόθηκε από τον Paul Baran, ο οποίος κατάφερε να σχεδιάσει ένα κατανεμημένο δίκτυο επικοινωνίας με τη χρήση της ψηφιακής τεχνολογίας. Μεγάλη ήταν και η συμβολή της θεωρίας ανταλλαγής πακέτων που διατύπωσε ο Leonard Kleinrock. Σύμφωνα με αυτή τη θεωρία τα πακέτα πληροφοριών θα μπορούσαν να ανταλλάσσονται μεταξύ των υπολογιστών, με την προϋπόθεση ότι θα είχαν την προέλευση και τον προορισμό τους.

Έτσι, λοιπόν με βάση αυτές τις τρεις θεωρίες δημιουργήθηκε το πρώτο δίκτυο, με το όνομα ARPANET. Λειτούργησε για πρώτη φορά το 1969 έχοντας τέσσερις κόμβους στους οποίους ήταν συνδεδεμένοι τέσσερις μίνι υπολογιστές:

1. Από το πανεπιστήμιο της Καλιφόρνια στην Σάντα Μπάρμπαρα,
2. Από το πανεπιστήμιο της Καλιφόρνια στο Λος Άντζελες,
3. το SRI στο Στάνφορντ
4. και από το πανεπιστήμιο της Γιούτα.

Η ταχύτητα του πρώτου είδους διαδικτύου που δημιουργήθηκε, έφθανε τα 50 kbps με αποτέλεσμα να γίνει η πρώτη **dial up** σύνδεση, φυσικά μέσω των γραμμών του τηλεφώνου. Σιγά σιγά, άρχισαν να συνδέονται κι άλλοι υπολογιστές σ' αυτό το δίκτυο, αγγίζοντας ως το 1972 τον αριθμό των είκοσι τριών. Τότε ήταν που δημιουργήθηκε η ανάγκη για τη χρήση του ηλεκτρονικού ταχυδρομείου. Εφαρμόστηκε, έτσι, το πρώτο σύστημα ανταλλαγής μηνυμάτων.

Συγχρόνως, δημιουργούνταν κι άλλα δίκτυα, τα οποία συνδέονταν με το δίκτυο ARPANET. Το NCP (Network Control Protocol) ήταν το πρωτόκολλο που χρησιμοποιούνταν από το δίκτυο ARPANET. Το μειονέκτημα, ωστόσο, ήταν ότι μπορούσε να συνδέσει μόνο συγκεκριμένους τύπους υπολογιστών. Έτσι, έπρεπε να δημιουργηθεί ένα πρωτόκολλο το οποίο θα ήταν ικανό να ενώσει όλα τα δίκτυα που είχαν δημιουργηθεί. Αυτό επιτεύχθηκε λίγο αργότερα, το 1974. Δημιουργήθηκε, αισίως, το πρωτόκολλο TCP (Transmission Control Protocol. Βέβαια αργότερα μετονομάστηκε σε TCP/IP, προστέθηκε δηλαδή το IP: Internet Protocol), το οποίο αποτέλεσε το κύριο πρωτόκολλο που μπορούσε να χρησιμοποιηθεί από το ARPANET.

Λίγα χρόνια αργότερα δημιουργείται το πρώτο σύστημα καταγραφής κόμβων. Το σύστημα αυτό, γνωστό και ως **DNS** (Domain Name System) μπόρεσε να καταγράψει χίλιους κεντρικούς κόμβους ενώ κατάφερε την αναγνώριση των υπολογιστών που συνδέονται στο δίκτυο από συγκεκριμένες διευθύνσεις. Η επόμενη κατάκτηση ήταν η δημιουργία του πρώτου διαδικτυακού κορμού (NSFNet) από τις ΗΠΑ, στον οποίο ενσωματώθηκαν κι άλλα σημαντικά δίκτυα (Usenet, Fidonet, Bitnet).

Την εποχή που συνδέθηκε το ARPANET με το NSFNet, έκανε την εμφάνισή του ο όρος διαδίκτυο (ιντερνέτ). Από εκείνη τη στιγμή Internet ονομαζόταν οποιοδήποτε δίκτυο χρησιμοποιούσε το πρωτόκολλο TCP/IP. Το σημαντικότερο, ωστόσο, βήμα έγινε όταν εφαρμόστηκε για πρώτη φορά ο Παγκόσμιος Ιστός. Η υπηρεσία του Παγκόσμιου Ιστού συνέβαλε στην ανάπτυξη του διαδικτύου, αφού ουσιαστικά αποτελεί την "πλατφόρμα" που διευκολύνει την πρόσβαση στο Ίντερνετ.

Υπάρχουν δύο τρόποι με τους οποίους οι χρήστες μπορούν να έχουν πρόσβαση στο διαδίκτυο: η επιλογική και η ευρυζωνική. Στις μέρες μας, οι βιβλιοθήκες και τα Internet cafes όπου υπάρχουν διαθέσιμοι υπολογιστές με σύνδεση στο διαδίκτυο, αποτελούν δημόσιους χώρους τους οποίους μπορούν να επισκέπτονται οι χρήστες προκείμενου να συνδεθούν. Φυσικά, υπάρχουν και σημεία πρόσβασης στο διαδίκτυο σε δημόσιους χώρους, (αίθουσες αναμονής αεροδρομίων) τα οποία μπορεί κανείς να χρησιμοποιεί όσο βρίσκεται σε αναμονή.

Πλέον, στη σημερινή εποχή η πρόσβαση στο διαδίκτυο επιτυγχάνεται μέσω του Wi Fi. Πρόκειται για μια ασύρματη σύνδεση, η οποία παρέχεται σε hotspots, δηλαδή σε σημεία που υπάρχει σήμα ίντερνετ μέσω κεραίας ρούτερ. Τέτοια σημεία πρόσβασης μπορεί να βρει κανείς σε καταστήματα εστίασης και όχι μόνο, και συνήθως αυτό δηλώνεται ως προσόν, στην είσοδο του μαγαζιού με σχετική επιγραφή. Η σύνδεση μπορεί να γίνει από τον οποιοδήποτε, αρκεί να είναι κάτοχος κάποιας συσκευής που έχει τη δυνατότητα να συνδέεται, όπως κινητό τηλέφωνο, λάπτοπ ή τάμπλετ. Η υπηρεσία πρόσβασης μπορεί να είναι δωρεάν σε όλους, μόνο σε πελάτες ή επί πληρωμή, αρκεί να είναι γνωστός στον χρήστη ο κωδικός πρόσβασης στο δίκτυο. Σαφώς και ένα σημείο

πρόσβασης δεν αφορά μόνο το κατάστημα ή τον χώρο που έχει τη σύνδεση. Υπάρχουν ολόκληρα χωριά και περιοχές που διαθέτουν ασύρματο δίκτυο πρόσβασης σε όλη την Ελλάδα.

Με την εξέλιξη της τεχνολογίας επετεύχθη η εύκολη πρόσβαση του χρήστη στο διαδίκτυο μέσω του δικού του τερματικού, υπολογιστή, λάπτοπ ή ακόμη και κινητού του τηλεφώνου, όπως προαναφέρθηκε. Αυτό βοηθά τον χρήστη στο να κατεβάζει αλλά και να ανεβάζει αρχεία στο διαδίκτυο, χωρίς ιδιαίτερους περιορισμούς. Επιπλέον, του επιτρέπει να χρησιμοποιεί τον δικό του browser, που συνεπάγεται ότι έχει πρόσβαση και στους δικούς του σελιδοδείκτες. Τέλος, δίνει την δυνατότητα στον χρήστη να εκτελεί όλες τις δραστηριότητές του μέσω των δικών του προγραμμάτων και δεδομένων. Είναι ορθό, σ' αυτό το σημείο, να αναφερθεί ότι η Νότια Κορέα, η Σουηδία καθώς και οι ΗΠΑ κατέχουν την πρωτιά στην εύκολη και γρήγορη πρόσβαση στο διαδίκτυο.

«Το δικαίωμα των Ευρωπαίων πολιτών για ελεύθερη πρόσβαση στο διαδίκτυο κατοχυρώνεται στο άρθρο 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης. Πρόσφατα στο Ευρωπαϊκό Κοινοβούλιο ψηφίστηκε τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση, εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη».

Ακόμη όμως, και με την εν λόγω τροπολογία η πρόσβαση στο διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας. Συγκεκριμένα, η τροπολογία αναφέρει επίσης «…η πρόσβαση στο Διαδίκτυο δεν μπορεί να περιοριστεί χωρίς να προηγηθεί δικαστική απόφαση. Εξαιρούνται οι περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών». Χαρακτηριστικό παράδειγμα αποτελεί η Βρετανία, στην οποία οι πάροχοι απαγόρευσαν την πρόσβαση σε μια λίστα ιστοσελίδων στην οποία μέχρι τώρα βρίσκονταν σελίδες παιδικής πορνογραφίας, όμως πρόσφατα προστέθηκαν κι άλλες, όπως αυτή που αφορά το χάκινγκ (hacking). Στους χρήστες που θα επιχειρούν να εισέλθουν σε κάποια από αυτές τις σελίδες θα απαγορεύεται η είσοδος, ενώ τα ηλεκτρονικά τους ίχνη θα καταγράφονται. Έτσι, παρά την εν λόγω τροπολογία, εξακολουθεί να μη λαμβάνεται υπ' όψιν ότι το αδιάσειστο δικαίωμα της πρόσβασης των πολιτών στο διαδίκτυο αποτελεί προαπαιτούμενο για την προάσπιση και άλλων θεμελιωδών δικαιωμάτων όπως η γνώση, η παιδεία, η ελευθερία έκφρασης και πολιτικής δράσης.»
Πηγή:
http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

1.2. ΠΛΗΡΟΦΟΡΙΕΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τα δύο σημαντικότερα πλεονεκτήματα του διαδικτύου, που το κατέστησαν άλλωστε, το νούμερο ένα εργαλείο έκφρασης των χρηστών, είναι η παροχή πληροφοριών και η δυνατότητα επικοινωνίας. Βέβαια, το διαδίκτυο χρησιμοποιείται και για ψυχαγωγία με τα online παιχνίδια του. Η μεγαλύτερη όμως συμβολή του στη διευκόλυνσή των χρηστών έγκειται στο online εμπόριο, καθώς και στην πραγματοποίηση εργασιών που θα απαιτούσαν αναμονές σε ουρές δημόσιων υπηρεσιών.

Επικοινωνία

Το διαδίκτυο, πρωταρχικά στοχεύει στην επικοινωνία των χρηστών και για αυτό τον λόγο υπερέχει σε αυτόν τον τομέα, ξεπερνώντας όλες τις προσδοκίες. Έχουν γίνει κατά καιρούς και συνεχίζουν να γίνονται έρευνες, με σκοπό να καταστήσουν το διαδίκτυο γρηγορότερο και πιο αξιόπιστο. Από την εμφάνιση του, άλλωστε, αποτέλεσε κόμβο επικοινωνίας και με την άνθησή του, όλος ο κόσμος έχει μετατραπεί σε Παγκόσμιο χωριό. Πλέον, η επικοινωνία με έναν χρήστη που βρίσκεται στην άλλη

άκρη της γης γίνεται σε κλάσματα δευτερολέπτου. Στις μέρες μας, οι άνθρωποι χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο για την αποστολή μηνυμάτων σε απομακρυσμένους υπολογιστές. Επιπλέον, χρησιμοποιούνται υπηρεσίες κοινωνικής δικτύωσης, μέσω ανάλογων σελίδων, όπως το facebook, το twitter, το myspace και άλλα. Τέλος, οι χρήστες «κατεβάζουν» εφαρμογές κινητού τηλεφώνου, για επικοινωνία με φίλους τους, μέσω του διαδικτύου, εύκολα, γρήγορα και χωρίς χρέωση μηνύματος ή κλήσης. Τέτοιες εφαρμογές είναι οι viber, whatsapp, skype και άλλες. Μέσω όλων των παραπάνω, η επαφή των χρηστών έχει γίνει πολύ πιο εύκολη, συμβάλλοντας έτσι στην Παγκόσμια Φιλία.

Πληροφορίες
Η παροχή πληροφοριών είναι ίσως το μεγαλύτερο πλεονέκτημα του διαδικτύου. Κάθε είδος πληροφοριών για όλα τα θέματα είναι διαθέσιμο στο διαδίκτυο. Μπορεί να εντοπιστεί σχεδόν οποιοσδήποτε τύπος στοιχείων όσον αφορά σχεδόν όλα τα είδη θεμάτων για τα οποία γίνεται αναζήτηση στο διαδίκτυο. Έτσι, για κάθε θέμα, υπάρχει ένα τεράστιο ποσό πληροφοριών διαθέσιμο στο διαδίκτυο, που αφορά από νομοθεσία, ως πληροφορίες αγοράς και ιατρικής. Οι κατηγορίες χρηστών που πιστεύεται ότι χρησιμοποιούν το διαδίκτυο για αυτό το σκοπό, δηλαδή για την έρευνα, είναι κυρίως οι φοιτητές και οι μαθητές. Πλέον, θεωρείται δεδομένο ότι οι φοιτητές πρέπει να χρησιμοποιήσουν το διαδίκτυο για την αναζήτηση πληροφοριών και τη συλλογή στοιχείων. Οι καθηγητές συνηθίζουν να αναθέτουν εργασίες που απαιτούν την έρευνα στο διαδίκτυο. Όπως αναφέρθηκε παραπάνω, έρευνες για ιατρικά θέματα δημοσιεύονται στο διαδίκτυο και όλοι μπορούν να ενημερωθούν άμεσα. Υπάρχουν, άλλωστε, πολλές σελίδες στο διαδίκτυο που προσφέρουν ιατρικές πληροφορίες στους χρήστες και άλλες στις οποίες ο επισκέπτης έχει τη δυνατότητα να συνομιλεί με γιατρούς on-line όπως, ο America's Doctor. Χαρακτηριστικό είναι το στοιχείο ότι καταγράφηκαν τη χρονιά 1998 σχεδόν 20 εκατομμύρια άνθρωποι να αναζητούν on-line πληροφορίες υγείας.

Ψυχαγωγία
Με την πάροδο των χρόνων, τα μέσα του διαδικτύου έχουν σημειώσει μεγάλη επιτυχία στο θέμα της ψυχαγωγίας. Το «κατέβασμα» παιχνιδιών από το διαδίκτυο είναι από τις αγαπημένες ασχολίες μικρών και μεγάλων. Η λήψη αυτών των παιχνιδιών μπορεί να γίνεται δωρεάν από συγκεκριμένες σελίδες, ή με κάποια χρέωση του χρήστη. Ωστόσο, τα πιο δημοφιλή παιχνίδια, σήμερα, είναι τα online παιχνίδια, με φανατικούς θαυμαστές σε όλον τον κόσμο. Σ' αυτού του είδους τα παιχνίδια, ο χρήστης μπορεί να παίξει οποιαδήποτε στιγμή της ημέρας, αρκεί να είναι συνδεδεμένος στο διαδίκτυο, μπορεί να μιλάει με τους συμπαίκτες του online ή ακόμα και να τζογάρει, ποντάροντας πραγματικά χρήματα. Ένας άλλος παράγοντας της ψυχαγωγίας είναι η συμμετοχή των χρηστών σε δωμάτια συνομιλίας. Εκεί ο ενδιαφερόμενος έρχεται σε επαφή με άλλους χρήστες. Τέλος, ένα μεγάλο ποσοστό χρηστών προτιμά την απλή πλοήγηση στο διαδίκτυο, κατά την οποία μπορεί να βλέπει online ή να κατεβάζει στον υπολογιστή του διάφορα δεδομένα προς ψυχαγωγία του. Οι ειδήσεις, αστεία βίντεο καθώς και η μουσική είναι κάποια από τα πιο συχνά δεδομένα που αναζητούν οι χρήστες και στη συνέχεια τα κατεβάζουν ή απλά τα μοιράζονται στο διαδίκτυο.

Υπηρεσίες
Στο διαδίκτυο παρέχονται πλέον πολλές υπηρεσίες που σκοπό έχουν την πιο εύκολη, γρήγορη και χωρίς κόπο εξυπηρέτηση των πολιτών, καθώς μπορούν όλες να πραγματοποιηθούν ενώ ο χρήστης είναι συνδεδεμένος και καθισμένος στο γραφείο του σπιτιού του. Τέτοιες υπηρεσίες είναι οι online τραπεζικές συναλλαγές, η ζήτηση και η προσφορά εργασίας, η δυνατότητα αγοράς εισιτηρίων για κινηματογράφο, θέατρο και συναυλίες, οι υπηρεσίες καθοδήγησης σε διάφορα θέματα ως και νομικά, οι κρατήσεις σε ξενοδοχεία, η αγορά ακτοπλοϊκών και αεροπορικών εισιτηρίων, η online πληρωμή λογαριασμών τηλεφώνου και ρεύματος κ.α. Κάποιες από αυτές τις υπηρεσίες, ωστόσο, μπορεί να έχουν κάποια χρέωση για τη χρήση του.

Ηλεκτρονικό Εμπόριο (E-Commerce)
Ο όρος Ηλεκτρονικό Εμπόριο είναι μια έννοια που χρησιμοποιείται για κάθε είδος εμπορικής διαδικασίας. Συγκεκριμένα, όταν μια επιχείρηση πραγματοποιεί παροχή υπηρεσιών ή και υλικών σε όλο τον κόσμο, με το ανάλογο κόστος, μέσω διαδικτύου, λέμε ότι πραγματοποιεί ηλεκτρονικό

εμπόριο. Πλέον, πάρα πολλοί χρήστες ανά τον κόσμο αγοράζουν και πωλούν μέσω διαδικτύου. Οι αγοραστές, πολλές φορές, διευκολύνονται στον τρόπο αγοράς, με διάφορους τύπους πληρωμής, όπως η αντικαταβολή, η χρήση πιστωτικών καρτών ή προπληρωμένων καρτών. Τις περισσότερες φορές, βέβαια, χρεώνονται τα έξοδα αποστολής των προϊόντων.

ΚΕΦΑΛΑΙΟ 2ο: ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 ΕΙΣΑΓΩΓΗ

Σήμερα, η αλήθεια είναι ότι μεταξύ των νέων τεχνολογιών, εκείνη που έχει την πιο προνομιακή θέση είναι αυτή της πληροφορικής. Έχει παίξει σπουδαίο ρόλο στην εξέλιξη κάθε μορφής τεχνολογίας και με αυτόν τον τρόπο έχει συμβάλει στο να ανοίξουν οι δρόμοι σε διάφορους κλάδους όπως οι υπηρεσίες υγείας, δημόσιας διοίκησης, η εκπαίδευση, η έρευνα και οι τηλεπικοινωνίες. Το διαδίκτυο, με την πάροδο του χρόνου έγινε ένα από τα σημαντικότερα εργαλεία για την επικοινωνία, την ανταλλαγή πληροφοριών, την ακαδημαϊκή έρευνα, την ψυχαγωγία και για πολλές άλλες υπηρεσίες.

Παρόλα αυτά, μεγαλώνει όλο και περισσότερο η ανησυχία των ειδικών για την εμφάνιση και την ανάπτυξη συμπεριφορών παθολογικού χαρακτήρα που σχετίζονται με το διαδίκτυο. Οι ηλικίες από όπου τα παιδιά ξεκινούν να έχουν πρόσβαση στο διαδίκτυο είναι όλο και μικρότερες. Μάλιστα το θεωρούν από τις πιο αγαπημένες τους ενασχολήσεις. Σύμφωνα με έρευνα η χρήση του διαδικτύου από την πλειοψηφία των παιδιών γίνεται πολλές φορές την ημέρα, ακόμη κι εκείνες τις ημέρες που έχουν σχολείο. Επιπρόσθετα, η χρήση των κινητών τηλεφώνων, των ηλεκτρονικών υπολογιστών, του διαδικτύου είναι αυτονόητη για τη νεολαία του δυτικού κόσμου.

Γενικά, οι νέοι γνωρίζουν τους κινδύνους όταν χρησιμοποιούν το διαδίκτυο. Ωστόσο, κι αυτό είναι ένα σημαντικό ζήτημα, όταν αντιμετωπίσουν κάποιο πρόβλημα απευθύνονται στους ενήλικες μόνο ως τελευταία λύση (Ευρωβαρόμετρο 2007). Επομένως, είναι πιο εύκολο, μέσω της άσκοπης και πολύωρης χρήσης του διαδικτύου, να οδηγηθούν στον εθισμό.

Μερίδα ακαδημαϊκών υποστηρίζει ότι η αλόγιστη χρήση του διαδικτύου μπορεί να έχει παθολογικά και εθιστικά αίτια. Σε σχέση με την ακαδημαϊκή ιστορία του εθισμού στο διαδίκτυο, από τις μεγαλύτερες δυσκολίες είναι το να διατυπωθεί ένας ολοκληρωμένος ορισμός της έννοιας. Οι επιστήμονες που ερευνούν τέτοιου είδους φαινόμενα δεν έχουν φτάσει σε κάποιον όρο που να ακουμπάει περιγράφοντας ακριβώς αυτό που είναι το ζητούμενο, το φαινόμενο της κατάχρησης του διαδικτύου.

Τα υψηλά ποσοστά εθισμού στη χώρα μας ερμηνεύεται ότι έρχονται σαν απόρροια του γεγονότος που ονομάζεται ψηφιακός αλφαβητισμός. Αφορά δε παιδιά και ενήλικες. Πιο συγκεκριμένα, στην Ελλάδα ο εθισμός ξεκίνησε σε μεγάλο ποσοστό, από το γεγονός ότι οι χρήστες δούλευαν στον ηλεκτρονικό υπολογιστή, με βάση την εμπειρική απασχόληση τους και όχι συντονισμένα σαν αποτέλεσμα μιας μαθησιακής διαδικασίας. Είναι ευρέως γνωστό, ότι οι σχέσεις των ανθρώπων κτίζονται σταδιακά, πόσο μάλλον με το διαδίκτυο. Επιπρόσθετα ο ρόλος της εκπαίδευσης είναι ιδιαίτερα σημαντικός για να μεταβεί ο κάθε ένας χρήστης ομαλά από την κοινωνία της πραγματικότητας στην κοινωνία της πληροφορίας.

Το Διαδίκτυο μπορεί να καλύπτει κάποιες ψυχολογικές ανάγκες του ανθρώπου. Χαρακτηριστικό του μέσου αυτού το οποίο, προκύπτει και από τη φύση, είναι ότι είναι δυνατό να δημιουργηθεί μια «ιδανική κατάσταση», όπου το κάθε άτομο έχει την ευχέρεια να ανακαλύψει και να ερευνήσει την προσωπικότητά του χωρίς να τον περιορίζει κάτι ή να έχει οποιαδήποτε συνέπεια. Στο διαδίκτυο υπάρχουν συνέπειες για τις πράξεις του χρήστη, αλλά δεν είναι άμεσες. Ο χρήστης μπορεί να μπαίνει στο διαδίκτυο, να βγαίνει σε οποιαδήποτε στιγμή, όποτε το θελήσει, και σίγουρα του είναι πολύ εύκολο μα καλύψει την εμφάνιση του αφού σε καμία περίπτωση δεν μπορεί κάποιος να τον δει χωρίς την έγκριση του.

Οι έφηβοι είναι εκείνοι οι χρήστες που πιο συχνά από άλλους μπαίνουν στη διαδικασία να ενσαρκώνουν διάφορους και διαφορετικούς ρόλους ανάλογα με την περίπτωση και ανάλογα με τη διαδικτυακή εμπειρία που προκύπτει κάθε φορά. Αυτό είναι ένα από τα κυριότερα χαρακτηριστικά του διαδικτύου.

Από έρευνες που έγιναν πρόσφατα στην Ελλάδα έχει να καταδείξει κανείς πόσο σημαντική είναι η επίβλεψη του ανηλίκου από το γονέα εάν και εφόσον το παιδί είναι χρήστης του διαδικτύου καθώς και πόσο σημαντική είναι η γονική μέριμνα και φροντίδα στην ανάπτυξη του εθισμού αυτού στο διαδίκτυο (Siomos, 2012). Η αποτελεσματικότερη παροχή γονικής μέριμνας έχει τα εξής

χαρακτηριστικά: α) φροντίδα και β) προστατευτικότητα, ώστε το παιδί να διαπαιδαγωγείται με ασφάλεια, χωρίς οι γονείς ή οι κηδεμόνες να μπαίνουν εμπόδιο στις προσπάθειες που κάνει ο ανήλικος χρήστης, να αναδείξει την προσωπικότητά του αλλά και να αυτονομηθεί. Από την άλλη πλευρά, οι υπερπροστατευτικοί γονείς οι οποίοι όμως δεν φροντίζουν όσο χρειάζεται τα παιδιά τους είναι πολύ κοντά στο πρότυπο εκείνο που ονομάζεται «έλεγχος χωρίς στοργή». Αυτό με τη σειρά του συνδέεται με υψηλά ποσοστά εθισμού στο διαδίκτυο.

Τέλος, καλό θα ήταν να γίνει συνειδητά κάποια διάκριση μεταξύ του εθισμού και της ενθουσιώδους χρήσης του δικτύου. Ο μεγάλος βαθμός ενασχόλησης με τη χρήση του διαδικτύου είναι μια δραστηριότητα που πολλές φορές μπερδεύεται με τον εθισμό στο διαδίκτυο. Συνήθως, ο χρήστης που εμπλέκεται σε μεγάλο βαθμό, ασχολείται με αυτή τη δραστηριότητα επειδή του προσφέρει ευχαρίστηση. Ωστόσο, σε ελάχιστες περιπτώσεις, η μεγάλη εμπλοκή μπορεί να συνδέεται με ανάπτυξη επαγγελματικών δεξιοτήτων, κάτι που νοείται σα θετική προοπτική.

Διαδικτυακή εξάρτηση: Παγκόσμιο φαινόμενο

Σε Ευρωπαϊκές χώρες όπως η Γερμανία και η Αγγλία, τα περισσότερα παιδιά, μετά το τέλος των σχολικών δραστηριοτήτων, γυρίζουν σ' ένα σπίτι το οποίο είναι άδειο. Επομένως, ξεκινούν να χρησιμοποιούν τον ηλεκτρονικό υπολογιστή χωρίς επίβλεψη, χωρίς περιορισμό, για πάρα πολλές ώρες. Οι χώρες αυτές αποτελούν την πιο μεγάλη διαδικτυακή αγορά αφού ο αριθμός των χρηστών που εξαρτούνται από το διαδίκτυο ξεπερνά το 1.000.000 χρήστες.

Η Γερμανία, είναι μια από τις Ευρωπαϊκές χώρες στις οποίες λειτουργούν ήδη θεραπευτικές κατασκηνώσεις για νέους και εφήβους, στις όποιες έχουν την ευκαιρία να συμμετάσχουν και να ασχοληθούν με διάφορες δραστηριότητες αλλά και με πλευρές της ζωής στις οποίες δεν έχει θέση ο ηλεκτρονικός υπολογιστής και το διαδίκτυο. Όλο αυτό τους βοηθάει να ανακαλύψουν μια πλευρά του εαυτού τους, μια πλευρά στη οποία δεν υπάρχει το μέσον προς την εξάρτηση.

Στην Ιαπωνία ο αριθμός των χρηστών πού παίρνουν μέρος σε ομαδικές αυτοκτονίες ή συμφωνίες-συμβόλαια αυτοκτονίας αυξάνεται διαρκώς. Η Ιαπωνική αστυνομία δήλωσε ότι 91 άνθρωποι-χρήστες αυτοκτόνησαν το 2007. Αξίζει να σημειωθεί ότι ο αριθμός αυτός κάθε χρόνο μεγαλώνει. Σημαντικό επίσης είναι, το ότι και στην Ιαπωνία ο κόσμος δηλώνει ότι οι γρήγοροι ρυθμοί της ζωής τους, τους αποξενώνουν από το κοινωνικό τους περιβάλλον έτσι, πολλές χιλιάδες νέων απομονώνονται και η μόνη τους διέξοδος, είναι η πλοήγηση στο διαδίκτυο και η επικοινωνία μέσω του παγκόσμιου ιστού. Να προστεθεί ότι όλα αυτά συμβαίνουν και στην Ελλάδα. Στην Ελλάδα τον Απρίλιο του 2009 εντοπίστηκε νεαρός μαθητής από το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος ο οποίος ήθελε να βάλει τέλος στη ζωή του. Ο έφηβος, είχε σημειώσει τη σκέψη του μέσω διαδικτύου, ηλεκτρονικά «στο ημερολόγιο του».

2.2. ΑΙΤΙΑ ΕΘΙΣΜΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Επιστήμονες υποστηρίζουν πως η συνεχής αλλαγή διάθεσης λόγω της συμπεριφοράς έχει άμεση σχέση με το ότι το άτομο-χρήστης είναι σε διαδικασία εθισμού. Όπως παραδείγματος χάριν ένα άτομο εθισμένο στο αλκοόλ νιώθει μια ευχαρίστηση και ταυτόχρονα αλλάζει η διάθεση του καταναλώνοντας οινοπνευματώδη ποτά. Το ίδιο συμβαίνει και με ένα άτομο εθισμένο στο διαδίκτυο, υπάρχει μια αίσθηση ανυπομονησίας έως ότου μπορέσει να έρθει σε επαφή με τον ηλεκτρονικό υπολογιστή και ταυτόχρονα υπάρχει μια γλυκιά ευχαρίστηση αμέσως μόλις ξεκινήσει η διαδικασία ανοίγματος του PC. Μερίδα ερευνητών πιστεύει ότι υπάρχουν βιοχημικές μεταβολές οι οποίες

συμβαίνουν στο ανθρώπινο σώμα που είναι εθισμένο. Επιπρόσθετα, από βιολογικής άποψης υπάρχει περίπτωση να υπάρχουν συνδυασμοί γονιδίων που κάνουν κάποια άτομα επιρρεπή σε οποιαδήποτε μορφή εθισμού, όπως υπάρχουν γονίδια, τα οποία ανακάλυψαν οι ερευνητές και συνδέονται άμεσα με τον εθισμό στο αλκοόλ.

Οι επιστήμονες, σε ότι αφορά τον εθισμό αμφισβητούν έντονα τον όρο της "εθιστικής προσωπικότητας", πράγμα που σημαίνει ότι είναι πολύ πιθανό, ένα άτομο το οποίο έχει ήδη έναν εθισμό να είναι επιρρεπής στο να εθιστεί πιο εύκολα σε ουσίες ή δραστηριότητες, όπως αυτή που έχει να κάνει με το διαδίκτυο.

Τα άτομα με διαταραχές στην ψυχολογική τους κατάσταση ή συμπτώματα, όπως η κατάθλιψη, το αίσθημα απομόνωσης ή το άγχος, έχουν την εντύπωση ότι θεραπεύονται με το να χρησιμοποιούν το διαδίκτυο, όπως υπάρχουν άλλοι που θεωρούν ότι θεραπεύονται καταναλώνοντας αλκοόλ και ουσίες. Την ίδια στιγμή, δύναται να υπάρχουν προσωπικά ή οικογενειακά προβλήματα που ωθούν το άτομό στην υπερβολική χρήση του παγκόσμιου ιστού.

Οι άνθρωποι στους οποίους έχουν αναπτυχθεί προβλήματα από τη χρήση του διαδικτύου, αρχικά έρχονταν σε επαφή με το αντικείμενο ευκαιριακά. Στη συνέχεια, σταδιακά αναπτύσσονται δυσλειτουργικές συμπεριφορές στο άτομο, μέσα από την ενασχόληση. Η χρήση του διαδικτύου είναι ικανή να ασκήσει άμεση επιρροή στην κοινωνική ζωή του χρήστη, το σχολείο, τη δουλειά, τις διαπροσωπικές σχέσεις και γενικότερα ότι έχει σχέση με τον κοινωνικό του περίγυρο.

Οι συνηθέστεροι λόγοι που οδηγούν τον χρήστη στον εθισμό στο διαδίκτυο είναι:

α. Οι έντονες συγκρούσεις στο οικογενειακό περιβάλλον, δυσλειτουργικές οικογένειες

β. Οι μειωμένες κοινωνικές δεξιότητες και η δυνατότητα εικονικής κοινωνικοποίησης

γ. Η δυνατότητα ανάληψης εικονικών ρόλων από τον χρήστη, εφόσον υπάρχει αδυναμία στην ανάληψη ρόλων στην πραγματική ζωή.

Απόρροια όλων αυτών είναι τα εξής ερωτήματα, το οποία δεν έχουν απαντηθεί, σε σχέση με τον εθισμό στο διαδίκτυο. Πόσο ιδιαίτερος λοιπόν είναι αυτός ο τύπος εθισμού; Είναι ένα παράδειγμα μιας καινούριας τεχνολογίας που χρησιμοποιείται για την υποστήριξη άλλου είδους εθισμών; Παραδείγματος χάριν, υπάρχουν λέσχες τυχερών παιχνιδιών στο διαδίκτυο που μπορούν να ενισχύσουν τον εθισμό που ήδη υπάρχει στα τυχερά παιχνίδια. Όμοια, κάποιος εθισμένος σε ορισμένες μορφές σεξουαλικής συμπεριφοράς είναι εύκολο να επισκεφτεί ιστοσελίδες πορνογραφικού περιεχομένου ή να συνομιλεί με άτομα που παρουσιάζουν ίδια συμπεριφορά και μαζί να προχωρούν σε όποιο σημείο θεωρούν ότι είναι αρκετό ώστε να ικανοποιήσει τις ορέξεις του.

2.3. ΣΥΜΠΤΩΜΑΤΑ ΕΘΙΣΜΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Έρευνες δείχνουν ότι το ένα πέμπτο των δεκαπεντάχρονων παιδιών που ζουν στην Αττική εμφανίζει κατά διαστήματα, διαφόρων ειδών προβλήματα σε σχέση με την κατάχρηση του διαδικτύου. Παρατηρείται, έντονα, ότι βρίσκονται πάρα πολύ κοντά στον εθισμό. Υπάρχουν ανήλικοι που ήδη παρακολουθούνται με συμπτώματα εθισμού και εξάρτησης από το διαδίκτυο. Τα αποτελέσματα λοιπόν της έρευνας της Μονάδας Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών, Νοσοκομείο Παίδων "Κυριακού", αναφέρουν ότι ο συχνότερος λόγος που οι έφηβοι χρησιμοποιούν το διαδίκτυο είναι τα online παιχνίδια. Τα στοιχεία ανακοινώθηκαν από την Ανοιχτή Γραμμή για καταγγελίες σε σχέση με δικτυακούς τόπους, "SafeLine".

Με βάση τα παραπάνω, διαπιστώνουμε ότι το 8% των εφήβων έως και 15ετών χρησιμοποιεί το διαδίκτυο περισσότερες από 20 ώρες την εβδομάδα και 3 από τους 10 εφήβους πλοηγούνται καθημερινά στο διαδίκτυο. Στις ΗΠΑ, η American Medical Association, προσπαθώντας να αντιμετωπίσει το πρόβλημα του εθισμού, έχει ξεκινήσει τις ενέργειες για να αναγνωριστεί επίσημα ο εθισμός στα ηλεκτρονικά παιχνίδια ως ψυχολογική διαταραχή. Αυτό θα συμβάλλει, κατά τη γνώμη τους, στην ευαισθητοποίηση του κοινού πάνω στο θέμα αλλά και στην εξασφάλιση ασφαλιστικής κάλυψης για όσους διαγνωσθούν με συμπτώματα εθισμού στα videogames.

Συμπτώματα και ενδείξεις

Σύμφωνα με τη SafeLine, οι προειδοποιητικές ενδείξεις για τον εθισμό στο διαδίκτυο περιλαμβάνουν τόσο ψυχολογικά όσο και σωματικά συμπτώματα.

Ψυχολογικά συμπτώματα:

- Αίσθηση ευφορίας για όσο το άτομο είναι σε επαφή με τον υπολογιστή
- Ανικανότητα του ατόμου να σταματήσει τη δραστηριότητα
- Παραμέληση του οικογενειακού και φιλικού κύκλου
- Θλίψη, οξυθυμία και άλλα όταν ο χρήστης δεν είναι σε επαφή με τον υπολογιστή
- Ψέματα στην οικογένεια και τους φίλους για τις δραστηριότητες στο διαδίκτυο
- Προβλήματα στη δουλειά

Σωματικά συμπτώματα:

- Διατροφικές διαταραχές
- Διαταραχές στον ύπνο
- Μυοσκελετικές παθήσεις
- Μειωμένη αθλητική δραστηριότητα
- Προβλήματα όρασης
- Ημικρανίες
- Παραμέληση προσωπικής υγιεινής
- Σύνδρομο καρπιαίου σωλήνα

Σε σχέση με τους ανηλίκους τα συμπτώματα είναι το ίδιο ανησυχητικά έως και σοβαρά σε αρκετές περιπτώσεις. Οι περισσότεροι δεν ξέρουν πώς να χειριστούν το ζήτημα όταν αντιληφθούν ότι, αντί να χρησιμοποιούν τα παιδιά, στο σπίτι, το διαδίκτυο για σχολικές εργασίες ή για έρευνα, εκείνα ανταλλάσουν μηνύματα με φίλους, παίζουν παιχνίδια ή συνομιλούν με αγνώστους στα διάφορα chat rooms. Αυτό γίνεται επειδή εύκολα μπορεί κανείς να κρύψει τι κάνει στο διαδίκτυο. Παιδιά, έφηβοι και άλλα άτομα νεαρής ηλικίας, πολύ εύκολα εγκλωβίζονται σε όλες αυτές τις δικτυακές δραστηριότητες, τα online παιχνίδια (τα οποία κατά κύριο λόγο απαρτίζονται από πολλούς παίκτες), τα δωμάτια συζήτησης κ.α.

Προειδοποιητικά σημάδια - συμπτώματα που πρέπει να ανησυχήσουν τους γονείς.
Παρακάτω, παρατίθενται επιγραμματικά ορισμένα συμπτώματα, τα οποία είναι σε θέση εύκολα να αναγνωρίσουν οι γονείς και να πράξουν αναλόγως.

• Συνεχής ασχολία με το διαδίκτυο ή με ότι έχει σχέση με αυτό, παραμελώντας υποχρεώσεις που έχει το παιδί για το σπίτι ή σχολείο
• Δεν υπάρχει συναίσθηση του χρόνου κατά τη διάρκεια του οποίου ασχολείται με τον υπολογιστή
• Προτίμηση στα διαδικτυακά παιχνίδια, από τα παιχνίδια με φίλους στον πραγματικό κόσμο. (απομόνωση)

• Κακές επιδόσεις στο σχολείο
• Ενασχόληση με το διαδίκτυο ακόμη και την ώρα του φαγητού.
• Νευρικές ή επιθετικές αντιδράσεις σε περίπτωση που κάποιος διακόψει το παιδί από το παιχνίδι ή από τη συζήτηση που είχε διαδικτυακά.
• Συχνά ξενύχτια μπροστά στον ηλεκτρονικό υπολογιστή και στο διαδίκτυο
• Επανάληψη συνεχώς των ίδιων φράσεων: όπως ¨θα παίξω ένα λεπτό ακόμη…¨
• Συμπτώματα άγχους, θυμού ή καταθλιπτικής συμπεριφοράς όταν το παιδί δεν βρίσκεται online

Έρευνες, αναφέρονται στο ότι παιδιά που ζουν με γονείς που είναι «μακριά» τους, αδιαφορούν και γενικά είναι απόντες, είναι εκείνα τα οποία είναι πιο επιρρεπή στο να αναπτύξουν «εθιστικές σχέσεις» με το ποτό, με ουσίες και στην περίπτωση που εξετάζουμε, με τον υπολογιστή.

Το χάσμα που δημιουργείται μεταξύ γονέων και παιδιού εξαιτίας της έλλειψης ουσιαστικής επικοινωνίας και εξαιτίας της έλλειψης ποιοτικού χρόνου στη σχέση των δύο πλευρών, είναι η κυριότερη αιτία, ικανή να στρέψει το παιδί στην αναζήτηση τρόπων, που θα του επιτρέψουν να δραπετεύσει από την πραγματικότητα μέσα στην οποία ζει. Ένας τρόπος λοιπόν είναι η προσκόλληση στο διαδίκτυο.

Επιπλέον, παιδιά-έφηβοι με εσωστρεφή συμπεριφορά, με χαμηλή αυτοπεποίθηση, με προβλήματα στις σχέσεις τους, ιδιαίτερα με άτομα της ίδιας ηλικίας, που νιώθουν μειονεκτικά απέναντι στους άλλους και δεν έχουν εμπιστοσύνη στις ικανότητες τους, είναι πολύ πιθανό να στραφούν ώστε να εκτονωθούν και να νιώσουν καλύτερα, στον ηλεκτρονικό τους υπολογιστή με αποτέλεσμα να έχουν και πάρα πολλές πιθανότητες να εθιστούν.

Αυτό συμβαίνει επειδή έχουν την ευκαιρία, χρησιμοποιώντας ένα απρόσωπο δίκτυο:

- να εκφραστούν χωρίς περιορισμούς
- να κατασκευάσουν μια ψεύτικη ταυτότητα
- να γίνουν κομμάτι μιας ομάδας
- να πολεμήσουν τη μοναξιά τους
- να τραβήξουν την προσοχή των άλλων
- να ξεφύγουν από ότι βιώνουν, ότι ζουν

Και όλα αυτά, επιτυγχάνονται πολύ εύκολα, μέσα από το σπίτι τους, στο γραφείο τους.

2.4. ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ ΕΘΙΣΜΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι επιπτώσεις από την κατάχρηση του διαδικτύου και όλων των ηλεκτρονικών παιχνιδιών είναι σοβαρότατες, πόσο μάλλον όταν πρόκειται για νεαρά άτομα, παιδιά, έφηβους, άνθρωποι δηλαδή οι οποίοι βρίσκονται σε μια ιδιαίτερη φάση ζωής και δεν έχει ακόμη διαμορφωθεί ολοκληρωμένα ο χαρακτήρας και η προσωπικότητα τους. Η υπερβολική χρήση του διαδικτύου έχει άμεσες συνέπειες στη συμπεριφορά των ατόμων κάθε ηλικίας.
Οι πιο συνηθισμένες επιπτώσεις από την υπερβολική χρήση του διαδικτύου είναι οι ακόλουθες:

- Κατάθλιψη
- Παθήσεις των ματιών
- Μυοσκελετικά Προβλήματα
- Παχυσαρκία

- Παραμέληση ατομικής καθαριότητας

Η ψυχική υγεία κυρίως των νεαρών σε ηλικία ατόμων εξαρτάται άμεσα από το βαθμό χρήσης του διαδικτύου. Όπως κάθε κατάχρηση έτσι και αυτή έχει μπορεί να προκαλέσει σοβαρά προβλήματα. Αυτό συμβαίνει, επειδή, όπως αναφέρθηκε παραπάνω η προσωπικότητα των παιδιών και των εφήβων δεν έχει διαμορφωθεί πλήρως Τα πρότυπα και τα ερεθίσματα αυτά τα λαμβάνουν από το ίντερνετ.. Κάποιες συνέπειες μπορεί να είναι οι ακόλουθες:

- Σωματοποίησης του άγχους
- Ανάπτυξη εμμονών στη σκέψη
- Αρνητικά πρότυπα και ταύτιση μαζί τους
- Απώλεια ελεύθερης σκέψης και θέλησης
- Παρορμητική και βίαιη συμπεριφορά
- Στείρα σκέψη
- Ισοπέδωση προσωπικών αρχών και αξιών

2.5. ΜΟΡΦΕΣ ΕΘΙΣΜΟΥ

Ο Εθισμός διακρίνεται σε κατηγορίες, ανάλογα με το στάδιο του εθισμού και ανάλογα με το είδος του εθισμού. Αναλυτικότερα, αναφέρεται ότι υπάρχουν τουλάχιστον έξι διαφορετικές έννοιες για τον όρο εθισμός στο διαδίκτυο όπως τα παρακάτω: Διαταραχή Εθισμού στο Διαδίκτυο, Παθολογική Χρήση του Διαδικτύου, Προβληματική Χρήση του Διαδικτύου, Υπερβολική Χρήση του Διαδικτύου όπως και Καταναγκαστική Χρήση του Διαδικτύου ή άλλες όπως, ο Εθισμός στον Κυβερνοχώρο, Εθισμός Σύνδεσης στο Διαδίκτυο, Εθισμός στο Δίκτυο, Διαταραχή Διαδικτυακού Εθισμού, Υψηλή Εξάρτηση από το Διαδίκτυο και άλλα.

Το 1995 ο Dave Goldberg πρότεινε την χρήση του όρου εθισμός στο διαδίκτυο ως αυτόν που θα περιέγραφε την υπερβολική χρήση του διαδικτύου και τη κυκλοθυμική συμπεριφορά που δημιουργείται κατά τη στέρηση του. Αυτή η κατηγορία εθισμού αν και επίσημα δεν έχει αναγνωριστεί ως κλινικό νόσημα,-τουλάχιστον από τις περισσότερες χώρες- είναι μια κατάσταση, η οποία μπορεί να φέρει επιπτώσεις στην κοινωνική και επαγγελματική ζωή του ατόμου. Οι επιστήμονες που ασχολούνται με την ψυχική υγεία, όλο και πιο συχνά βρίσκονται αντιμέτωποι με περιστατικά στα οποία είναι πρωταγωνιστές άτομα με προβληματική χρήση του ίντερνετ.

Ο εθισμός αυτός στο διαδίκτυο είναι ένας ευρύτατος όρος, όρος που περιλαμβάνει μεγάλο φάσμα συμπεριφορών και προβλημάτων ελέγχου των κινήσεων του ατόμου. Επίσης, ο όρος μπορεί να διαχωριστεί στις εξής υποκατηγορίες:

- Εθισμός στο ηλεκτρονικό πορνό
- Εθισμός στις διαδικτυακές διαπροσωπικές σχέσεις
- Εμμονή στο τζόγο ή στις αγορές μέσω διαδικτύου
- Καταναγκαστική περιήγηση στο Διαδίκτυο
- Εθισμός στους ηλεκτρονικούς υπολογιστές

Έτσι, και αφού μελετήσουμε της παραπάνω υποκατηγορίες μπορούμε να προσεγγίσουμε τον εθισμό στο διαδίκτυο ως μια έννοια, η οποία διακρίνεται σε σχέση και με τη βαρύτητα της χρήσης. Κατά αναλογία λοιπόν, μπορούμε να διακρίνουμε και εδώ κατηγορίες συμπεριφορών ποσοτικά πια.

α) Τυπική χρήση:

Η καλή χρήση του διαδικτύου στον εργασιακό χώρο, στο σπίτι, η χρήση που γίνεται για λόγους ψυχαγωγίας ή στα πλαίσια δραστηριοτήτων που αφορούν επαγγελματικά το χρήστη.

β) Προβληματική χρήση:

Σ' αυτήν την περίπτωση δεν εξυπηρετείται κάποιος σκοπός για τον οποίο γίνεται η χρήση. Είναι προειδοποίηση για την κατάχρηση.

γ) Κατάχρηση:

Μια κατάσταση που επαναλαμβάνεται και που οδηγεί άμεσα σε επιπτώσεις στη λειτουργικότητα του ατόμου κατά τη διάρκεια μεγάλης περιόδου, διάστημα στο οποίο παρουσιάζονται συμπτώματα όπως η δυσκολία να έλθουν εις πέρας σημαντικές υποχρεώσεις στη δουλειά, στο σχολείο, στο σπίτι, στον κοινωνικό περίγυρο. Ύπαρξη αρνητικών καταστάσεων οι οποίες δημιουργούνται από τη χρήση και έχουν αντίκτυπο στη σωματική και την ψυχική υγεία των χρηστών αυτών. Επιπλέον, παρουσιάζονται ακόμη και προβλήματα με τον νόμο.

δ) Εξάρτηση:

Εδώ ο χρήστης εμφανίζει σημάδια, τα οποία δηλώνουν την καταναγκαστική χρήση του διαδικτύου. Επιπλέον, πρέπει να ληφθεί υπόψη ότι ο χρήστης χάνει πολύ εύκολα τον έλεγχο της χρήσης. Με αυτόν τον τρόπο μπορεί να διαγνωστεί αυτή η χρόνια «ασθένεια». Ωστόσο, η διαδικασία της διάγνωσης χρειάζεται τουλάχιστον ένα χρόνο και προϋποθέτει εμφάνιση συγκεκριμένων συμπτωμάτων, όπως, τη χρήση του υπολογιστή όλο και περισσότερο, τη στέρηση όταν δεν υπάρχει επαφή κτλ. καθώς επίσης και σωματικά και ψυχολογικά προβλήματα όπως η κυκλοθυμία ή ο υποσιτισμός.

ε) Εθισμός:

Εδώ παρατηρούνται όλα τα στοιχεία της εξάρτησης, πράγμα που είναι πια σύνηθες για τον χρήστη. Οι εθισμένοι χρήστες λαχταρούν να χρησιμοποιούν το διαδίκτυο με συγκεκριμένο τρόπο, σε χρονικό διάστημα και συχνότητα τα οποία ενδεχόμενος να αποβούν μοιραία για τον ίδιο και όσους έχουν επαφές μαζί τους.

ΚΕΦΑΛΑΙΟ 3ο : ΠΡΟΛΗΨΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΕΘΙΣΜΟΥ.

3.1. ΠΡΟΛΗΨΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

Η θεραπεία για όσους έχουν εθιστεί στο διαδίκτυο είναι πολύ δύσκολη υπόθεση. Καταρχήν, επειδή ακόμη και σήμερα που πολλοί από εκείνους που παρουσιάζουν προβλήματα απευθύνονται σε επιστήμονες-ειδικούς για να θεραπεύσουν τη διαταραχή η οποία έχει προκληθεί από την κατάχρηση του διαδικτύου, η θεραπεία της διαταραχής αυτής είναι πάρα πολύ δύσκολο να διαγνωστεί διότι δεν υπάρχουν συγκεκριμένα συμπτώματα. Επίσης υπάρχει περίπτωση κάποια από αυτά να μην είναι μόνιμα και να τα συναντάμε σε ανθρώπους οι οποίοι δεν πάσχουν από τη διαταραχή η οποία μελετάται.

Μεγάλη είναι η δυσκολία προσέγγισης του ζητήματος για έναν ακόμη λόγο. Η συγκεκριμένη διαταραχή είναι καινούρια για τα επιστημονικά δεδομένα πράγμα που σημαίνει ότι τα στοιχεία που σχετίζονται μ' αυτήν δεν είναι ακόμη αρκετά ώστε να γίνεται σωστή μεταχείριση των ασθενών. Συνήθως όλο αυτό αντιμετωπίζεται από γιατρούς, ψυχολόγους και άλλους ειδικούς όπως και οι άλλοι εθισμοί. Για να μπορέσει όμως ένα θεραπευτικό πρόγραμμα να είναι λειτουργικό και να πατάει πάνω στις ανάγκες του κάθε θεραπευόμενου πρέπει να είναι ανάλογο της κατάστασης του.

Είναι αρκετοί αυτοί που πιστεύουν ότι ο εθισμός στο διαδίκτυο μοιάζει με τον εθισμό στα τυχερά παιχνίδια και τον τζόγο. Σύμφωνα με έρευνες, τα άτομα που είναι εθισμένα στο διαδίκτυο, όταν είναι συνδεδεμένα στο διαδίκτυο, ο εγκέφαλός τους εκκρίνει ουσίες όμοιες με εκείνες που εκκρίνονται και όταν παίζει ένας εθισμένος στον τζόγο, τυχερά παιχνίδια. Η λύση που δίδεται εδώ είναι η φαρμακευτική αγωγή.

Υπάρχουν επίσης ειδικοί που αντιμετωπίζουν τους ασθενείς με προσέγγιση στην ανθρώπινη ψυχολογία . Το πρόγραμμα στο οποίο βρίσκεται ο θεραπευόμενος θα πρέπει να είναι κομμένο και ραμμένο στις δικές του ανάγκες και το διαδίκτυο να χρησιμοποιείται για να θεραπευτεί ο πάσχων.

Οι πιθανότητες να αναπτυχθεί εθιστική συμπεριφορά σε ένα χρήστη εξαρτάται από τα βιώματα και τις εμπειρίες του ατόμου. Η καλύτερη θεραπεία σε αυτή την περίπτωση είναι η ψυχανάλυση. Αυτό συμβαίνει επειδή θεωρείται ότι πρέπει να γίνει προσέγγιση της συμπεριφοράς του χρήστη από τότε που άρχισε να διαμορφώνεται η προσωπικότητά του

3.2. ΠΑΙΔΙ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Μια από της βασικότερες αιτίες για την κατάχρηση του διαδικτύου είναι το ότι τα παιδιά και οι νέοι έχουν γνώσεις και εμπειρίες σε σχέση με το διαδίκτυο και τους ηλεκτρονικούς υπολογιστές που οι γονείς τους αλλά και οι καθηγητές τους, συνήθως δεν έχουν. Σε γενικές γραμμές η εξάρτηση αυτή δεν είναι κάτι νέο. Σημαντικός παράγοντας ο οποίος παίζει καθοριστικό ρόλο είναι η διαπαιδαγώγηση των παιδιών πάνω στο θέμα.

Ένας ενήλικας ή ένας ανήλικος ο οποίος είναι εθισμένος στο διαδίκτυο εμφανίζει συνήθως τα παρακάτω συμπτώματα:

• Εξιδανίκευση του μέσου: Ο χρήστης πιστεύει ότι ο ηλεκτρονικός υπολογιστής και το διαδίκτυο είναι το πιο σημαντικό κομμάτι της ζωής του.

• Τροποποίηση της διάθεσης: Αυτό οφείλεται στο ότι ο νευροδιαβιβαστής του εγκεφάλου αυξάνει την παραγωγή μια ουσίας που λέγετε ντοπαμίνη. Η ουσία αυτή συνδέεται με την ευχαρίστηση που νιώθει ο χρήστης

• Ανοχή: Ο χρήστης αρχίζει να νιώθει ευχαρίστηση χρησιμοποιώντας όλο και περισσότερες ώρες τον ηλεκτρονικό υπολογιστή και το διαδίκτυο.

• Σύγκρουση: Ο χρήστης ενώ αντιλαμβάνεται την ύπαρξη του προβλήματος δεν μπορεί να δράσει έτσι ώστε να ελαττώσει τη χρήση του ηλεκτρονικού υπολογιστή
Είναι πολλοί αυτοί που δεν ξέρουν πώς να διαχειριστούν μια τέτοια κατάσταση σε περίπτωση που γίνει αντιληπτή η ύπαρξη της. Επίσης, υπάρχει και η πλευρά η οποία δεν έχει αντιληφτεί τι πραγματικά κάνουν τα παιδιά στο διαδίκτυο και πέφτουν από τα σύννεφα με την ανακάλυψη του. Αντί για τις εργασίες του σχολείου ή για έρευνες, αυτά στέλνουν ηλεκτρονικά μηνύματα, παίζουν παιχνίδια online ή συζητούν ακόμη και με αγνώστους στα chat rooms. Αυτό γίνεται επειδή είναι ευκολότερο να κρύβει κανείς τα ίχνη του στο διαδίκτυο και επειδή η εξάρτηση από το αυτό δεν έχει αναγνωριστεί ευρύτερα. Κυρίως οι νεαρές εγκλωβίζονται ευκολότερα σε τέτοιου είδους εξαρτήσεις. .

Μεγάλος αριθμός εφήβων, οι οποίοι είναι εθισμένοι στους ηλεκτρονικούς υπολογιστές παραμελούν οικογενειακές και φιλικές σχέσεις και υποχρεώσεις, ξεχνούν να φάνε ακόμη και να κοιμηθούν. Όλα αυτά όμως οφείλονται όχι μόνο στο διαδίκτυο, αλλά σίγουρα είναι θέμα διαπαιδαγώγησης αρχικά από του γονείς στα παιδιά. Οι νέοι μεταξύ 10-18, εκμεταλλευόμενοι την άγνοια των γονέων και των κηδεμόνων χρησιμοποιούν αλόγιστα το διαδίκτυο χωρίς να τους επιβλέπει και να τους ελέγχει κάποιος. Αυτό που πρέπει να κάνουν γονείς και εκπαιδευτικοί είναι να καλύψουν το τεχνολογικό κενό που υπάρχει ανάμεσα στους προαναφερθέντες και στα παιδιά, έτσι, θα είναι ευκολότερο να προστατεύσουν και να συμβουλεύουν τη νέα γενιά. Η αντιμετώπιση του προβλήματος θα ξεκινήσει όταν όσοι έρχονται σε επαφή με νέους που κάνουν χρήση του διαδικτύου αρχίσουν να ενημερώνονται σωστά και σε επίπεδο που οι γνώσεις θα είναι αρκετές ώστε να βοηθήσουν τα παιδιά τους.

Επιπλέον, σημαντικό ρόλο στο παρόν φαινόμενο έχει και ολόκληρη η κοινωνία, η οποία δεν έχει ούτε τη στοιχειώδη επάρκεια να αντιμετωπίσει τα θέματα που αφορούν τις νέες τεχνολογίες. Είναι σημαντικό να αναφερθεί ότι η εξέλιξη της τεχνολογίας και η χρησιμότητά της πρέπει να ενσωματώνονται στο σχολικό πρόγραμμα, έτσι ώστε να θωρακίζονται τα παιδιά και να προστατεύονται από τους ενήλικες. Το πιο σίγουρο είναι ότι η θεραπεία πρέπει να ξεκινήσει από το σπίτι και την οικογένεια.

<u>Βοήθεια και ενημέρωση γονέων</u>

Η πιο σημαντική προσπάθεια που χρειάζεται να κάνουν γονείς και κηδεμόνες για να καταφέρουν να ελέγχουν την κατάσταση με αποτελεσματικότητα είναι να βρουν τρόπο και χρόνο να μάθουν να χρησιμοποιούν τον ηλεκτρονικό υπολογιστή και το διαδίκτυο. Οι γονείς πρέπει να γνωρίσουν το διαδίκτυο και την τεχνολογία και επιπρόσθετα να διαθέσουν χρόνο στο να έρθουν σε επαφή με το αντικείμενο και να ενδιαφερθούν για τις δραστηριότητες που έχουν τα παιδιά τους στο διαδίκτυο. Θα πρέπει, δηλαδή, να χρησιμοποιούν το διαδίκτυο παρέα με το παιδί ή τα παιδιά, και θα πρέπει να ψάχνουν και να βρίσκουν τρόπους και αφορμές ώστε να συμβουλεύουν τα νεαρά μέλη της οικογένειας τους χωρίς να τα καταπιέζουν. Επίσης, θα πρέπει να γνωρίζουν ότι η εγκατάσταση

συγκεκριμένων φίλτρων στον υπολογιστή μπορεί να προστατέψει τα παιδιά από την εμφάνιση ακατάλληλων ιστοσελίδων.

Βασικό επίσης είναι ο υπολογιστής να μην βρίσκεται στο παιδικό δωμάτιο ώστε να μπορούν να ελέγχουν οι γονείς με διακριτικότητα πάντα τα παιδιά τους. Οι γονείς θα πρέπει να συζητούν με τα παιδιά τους για τον τρόπο που χρησιμοποιούν το διαδίκτυο. Θα πρέπει να είναι σε επαφή με τα παιδιά τους και να τα κάνουν να τους εμπιστεύονται ώστε να μοιράζονται μαζί τους ότι έχει να κάνει με τις δραστηριότητές τους στο διαδίκτυο. Τέλος, θα πρέπει να έχουν τη δυνατότητα να αντιλαμβάνονται αν τα παιδιά τους κάνουν κατάχρηση του διαδικτύου.

Διάφορες θεραπευτικές μονάδες προτείνουν μερικές από τις συμβουλές που πρέπει να ακολουθήσουν οι γονείς

- Ενασχόληση και εκμάθηση διαδικτύου από τους γονείς.

- Αφιέρωση χρόνου στο διαδίκτυο με τα παιδιά

- Τοποθέτηση χρονικών ορίων.

- Έλεγχος των ιστοσελίδων που επισκέπτεται το παιδί και των συνομιλιών των.

- Χρήση ειδικών φίλτρων για επιβλαβείς ιστοσελίδες.

- Συζήτηση για τους κινδύνους.

- Δημιουργία λίστα από πράγματα που θα μπορούσε να κάνει το παιδί αντί να σπαταλάει τον χρόνο του στον ηλεκτρονικό υπολογιστή ή τα βιντεοπαιχνίδια.

- Ενθάρρυνση άλλων δραστηριοτήτων. Σημαντικές στην ανάπτυξη των παιδιών και των εφήβων είναι η ώθηση σε κοινωνικές και αθλητικές δραστηριότητες και η καθιέρωση οικογενειακών δραστηριοτήτων που δεν εμπεριέχουν τη χρήση υπολογιστή και διαδικτύου.

Όσο αφορά την πρόληψη, υπάρχουν πολλοί παράγοντες που επηρεάζουν τον χρήστη και σίγουρα μπορούν να συμβάλουν στην προστασία του. Οι περισσότερες προσπάθειες γίνονται στα πλαίσια της ενημέρωσης των νέων, καθώς αυτή είναι η ηλικιακή ομάδα που κινδυνεύει περισσότερο.

Πιο συγκεκριμένα διακρίνονται οι εξής παράγοντες:

- Η **οικογένεια** είναι αυτή που θα θέσει τα όρια χρήσης σε ότι έχει να κάνει με το πόσο χρόνο ασχολείται με το διαδίκτυο αλλά και για τον τρόπο που το χρησιμοποιεί το παιδί.

- Το **σχολείο** είναι υπεύθυνο να για την πληροφόρηση μαθητών και γονέων σχετικά με τους κινδύνους του διαδικτύου, μέσω των ενημερωμένων εκπαιδευτικών που οφείλει να διαθέτει. Συγκεκριμένα, θα προτείνουν μέτρα πρόληψης άλλα και με τη βοήθεια ειδικών ψυχολόγων θα αντιμετωπίζουν τις περιπτώσεις εκείνες που χρήζουν άμεσης βοήθειας. Ωστόσο, οι εκπαιδευτικοί θα πρέπει να αναλάβουν και έναν ακόμη ρόλο. Θα πρέπει να παρακινούν τους μαθητές τους ώστε να πραγματοποιούν αρκετές από τις σχολικές εργασίες μέσω του υπολογιστή και του διαδικτύου για να γίνουν ευκολότερα αντιληπτές και οι θετικές πλευρές της χρήσης τους.

- **Η κοινωνία** παίζει κι αυτή ένα πολύ σημαντικό ρόλο. Θα ήταν ορθό να συζητηθεί εάν απαιτείται ρύθμιση του ορίου ηλικίας για να εισέλθει ένας έφηβος σε internet cafes. Επιπλέον, θα πρέπει να διευθετηθεί το ζήτημα της ύπαρξης φίλτρων προστασίας σε αυτά τα καταστήματα, ειδικά σε υπολογιστές που χρησιμοποιούν ανήλικοι και τέλος, θα πρέπει να καθοριστεί κάποιο όριο χρόνου που μπορούν να χρησιμοποιούν το διαδίκτυο. Η κοινωνία μπορεί να συμβάλλει και με ενημέρωση γονέων και παιδιών προχωρώντας σε σχετικές καταχωρήσεις σε Μέσα Μαζικής Ενημέρωσης για το

φαινόμενο ή συμμετέχοντας στις μονάδες ενημέρωσης και αντιμετώπισης, στις συμβουλευτικές τηλεφωνικές γραμμές και σε άλλους φορείς που δύνανται να βοηθήσουν. Τέλος, η συμβολή της κοινωνίας θα μπορούσε να ολοκληρωθεί με παροχή πληροφοριών για την ασφαλή χρήση διαδικτύου με υλικό σε έντυπη μορφή, σε μέρη που συχνάζουν οι έφηβοι, καθώς και μέσα από διάφορες ιστοσελίδες που συνήθως επισκέπτονται.

- **Ο τομέας της υγείας** θα μπορεί να ενημερώσει τους χρήστες για την κακή χρήση του διαδικτύου, μέσω του ιατρικού του προσωπικού. Το φαινόμενο της αλόγιστης χρήσης και του εθισμού θα πρέπει να αποτελεί θέμα ανάλυσης σε συνέδρια και ημερίδες, με σκοπό την ευαισθητοποίηση των ειδικών του τομέα υγείας, οι οποίοι με τη σειρά τους θα ευαισθητοποιήσουν γονείς και παιδιά και θα έρθουν οι ίδιοι σε άμεση επαφή με προβληματικές περιπτώσεις.

- Το **κράτος,** από την πλευρά του, θα πρέπει να αναλάβει την ενημέρωση όλου του πληθυσμού, καθώς και την εφαρμογή των μέτρων που προαναφέρθηκαν για την αντιμετώπιση στο σχολείο και την Νομοθεσία για τον τρόπο λειτουργίας των internet cafe.

Θεραπευτική αντιμετώπιση

Περνώντας από το στάδιο της πρόληψης, στο στάδιο της αντιμετώπισης, θα πρέπει να γίνει ξεκάθαρο ότι ίσως χρειαστεί να ακολουθηθεί μια πιο ειδική αγωγή. Σημαντικό ρόλο στην πρόληψη, όπως και στη θεραπεία, παίζουν οι γονείς των παιδιών και των εφήβων. Ωστόσο, σε ορισμένες περιπτώσεις έντονης εξάρτησης, μια πιο επιστημονική και ιατρική θεραπευτική αγωγή είναι το κλειδί για την σίγουρη αντιμετώπιση. Αυτού του είδους η αντιμετώπιση των διαγνωσμένων περιπτώσεων εθισμού στο διαδίκτυο γίνεται με αρκετούς τρόπους, κάποιοι από τους οποίους αναφέρονται επιγραμματικά παρακάτω :

• Συμβουλευτική προσέγγιση στο παιδί ή στον έφηβο καθώς και στην οικογένεια.

• Εφαρμογή Ειδικού εξατομικευμένου προγράμματος για τον περιορισμό της υπερβολικής χρήσης του διαδικτύου.

• Διαπαιδαγώγηση των νέων με σκοπό έναν ορθολογικότερο τρόπο χρήσης των νέων τεχνολογιών.

• Ψυχοθεραπευτική παρέμβαση στις περιπτώσεις εθισμένων χρηστών.

• Φαρμακοθεραπεία, ειδικά σε σοβαρές περιπτώσεις, στις οποίες μπορεί να παρατηρείται αυτοκτονικός ιδεασμός ή καταθλιπτική διαταραχή. Η θεραπεία με φάρμακα ενδείκνυται και σε περιπτώσεις χρηστών με συμπτώματα καχεξίας λόγω της ασταμάτητης πολυήμερης ενασχόλησης με τον υπολογιστή και το διαδίκτυο (π.χ online παιχνίδια). Σε αυτές τις περιπτώσεις, υπάρχει και η δυνατότητα εισαγωγής και νοσηλείας του χρήστη στην παιδοψυχιατρική κλινική.

Πρέπει να γίνει σαφές, ότι το πρόβλημα του εθισμού στο Διαδίκτυο αναγνωρίζεται δύσκολα ως ξεχωριστή ψυχιατρική διαταραχή. Η πρώτη χώρα που αναγνώρισε επισήμως τη διαταραχή είναι η Κίνα τον Νοέμβριο του 2008.

Φίλτρα προστασίας

Τα φίλτρα προστασίας ρυθμίζουν την πρόσβαση του χρήστη σε πληροφορίες ή υπηρεσίες στο Διαδίκτυο με βάση συγκεκριμένα κριτήρια.

Τα συστήματα αυτά μπορούν να εγκατασταθούν στον υπολογιστή ενός χρήστη, σε έναν κεντρικό υπολογιστή κάποιου φορέα, για παράδειγμα σε μια σχολική μονάδα ή στους υπολογιστές

ενός παροχέα υπηρεσιών Διαδικτύου. Έχουν την ικανότητα να προειδοποιήσουν για ενδεχόμενες επικίνδυνες ιστοσελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη, να μπλοκάρουν ύποπτους ιστοχώρους ακόμα και να κλείσουν τελείως τον υπολογιστή.

Τα φίλτρα, επίσης, παρέχουν ένα αξιόπιστο φράγμα, το οποίο αποτρέπει την πρόσβαση του χρήστη σε ύποπτο περιεχόμενο που θεωρείται επικίνδυνο ή δύναται να προκαλέσει ηθικά προβλήματα στην ανάπτυξη των νέων. Παράλληλα, επιτρέπουν την πρόσβαση των παιδιών σε ακίνδυνες ιστοσελίδες. Συμβάλλοντας, επομένως, στην προστασία του παιδιού, τα συστήματα αυτά φιλτράρουν και τα εξερχόμενα από τον υπολογιστή δεδομένα. Αυτό εξυπηρετεί τον γονικό έλεγχο, καθώς μπλοκάρεται η δημοσίευση προσωπικών στοιχείων όπως ονοματεπώνυμο, διεύθυνση σπιτιού ή σχολείου, στοιχεία πιστωτικών καρτών κ.λπ. Κάποια από τα λογισμικά αυτά προγράμματα διατίθενται δωρεάν στο Διαδίκτυο για όλους τους χρήστες. Οι πιο πρόσφατες εκδόσεις λειτουργικών συστημάτων, όπως τα Windows Vista, περιλαμβάνουν τέτοια συστήματα φιλτραρίσματος.

Οι παροχές των φίλτρων προστασίας είναι πολύ σημαντικές, καθώς ενισχύουν τον γονικό έλεγχο, χωρίς ωστόσο, αυτό να σημαίνει ότι είναι ικανά να τον αντικαταστήσουν κιόλας. Μεγάλη προσοχή θα πρέπει να δοθεί στο γεγονός ότι αυτά τα εργαλεία προστασίας μπλοκάρουν πληροφορίες αλλά δεν είναι απαραβίαστα. Επίσης, ενδέχεται να αποκλείσουν αθώο υλικό, το οποίο μπορεί να είναι χρήσιμο για τον χρήστη.

Σε κάθε περίπτωση, θα πρέπει να τονιστεί ότι τα φίλτρα προστασίας είναι κατάλληλα για μικρά παιδιά, ωστόσο, όταν περνούν κάποια ηλικία θα πρέπει να ενημερώνονται ώστε να αναπτύσσουν υπεύθυνη στάση απέναντι στο διαδίκτυο.

Τα είδη φίλτρων που διατίθενται είναι τα εξής:

Περιφραγμένες τοποθεσίες: Οι λεγόμενες «περιφραγμένες τοποθεσίες» είναι λίστες από ιστοσελίδες που είναι κατάλληλες για μικρά παιδιά και επιτρέπουν στον χρήστη να έχει πρόσβαση μόνο σε αυτές.

Λίστες «Οχι»: Πρόκειται για μια λίστα από ιστοσελίδες που πρέπει να αποφευχθούν καθώς περιέχουν προσβλητικό, βίαιο ή ρατσιστικό περιεχόμενο. Όταν το παιδί προσπαθήσει να μπει σε κάποια από αυτές, τότε η πρόσβασή του μπλοκάρεται. Ορισμένα από αυτά τα προγράμματα λειτουργούν και με λίστες απαγορευμένων λέξεων. Μόλις εντοπιστεί κάποια από αυτές τις λέξεις σε μια ηλεκτρονική διεύθυνση ή στην ίδια την ιστοσελίδα, τότε μπλοκάρεται η πρόσβαση. Το μειονέκτημα εδώ είναι ότι απαιτείται συνεχής αναβάθμιση του προγράμματος.

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

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

Αυτοαξιολόγηση ιστοσελίδων: Οι πάροχοι της διαδικτυακής πληροφορίας τοποθετούν εθελοντικά στον ιστοχώρο τους μια ετικέτα η οποία δείχνει αν η ιστοσελίδα αυτή περιέχει ακατάλληλο υλικό (π.χ. βία, γυμνό, τυχερά παιχνίδια, κ.λπ.). Οι ετικέτες αυτές είναι δημιούργημα της Ένωσης Αξιολόγησης Περιεχομένου του Διαδικτύου ICRA. Το φίλτρο, λοιπόν, διαβάζει αυτές τις ετικέτες και αποφασίζει αν θα μπλοκάρει την πρόσβαση, με βάση το περιεχόμενο που οι γονείς επέλεξαν να επιτρέψουν στα παιδιά τους να δουν. Το σημαντικό μειονέκτημα εδώ, είναι ότι βρίσκεται στα χέρια των ιδιοκτητών των ιστοσελίδων να τοποθετήσουν ετικέτες εθελοντικά. Με τα μέχρι τώρα δεδομένα, λίγοι είναι εκείνοι που αξιολογούν τις ιστοσελίδες τους, με βάση το περιεχόμενο.

Συνδυασμός μεθόδων φιλτραρίσματος: Σήμερα, τα προγράμματα φιλτραρίσματος συνδυάζουν πολλούς τρόπους, ώστε να εξασφαλιστεί μεγαλύτερη αποτελεσματικότητα στην προστασία των νέων. Επιπλέον, ο συνδυασμός αυτός βοηθάει και στην διαφοροποίηση του υλικού που πρέπει να βλέπει ένας χρήστης, ανάλογα με την ηλικία του.

Γνώση της πολιτικής απορρήτου κάθε ιστότοπου:

Η πολιτική απορρήτου είναι ουσιαστικά ο τρόπος που μια τοποθεσία χρησιμοποιεί, κοινοποιεί και αποθηκεύει τα προσωπικά δεδομένα που συλλέγει από τους χρήστες. Οι γονείς θα πρέπει κάθε φορά να διαβάσουν την πολιτική απορρήτου μιας διαδικτυακής τοποθεσίας και να δείξουν στα παιδιά τους τι θα πρέπει να προσέχουν πριν προβούν στη δήλωση προσωπικών δεδομένων τους. Τις περισσότερες φορές, οι πολιτικές απορρήτου είναι μακροσκελείς, λεπτομερείς και ασαφείς. Ωστόσο, ο χρήστης θα πρέπει να γνωρίζει ότι αν μια διαδικτυακή τοποθεσία δεν διαθέτει πολιτική απορρήτου, τότε θα πρέπει να αποφεύγει, ή να πραγματοποιεί με προσοχή, αγορές ή δηλώσεις προσωπικών δεδομένων σε αυτή την τοποθεσία.

Ο χρήστης που διαβάζει μια πολιτική απορρήτου, θα πρέπει να γνωρίζει:

- Με ποιον τρόπο χρησιμοποιεί η συγκεκριμένη τοποθεσία τις πληροφορίες που συλλέγει από τον ίδιο.

- Εάν ο χρήστης ή ο κηδεμόνας του, μπορούν να αλλάξουν ή να διαγράψουν δεδομένα που έχουν φανερώσει στην τοποθεσία.

Όσο εύκολο είναι να γίνει έλεγχος των ιστοσελίδων που επισκέπτεται ένας χρήστης, άλλο τόσο εύκολο είναι για έναν γνώστη των ηλεκτρονικών υπολογιστών να καλύψει τα ίχνη του στο διαδίκτυο. Στις μέρες μας, είναι γνωστό ότι τα παιδιά και οι έφηβοι είναι καλοί γνώστες του αντικειμένου, ίσως και καλύτεροι από κάποιους ενήλικες. Θα ήταν αποτελεσματικότερο να θεσπιστούν συγκεκριμένοι κανόνες σχετικά με τη χρήση του Διαδικτύου καθώς και να υπάρχει ανοικτή επικοινωνία με το παιδί.

Όταν λαμβάνει χώρα κάποια περιήγηση στο Διαδίκτυο, το πρόγραμμα πλοήγησης του Ιστού συλλέγει πληροφορίες σχετικά με τις τοποθεσίες που έχει επισκεφτεί ο χρήστης. Όλες αυτές οι πληροφορίες αποθηκεύονται στον υπολογιστή. Τα προγράμματα πλοήγησης κρατούν, συνήθως, ένα ιστορικό των τελευταίων δικτυακών ιστοσελίδων, στις οποίες έγιναν επισκέψεις από τον χρήστη. Ο πιο εύκολος τρόπος για να ελεγχθούν οι ιστοσελίδες που επισκέπτονται τα παιδιά, είναι πατώντας το κουμπί Ιστορικού που βρίσκεται πάνω δεξιά στη γραμμή εργαλείων και είναι διαθέσιμο στα περισσότερα προγράμματα πλοήγησης. Ο χρήστης μπορεί να προβάλει ξανά όλες τις ιστοσελίδες που επισκέφτηκε το παιδί, κάνοντας απλά διπλό κλικ στις σελίδες της λίστας ιστορικού. Τα προγράμματα πλοήγησης μπορούν επίσης να κρατούν προσωρινά αντίγραφα των ιστοσελίδων του ιστορικού και τα αποθηκεύουν στον υπολογιστή.

Δομές στην Ελλάδα για την αντιμετώπιση του Εθισμού στο Διαδίκτυο

Ελληνική Εταιρία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο

Η Ελληνική Εταιρία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο είναι μία από τις αξιόλογες προσπάθειες που γίνονται στην Ελλάδα, για τη μελέτη του διαδικτυακού Εθισμού. Σκοπός της Εταιρείας αυτής είναι να συμβάλλει με τη δράση της κυρίως στην αναγνώριση, τη μελέτη και την αντιμετώπιση του φαινομένου της Διαταραχής Εθισμού στο Διαδίκτυο. Ο ρόλος της Εταιρίας είναι

τόσο επιστημονικός όσο και κοινωφελής. Επιπλέον, φροντίζει για την πρόληψη των δυσάρεστων επιπτώσεων της μη έγκαιρης διάγνωσης του Εθισμού στο Διαδίκτυο.

Η Εταιρεία ιδρύθηκε τον Σεπτέμβριο του 2008, με σκοπό να παρέχει εξειδικευμένες υπηρεσίες Ψυχικής υγείας, ένας τομέας που μειονεκτεί στην Ελλάδα. Προσπαθώντας, επομένως, να αντιμετωπίσει διαταραχές εθισμού στο διαδίκτυο των παιδιών και των εφήβων, έχει ήδη αναλάβει με επιτυχία, αρκετές κλινικές περιπτώσεις. Διακεκριμένοι επιστήμονες και επαγγελματίες της ψυχικής υγείας διαφόρων ειδικοτήτων στελεχώνουν το προσωπικό της Εταιρίας, με έδρα τη Λάρισα, στη Θεσσαλία.

Το ειδικό αυτό ιατρείο ασχολείται με διάφορα περιστατικά και θέτει ως στόχους του τα εξής:

α) Την εξέταση όλων των εφήβων, από 10 έως 18 ετών τα οποία εντοπίζονται να πραγματοποιούν προβληματική χρήση του υπολογιστή και του διαδικτύου,

β) Τη διάγνωση του εθισμού των εφήβων στους Υπολογιστές με την ήδη γνωστή Κλίμακα εθισμού των εφήβων στους ηλεκτρονικούς υπολογιστές (Κ.Ε.ΕΦ.Υ) (Σιώμος 2008) και την Κλίμακα YDQ, η οποία περιλαμβάνει 8 ερωτήσεις για τον εθισμό του ατόμου στο Διαδίκτυο (προσαρμοσμένο στην ελληνική γλώσσα) και τέλος

γ) Τη θεραπεία των διαγνωσμένων περιπτώσεων εθισμού στους ηλεκτρονικούς υπολογιστές και στο διαδίκτυο.

Συμβουλευτική υπηρεσία για την αντιμετώπιση της παθολογικής χρήσης Η/Υ και Διαδικτύου από φοιτητές

Η συμβουλευτική αυτή υπηρεσία δημιουργήθηκε για να αντιμετωπίσει εξειδικευμένες υπηρεσίες ψυχικής υγείας που αφορούν την κακή χρήση Η/Υ και Διαδικτύου στο κομμάτι των φοιτητών σε ιδρύματα Ανώτερης και Ανώτατης εκπαίδευσης στην Θεσσαλονίκη. Πρόκειται για μια επέκταση των υπηρεσιών της Β' Πανεπιστημιακής Ψυχιατρικής κλινικής, η οποία ήδη από το 1986 έχει αναπτύξει συμβουλευτικό τμήμα Ψυχικής Υγείας απευθυνόμενο στον πληθυσμό των φοιτητών της πόλης της Θεσσαλονίκης. Πλέον είναι σε θέση να καλύψει περιστατικά διαταραχής που αναπτύχθηκαν από τους σπουδαστές στη διάρκεια των τελευταίων χρόνων, με την εξέλιξη των νέων τεχνολογιών.

Μονάδα Απεξάρτησης 18 Άνω.

Αυτή η Μονάδα Απεξάρτησης αφορά σε όλα τα άτομα ηλικίας 18 και άνω. Ιδρύθηκε κι αυτή με τη σειρά της στην Ελλάδα με σκοπό να προσφέρει εξειδικευμένες υπηρεσίες υποστήριξης στα άτομα που κάνουν προβληματική χρήση του διαδικτύου. Συγκεκριμένα, καλύπτει πολλά περιστατικά εθισμού και ειδικεύεται στην πρόληψη, θεραπεία και κοινωνική επανένταξη των χρηστών.

Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.)

Ακόμη μια ισχυρή δομή στην Ελλάδα, αποτελεί η **Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ)** της Β' Παιδιατρικής Κλινικής του Παν/μιου Αθηνών στο Νοσοκομείο Παίδων «Π.&Α. Κυριακού». Η συγκεκριμένη Μονάδα αποτελεί δομή-πρότυπο και στοχεύει στην παροχή υπηρεσιών σε έφηβους ηλικίας 11εώς 18 ετών και στις οικογένειες τους, για θέματα που αφορούν οποιοδήποτε πρόβλημα (χρόνια νοσήματα, θέματα ανάπτυξης, γυναικολογικά προβλήματα, θέματα διαταραχής, μαθησιακά και ψυχοκοινωνικά προβλήματα και πολλά άλλα). Ωστόσο, το 2007 η Μονάδα κλήθηκε να αντιμετωπίσει περιστατικά εφήβων που δεν πραγματοποιούσαν ορθή χρήση του διαδικτύου, το οποίο

κατέληξε να αποτελεί αναπόσπαστο κομμάτι της ζωής τους. Από τότε η ενασχόληση με το θέμα της **διαδικτυακής ασφάλειας,** ανταποκρινόμενη στις ανάγκες της σημερινής κοινωνίας, σε πολλά επίπεδα, αποτέλεσε για τη Μονάδα μονόδρομο.

Θα πρέπει να τονιστεί ότι η Μονάδα διαθέτει Τμήμα Ασφάλειας του Διαδικτύου, το οποίο είναι υπεύθυνο για τη φροντίδα και την εξατομικευμένη αντιμετώπιση των προβλημάτων που αντιμετωπίζουν παιδιά και έφηβοι λόγω προβληματικής χρήσης του διαδικτύου. Τα θέματα που τους απασχολούν συνήθως είναι ακατάλληλο περιεχόμενο στο Διαδίκτυο, εκφοβισμός του χρήστη, κακοποίηση, συμπεριφορές εξάρτησης και άλλα. Η Μ.Ε.Υ. αποτέλεσε την πρώτη από τις δομές στην Ελλάδα που πρωτοάγγιξε το πρόβλημα της υπερβολικής χρήσης στο διαδίκτυο.

Συγχρόνως, παρέχονται συγκεκριμένες προτάσεις σχετικά με τη δημιουργική απασχόληση στο διαδίκτυο. Υπάρχουν πολλά προγράμματα με συμβουλές για την αποφυγή κινδύνων μέσω του διαδικτύου. Τα περισσότερα παιδιά που απευθύνονται στη Μονάδα, επιθυμούν να συμμετέχουν σε αυτά τα προγράμματα, προστατεύοντας έτσι τους εαυτούς τους από τις παγίδες που κρύβει το διαδίκτυο.

ΚΕΦΑΛΑΙΟ 4ο : ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

4.1. ΕΙΣΑΓΩΓΗ

Ένα φαινόμενο πραγματικά μοναδικό στην ιστορία του εγκλήματος είναι τα εγκλήματα μέσω διαδικτύου. Ο θύτης διαπράττει ευκολότερα ένα έγκλημα, όταν γνωρίζει ότι δεν υπάρχουν στοιχεία που θα τον καταστήσουν ένοχο. Η αποκάλυψη των στοιχείων είναι εκείνη που οδηγεί τελικά στον εντοπισμό του. Αυτή η πραγματικότητα είναι που βοηθάει στο να γίνουν κατανοητοί οι λόγοι για τους οποίους χρησιμοποιείται το δίκτυο από εγκληματίες κάθε είδους.

Τα εγκλήματα στο διαδίκτυο είναι γρήγορα, καθώς διαπράττονται σε ελάχιστο χρόνο και τις περισσότερες φορές δεν το καταλαβαίνει ούτε το θύμα. Βέβαια το να διαπράξει κάποιος ένα τέτοιου είδους έγκλημα είναι ευκολότερο όταν γνωρίζει το αντικείμενο. Σ αυτήν την περίπτωση ενδέχεται να μην αφήνει καν ψηφιακά ίχνη. Επίσης μπορεί να διαπραχθεί έγκλημα χωρίς να χρειάζεται να κουνηθεί ο θύτης από τη θέση του, το σπίτι του, το γραφείο του.

Οι εγκληματίες διαδικτύου τις πιο πολλές φορές δεν παρουσιάζονται με την αληθινή τους ταυτότητα, αλλά εμφανίζονται παρουσιάζοντας μια ψεύτικη. Ένα έγκλημα διαδικτύου μπορεί να πραγματοποιηθεί την ίδια στιγμή σε πολλά διαφορετικά μέρη. Επιπλέον, θεωρείται αρκετά δύσκολη η διερεύνηση του εγκλήματος και ο εντοπισμός των ατόμων που εμπλέκονται, αν και η δίωξη ηλεκτρονικού εγκλήματος τα τελευταία χρόνια κυρίως κάνει θαύματα Υπάρχει, παραδείγματος χάριν, η περίπτωση να εντοπιστεί το στίγμα κάποιου, ο οποίος έδρασε κακόβουλα, στην Ελλάδα αλλά τα στοιχεία της ενοχής του να εντοπιστούν στην Ιαπωνία ή ακόμη και να βρίσκονται σε πάρα πολλές διαφορετικές χώρες. Το ενδεχόμενο κάποιος να δράσει στα όρια μόνο μιας χώρας είναι εξαιρετικά σπάνιο. Η καταγραφή της εγκληματικότητας στο διαδίκτυο είναι κάτι πολύ δύσκολο, επειδή οι περιπτώσεις εγκλημάτων που αφορούν το διαδίκτυο και καταγγέλλονται, είναι ελάχιστες. Αυτό έχει σαν αποτέλεσμα, οι εγκληματικές δράσεις του διαδικτύου να μην περιορίζονται και να είναι περισσότερες και από αυτές που διαπράττονται σε ένα οποιοδήποτε πραγματικό χώρο.

Αφότου ο ηλεκτρονικός υπολογιστής και το διαδίκτυο εισέβαλαν στη ζωή μας, δημιουργήθηκαν πολλές δυνατότητες χρήσης αλλά σίγουρα και κατάχρησης. Τα εγκλήματα στο διαδίκτυο συνεχώς εξαπλώνονται, άρα και οι πιθανότητες να κάνουν την εμφάνιση τους νέες μορφές είναι μεγάλες. Συνεπώς επιβάλλεται η ταχύτερη, έγκαιρη και καλύτερη αντιμετώπιση του ζητήματος πάντα μέσα στα πλαίσια του νόμου, εντός και εκτός συνόρων.

ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

4.2. ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

Ο κύριος όγκος των πληροφορικών εγκλημάτων εντάσσεται στην υποκατηγορία των πληροφορικών οικονομικών εγκλημάτων. Ακριβέστερα, τα πληροφορικά οικονομικά εγκλήματα απαρτίζουν, τον κύριο όγκο των διαπιστωμένων πληροφορικών εγκλημάτων και τα εγκλήματα που τραβούν την προσοχή της πλειονότητας των ερευνητών του πληροφορικού εγκλήματος.

Στη διεθνή βιβλιογραφία, η αναλογία μεταξύ των διάφορων υποκατηγοριών πληροφορικού εγκλήματος που απασχολούν τους ειδικούς είναι χαρακτηριστική: σε κάθε δώδεκα περιπτώσεις πληροφορικού οικονομικού εγκλήματος αναλογεί μόλις μία περίπτωση των άλλων κατηγοριών. Ένας παράγοντας που συμβάλλει σ' αυτή τη δυσαναλογία αποτελεί το γεγονός ότι το πληροφορικό οικονομικό έγκλημα είναι ευκολότερα διαπιστώσιμο: Κατά κανόνα, γίνεται αντιληπτό από τους ενδιαφερόμενους σε σχετικά μικρό χρονικό διάστημα μετά την τέλεσή του. Επιπλέον, είναι μετρήσιμο με αρκετή ακρίβεια - τουλάχιστον όσον αφορά στα οικονομικά του μεγέθη.

Ένας δεύτερος παράγοντας είναι το γεγονός ότι οι ίδιες οι επιχειρήσεις έχουν δείξει μεγάλο ενδιαφέρον γι ' αυτό τον τύπο πληροφορικού εγκλήματος και έχουν διαθέσει πολύ σημαντικούς πόρους για τη διερεύνησή του. Συνεπώς, η ισχύς των επιχειρήσεων συμβάλλει σε σημαντικό βαθμό στην αύξηση της αντιπροσώπευσης του πληροφοριακού οικονομικού εγκλήματος μέσα στο ευρύτερο πληροφορικό έγκλημα.

Ένας τρίτος παράγοντας είναι ότι συχνά το πληροφορικό οικονομικό έγκλημα είναι ευκολότερα ανακοινώσιμο, τόσο σε σύγκριση με μία σημαντική μερίδα υπερατομικών πληροφορικών εγκλημάτων όπως είναι οι περιπτώσεις κατασκοπείας, όσο και σε σύγκριση με μερίδα των πληροφορικών εγκλημάτων κατά των προσωπικών δικαιωμάτων όπου, συχνά, το ίδιο το θύμα δεν επιθυμεί την αποκάλυψη.

Στο πλαίσιο των πληροφορικών οικονομικών εγκλημάτων, η απάτη μέσω υπολογιστή περιλαμβάνει την παραποίηση κάποιων δεδομένων ή πληροφοριών που φιλοξενούνται στις βάσεις δεδομένων ή σε προγράμματα με σκοπό το οικονομικό κέρδος . Λεπτομερέστερα , αφορά κυρίως στην κλοπή , διαγραφή , αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος .

Κεντρικό αντικείμενο-στόχος της συγκεκριμένης μορφής απάτης είναι τα δεδομένα που φιλοξενούνται στον υπολογιστή και αφορούν σε οικονομικά μεγέθη. Η συγκεκριμένη απάτη μετεξελίχθηκε στο πέρασμα του χρόνου από ένα ομοιογενές σύνολο αδικημάτων, της εποχής των κεντρικών πληροφορικών συστημάτων, σε μία διαφοροποιημένη ενότητα που περιγράφει ένα μεγάλο φάσμα διαφορετικών υποθέσεων στο πεδίο του οικονομικού εγκλήματος.

Παραποίηση λογιστικών λογαριασμών

Η απάτη σε βάρος μιας επιχείρησης ή ενός ιδιώτη μέσω της εστίασης, και παραποίησης, σε πληροφορίες και δεδομένα, τα οποία τους αφορούν άμεσα και έμμεσα, έχει να κάνει με τους άυλους πόρους, όπως χρηματικές καταθέσεις, οικονομικούς τίτλους, για παράδειγμα, ομόλογα, και λογιστικά μεγέθη, όπως ισολογισμούς. Συχνά, υπάρχουν περιπτώσεις βελτίωσης της πίστης μέσω της παραποίησης των δεδομένων που αναφέρονται σε ένα άτομο ή μία επιχείρηση, ώστε για παράδειγμα, να μπορεί να πάρει δάνειο ή να πάρει δάνειο με καλύτερους όρους, αλλά και χειροτέρευσης της φερεγγυότητας ενός ατόμου ή μιας επιχείρησης, για τους αντίθετους λόγους, που μπορεί να πραγματοποιηθεί από κάποιο άτομο ή επιχείρηση εχθρικά διακείμενων ή αντίθετων συμφερόντων.

Αναφορικά με τους άυλους πόρους, ένα παράδειγμα τυπικής παραποίησης, μέσω εισαγωγής δεδομένων για προσωπικό όφελος, αποτελεί η περίπτωση υπαλλήλου που εργαζόταν ως χειριστής και ελεγκτής δεδομένων στο τμήμα επεξεργασίας δεδομένων τράπεζας στη Ζυρίχη, μιας από τις μεγαλύτερες τράπεζες της Ελβετίας. Ο υπάλληλος πέτυχε να θέσει μερικώς, υπό τον έλεγχό του, το αυτόματο σύστημα μεταβίβασης ξένων πληρωμών. Στη συνέχεια, υπέκλεψε πολλές και διάφορες εντολές μεταβίβασης από τους συνεργάτες του στο τμήμα κωδικοποίησης της τράπεζας. Κατόπιν, αντί να τροφοδοτεί τον υπολογιστή με τα ακριβή ποσά μεταβίβασης , κάθε φορά τροφοδοτούσε, τα εν λόγω ποσά με ανακριβή δεδομένα. Έχοντας άφθονο χρόνο στη διάθεσή του, εντόπισε με ακρίβεια και παρέκαμψε τα μέτρα ασφαλείας της τράπεζας που είχαν οργανωθεί με σκοπό την αποτροπή τέτοιων χειρισμών. Έτσι, για παράδειγμα, όταν 98 Γερμανικά μάρκα καταθέτονταν στην Φρανκφούρτη, οι συνεργοί του - αποσύροντας τα χρήματα στο Λουγκάνο και το Νταβός δεν παραλάμβαναν 100 αλλά 100.000 Ελβετικά φράγκα. Παρόμοια, για μία κατάθεση 97 δολαρίων στην Νέα Υόρκη, δεν αποκόμιζαν 251 αλλά 251.000 Ελβετικά φράγκα. Κατ ' αυτό τον τρόπο , οι δράστες αποκόμισαν συνολικά κέρδη της τάξης των 700.000 Ελβετικών φράγκων.

Παραποιημένη εφαρμογή ηλεκτρονικών πληρωμών

Η απάτη μέσω υπολογιστή με την παρέμβαση στο σύστημα επεξεργασίας δεδομένων ενός οργανισμού ή μιας επιχείρησης απαντάται συχνά σε ζητήματα μισθών, συντάξεων αλλά και των τραπεζικών καταθέσεων. Σε ένα απροστάτευτο σύστημα, η δημιουργία ενός τραπεζικού λογαριασμού πολλών μηδενικών είναι ζήτημα λεπτών - και για έναν έμπειρο hacker, είναι ζήτημα δευτερολέπτων. Αν το πληροφορικό σύστημα διαθέτει έναν αμυντικό μηχανισμό προηγούμενης γενιάς και αν ο

συγκεκριμένος hacker έχει τον απαιτούμενο χρόνο ώστε να αρκείται σε έναν αρχικό λογαριασμό ενός ή δύο μηδενικών, και κατόπιν να εισάγει μία ρουτίνα προσθήκης πέντε μηδενικών σε κάποια συχνά μεν, αλλά άτακτα χρονικά διαστήματα, δεν έχει λόγους να φοβάται τυχόν αποτυχία του.

Πέρα όμως, από τις περιπτώσεις παράνομης κατασκευής δεδομένων, συχνά εμφανίζονται στη διεθνή βιβλιογραφία και ειδησεογραφία, πολλές περιπτώσεις παραβίασης καρτών συναλλαγής και ανάλογων μέσων πληρωμής. Ακόμη και αν τέτοιου είδους απάτες οδηγούν σε μικρές συνολικά ζημιές, οι στατιστικές δείχνουν πως η κακοχρησία των καρτών αποτελεί μία από τις πιο συχνές υποθέσεις πληροφορικού εγκλήματος. Μια παραποιημένη πληρωμή διαπράττεται μέσω τράπεζας, που διαθέτει σύστημα αυτόματης ανάληψης ή χορήγησης χρήματος (μηχανήματα ATM, υπηρεσίες win- banking και άλλα).

4.3. ΠΟΡΝΟΓΡΑΦΙΑ

Η διακίνηση πορνογραφικού υλικού, δεν είναι ένα νέο έγκλημα. Η εξάπλωση όμως, του Διαδικτύου, έχει διευκολύνει τη διάπραξη του. Στατιστικές μελέτες έχουν δείξει ότι η διακίνηση υλικού πορνογραφίας μέσω διαδικτύου, αποτελεί, μια από τις πιο συχνές μορφές εγκλήματος. Τα αδικήματα που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται τόσο με τη δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνηση του. Η παράνομη διακίνηση υλικού παιδικής πορνογραφίας έχει λάβει τεράστιες διαστάσεις, προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές αρχές. Το πορνογραφικό υλικό, που διακινείται μέσω διαδικτύου, μπορεί να είναι σε μορφή πολυμέσων. Ο κάθε χρήστης μπορεί εύκολα να το «κατεβάσει» στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητα του. Δυστυχώς, τέτοιου είδους υλικό, βρίσκεται σε διαφόρους διαδικτυακούς τόπους. Μάλιστα, σε συγκεκριμένους διαδικτυακούς τόπους, γίνεται ανταλλαγή υλικού, δηλαδή αντί ο χρήστης να πληρώσει για υλικό που προμηθεύεται, προσφέρει άλλο υλικό ως αντάλλαγμα.

Η σεξουαλική κακοποίηση ανηλίκων και γυναικών είναι μια από τις αρχαιότερες μορφές εγκλήματος. Με την εμφάνιση και τη χρήση του διαδικτύου έχουμε μια νέα γέφυρα προς το έγκλημα. Η παιδική πορνογραφία στο διαδίκτυο εμφανίζεται με τη μορφή εικόνων, φωτογραφιών καθώς και μαγνητοσκοπημένων σκηνών στις οποίες παρουσιάζονται γυμνά κορμιά παιδιών, ανήλικοι να αυνανίζονται και ακόμη χειρότερα, ανήλικοι να κακοποιούνται σεξουαλικά από ενηλίκους. Αυξημένη ζήτηση υπάρχει στην κακοποίηση ανηλίκων από υπερήλικες και γενικότερα στο οτιδήποτε διαστροφικό. Η νέα τεχνολογία δίνει τη δυνατότητα παρακολούθησης ή και συμμετοχής σε διαστροφικά παιχνίδια μέσω διαδικτύου, με θύματα γυναίκες και παιδιά.

Το πρόβλημα μπορεί να προσεγγισθεί από δύο διαφορετικές πλευρές, όσον αφορά το πώς επηρεάζεται η συμπεριφορά των παιδόφιλων με την είσοδό τους σε πορνογραφικές ιστοσελίδες. Ενδέχεται, οι ορέξεις του δράστη να ικανοποιηθούν και να εκτονωθούν αποκλειστικά και μόνο με τον τρόπο αυτό και να μην εκδηλωθούν οι διαστροφικές του τάσεις στο υπόλοιπο κοινωνικό περιβάλλον. Ωστόσο, ενδέχεται τα θεάματα αυτά να του δημιουργήσουν κάποιου είδους ψύχωση, την οποία θα προσπαθήσει να εκδηλώσει στον κοινωνικό του περίγυρο, κακοποιώντας σεξουαλικά κάποιο ανήλικο άτομο. Επιπλέον, οι παιδόφιλοι δημιουργούν τα δικά τους δωμάτια επικοινωνίας στο διαδίκτυο, στα οποία είναι μόνο αυτοί ευπρόσδεκτοι, ανταλλάσσοντας ιδέες, εμπειρίες και τακτικές προσέγγισης ανηλίκων.

Η σεξουαλική κακοποίηση των παιδιών για πορνογραφικούς σκοπούς, μπορεί να αποδειχτεί μια πολύ επικερδής επιχείρηση. Έτσι, με τη δουλειά αυτή ασχολούνται άτομα με τεράστια γνώση στο χώρο των υπολογιστών και μακρά πείρα χρήσης του μέσου. Τα πιο αισχρά και πλέον διαδεδομένα κυκλώματα παιδικής πορνογραφίας κρύβονται πολύ προσεκτικά στο Διαδίκτυο, πίσω από

κρυπτογραφημένες διευθύνσεις και κωδικούς που γνωρίζουν μόνον όσοι πληρώνουν αδρά. Υπάρχουν δυστυχώς πάρα πολλοί δικτυακοί τόποι που έχουν πορνογραφικό περιεχόμενο και λειτουργούν ως «κλάμπ παιδεραστών» και τα οποία πουλούν φωτογραφίες και βιντεοταινίες με ανήλικους πρωταγωνιστές. Πολλοί από αυτούς τους δικτυακούς τόπους διοργανώνουν ακόμα και ταξίδια σε χώρες όπως η Ιαπωνία ή η Ταϊλάνδη υποσχόμενοι να ικανοποιήσουν ακόμα και τις πιο απαιτητικές και διαστροφικές επιθυμίες των πελατών τους.

Οι δικτυακοί τόποι της παιδικής πορνείας δεν βρίσκονται επισήμως καταχωρημένοι στο διαδίκτυο. Οι ενδιαφερόμενοι μπορούν να αναζητήσουν ηλεκτρονικές διευθύνσεις με «μαλακό πορνό», μέσω άλλων ηλεκτρονικών διευθύνσεων ερωτικού ή συναφούς περιεχόμενου. Στις διευθύνσεις εκείνες όμως που έχουν πιο «σκληρό πορνό» μπορεί να φτάσει κάποιος μόνο αν ψάξει ενδελεχώς στο διαδίκτυο. Οι κωδικοποιημένες πορνογραφικές διευθύνσεις ανακοινώνονται μόνο ιδιωτικά, μέσω ηλεκτρονικού ταχυδρομείου, ενώ οι παράνομες υπηρεσίες που προσφέρονται, γίνονται γνωστές μέσα από διάφορες ομάδες συζητήσεων, που κρύβονται πίσω από παραπλανητικούς τίτλους με πλαστά ενδιαφέροντα, όπως μουσική, ταξίδια ή αθλητισμός. Οι μηχανές αναζήτησης του διαδικτύου σπάνια θα καταδείξουν μια ηλεκτρονική διεύθυνση που έχει ως κύριο περιεχόμενο την παιδική πορνογραφία.

Στο διαδίκτυο παρουσιάζονται και διακινούνται καθημερινά χιλιάδες φωτογραφίες βασανιστηρίων χωρίς έλεγχο, οι οποίες χωρίς δυσκολία χαρακτηρίζονται αδικαιολόγητα ως «ερωτικές». Οι έμποροι της παιδικής σάρκας, προκειμένου να στοχεύσουν σε κοινό με συγκεκριμένα ενδιαφέροντα, τονίζουν την καταγωγή και την ηλικία των ανήλικων θυμάτων.

Η εξάπλωση του φαινομένου της πορνογραφίας και της πορνείας ανηλίκων στο διαδίκτυο είναι πλέον γεγονός. Αυτό σαφώς δικαιολογείται, καθώς το διαδίκτυο αποτελεί τον ιδανικό χώρο όπου οποιοσδήποτε μπορεί να περάσει από το πραγματικό στο φανταστικό, από έναν κόσμο με κανόνες ηθικής και νόμους σε έναν άλλον κόσμο, όπου όλα επιτρέπονται, και δεν υπάρχουν ηθικοί ή άλλοι φραγμοί. Ο χρήστης του δικτύου που αναζητά πορνογραφικό υλικό, ζει σε έναν κόσμο φανταστικό όπου μπορεί να βγάλει στην επιφάνεια τις ερωτικές και σεξουαλικές του προτιμήσεις ελεύθερα, χωρίς τον κίνδυνο της αποκάλυψης των ορέξεών του ή της ταυτότητάς του, της κριτικής, του κοινωνικού ελέγχου, ή ακόμα και της ποινικής διώξεώς του. Πολλοί από αυτούς τους χρήστες της αναζήτησης υλικού παιδικής πορνογραφίας είναι οικογενειάρχες, επαγγελματίες με υψηλό εισόδημα, ίσως και επιφανή μέλη της κοινωνίας, που δε θα μπορούσαν διαφορετικά να εξωτερικεύσουν ασφαλώς αυτή την ερωτική τους διαστροφή. Μέσω όμως του Διαδικτύου δε ρισκάρουν απολύτως τίποτα και νιώθουν ασφαλείς, φυσιολογικοί και νόμιμοι, αφού καλύπτονται πίσω από την ανωνυμία μιας τυχαίας διεύθυνσης ηλεκτρονικού ταχυδρομείου.

Είναι χαρακτηριστικό πως ο αριθμός των δικτυακών τόπων, που προβάλλουν την παιδική πορνογραφία έχει ξεπεράσει τις 100.000 και αυξάνεται διαρκώς. Αυτό προκύπτει από το γεγονός ότι και οι επισκέπτες αυτών των sites αυξάνονται με γρήγορους ρυθμούς. Χαρακτηριστικό της δυναμικής αυτού του φαινομένου είναι το γεγονός ότι τον πρώτο μήνα λειτουργίας μίας τέτοιας ιστοσελίδας έγιναν 3.000 επισκέψεις, τον δεύτερο μήνα 90.000 και τον τρίτο μήνα (λίγο πριν το κλείσιμο) ο αριθμός των επισκεπτών είχε φθάσει τα 3,2 εκατομμύρια. Αναζητώντας την αιτιολογία του φαινομένου καταλήγουμε ότι η φτώχεια είναι ο κύριος καταλύτης, αν και δεν μπορεί να εξηγήσει επαρκώς την εμπορική σεξουαλική εκμετάλλευση των παιδιών.

Το πρόβλημα της διαδικτυακής παιδικής πορνογραφίας διακρίνεται σε τρεις συνιστώσες: την παραγωγή, τη διακίνηση και το κατέβασμα (downloading) υλικού. Το διαδίκτυο προσφέρει μια μεγάλη ποικιλία τρόπων για τη δημιουργία, τη συλλογή και τη διακίνηση αρχείων, τους οποίους όπως είναι φυσικό εκμεταλλεύονται οι παραγωγοί αλλά και οι διανομείς παιδικού πορνογραφικού υλικού για την ικανοποίηση του πάθους τους και φυσικά για την αποκομιδή κέρδους.

Παραγωγή.

Η παραγωγή αφορά στη δημιουργία παιδικών πορνογραφικών εικόνων και βίντεο. Μεγάλο μέρος του πορνογραφικού υλικού που κυκλοφορεί στο διαδίκτυο είναι σχετικά παλαιό, και συνήθως αποτελείται από εικόνες αποσπασμένες από ταινίες ή περιοδικά που είχαν κυκλοφορήσει πολλά χρόνια πριν. Εξαιτίας αυτού βέβαια, πολλοί συλλέκτες τέτοιου υλικού προκηρύσσουν και δίνουν αμοιβή, σε όποιον αναρτήσει στο διαδίκτυο νέο παιδικό πορνογραφικό υλικό.

Οι καινούργιες αυτές πορνογραφικές εικόνες, παράγονται είτε από επαγγελματίες και απεικονίζουν τη σεξουαλική κακοποίηση αλλοδαπών κυρίως παιδιών, είτε τις περισσότερες φορές από ερασιτέχνες, οι οποίοι καταγράφουν την κακοποίηση ανηλίκων από τους ίδιους. Δημιουργούν έτσι ταινίες ή φωτογραφίες υψηλής ποιότητας, με τη χρήση ψηφιακών ηλεκτρονικών μέσων, όπως κάμερες και φωτογραφικές μηχανές, οι οποίες συνδέονται με τον υπολογιστή με ένα USB καλώδιο ή με κάρτα μνήμης και δίνουν τη δυνατότητα εύκολης και γρήγορης ανάρτησης στο διαδίκτυο του υλικού. Είναι ευρέως γνωστό ότι προγράμματα υπολογιστών για την επεξεργασία φωτογραφιών, τα οποία είναι ιδιαίτερα εύκολα στη χρήση, όπως το photoshop, επιτρέπουν στον οποιονδήποτε χρήστη τη δημιουργία μορφοποιημένων εικόνων και πλαστών φωτογραφιών από το ήδη υπάρχον πορνογραφικό υλικό, δημιουργώντας ουσιαστικά νέες απεικονίσεις.

Τέλος, η τεχνολογία που χρησιμοποιείται σήμερα στα κινητά τηλέφωνα, επιτρέπει στους κατόχους τους, και φυσικά στον οποιοδήποτε, να τραβήξει φωτογραφίες κάποιον τρίτο σε ανύποπτη στιγμή και με τη χρήση υπέρυθρων ακτινών και Bluetooth να τις μοιραστεί με άλλους. Επίσης, μέσω του δικτύου Wi-Fi μπορεί να αναρτήσει αυτές τις φωτογραφίες στο διαδίκτυο.

Υλικό όπως φωτογραφίες μαθητών και μαθητριών, ληφθείσες μέσω κινητού τηλεφώνου σε τουαλέτες σχολείων, γυμναστηρίων και άλλων χώρων συγκέντρωσης ανηλίκων, καθώς και μικρής διάρκειας βίντεο ληφθέντα από παιδόφιλους χρήστες κινητού, κατά τη διάρκεια ερωτικών δραστηριοτήτων μεταξύ ενηλίκων και παιδιών, αναρτώνται στο διαδίκτυο, εύκολα, γρήγορα και ανέξοδα.

Διακίνηση.

Η διακίνηση πορνογραφικού υλικού ανηλίκων αφορά στην ανάρτηση (uploading) και διανομή πορνογραφικών εικόνων και βίντεο. Η διακίνηση αυτή, πραγματοποιείται κυρίως από καλά οργανωμένες ομάδες παιδόφιλων ή ομάδες οργανωμένου εγκλήματος στα πλαίσια αναζήτησης κέρδους. Ωστόσο, πιο συχνά πραγματοποιείται όμως από απλούς χρήστες, οι οποίοι δεν στοχεύουν σε κάποιου είδους χρηματική αμοιβή. Οι αποτυπώσεις της παιδικής πορνογραφίας αναρτώνται και ανταλλάσσονται στο διαδίκτυο μέσα από ιστοσελίδες (websites), μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), με άμεσα ηλεκτρονικά μηνύματα (instant messages μέσω των υπηρεσιών messenger), μέσα από δωμάτια ανοιχτής επικοινωνίας (chat rooms) καθώς και σε ομάδες συζητήσεων (forum).

Ιστοσελίδες (sites).

Η χρήση ιστοσελίδων με παιδικό πορνογραφικό υλικό είναι ο πλέον διαδεδομένος και εύκολος τρόπος πρόσβασης και διακίνησής τέτοιου είδους υλικού. Με τη βοήθεια των «κυβερνοπυλών» (portals), όπως είναι π.χ. τα Yahoo και Google, μπορεί κάθε χρήστης, με την πληκτρολόγηση στο πεδίο αναζήτησης της σχετικής λέξης ή φράσης, να βρεθεί σε κάποιο site με πορνογραφικό υλικό που αφορά σε ανήλικους, εύκολα, γρήγορα και δωρεάν.

Βέβαια, εκτός των ιστοσελίδων που προσφέρουν τέτοιο υλικό χωρίς αμοιβή, υπάρχουν και διαδικτυακοί τόποι που με χρηματική συνδρομή προσφέρουν πρόσβαση σε πολύ περισσότερες και πιο εξεζητημένες φωτογραφίες ή βίντεο, διασφαλίζοντας έτσι καλύτερα την ανωνυμία και την προστασία των επισκεπτών τους. Τέλος, πολλά τέτοια sites όπως αναφέρθηκε παραπάνω, επιτρέπουν την πρόσβαση σε πορνογραφικό υλικό, μόνο στους χρήστες εκείνους, που με τη σειρά τους αναρτούν (κάνουν upload) στη συγκεκριμένη ιστοσελίδα νέες εικόνες με παιδική πορνογραφία. (ανταλλαγή υλικού)

Ηλεκτρονικό ταχυδρομείο (E-mail).

Τα ηλεκτρονικά μηνύματα (e-mails) είναι η παλαιότερη και πιο συχνά χρησιμοποιούμενη μέθοδος για την αποστολή και ανταλλαγή φακέλων και αρχείων ανεξαρτήτως μεγέθους και μορφής. Η μεγάλη χωρητικότητα και δυνατότητα αποθήκευσης που προσφέρουν οι ειδικοί φάκελοι εισερχομένων (inbox) των ηλεκτρονικών διευθύνσεων, καθώς και η δυνατότητα ταυτόχρονης αποστολής μηνυμάτων σε περισσότερους του ενός χρήστες, επιτρέπει στους παιδόφιλους τη

μεταφορά, ανταλλαγή αλλά και διατήρηση αρχείων με φωτογραφίες και βίντεο μεγάλου μήκους με υλικό παιδικής πορνογραφίας. Σε αρκετές περιπτώσεις για να μη γίνουν αντιληπτοί, οι χρήστες του διαδικτύου αποστέλλουν ηλεκτρονικά μηνύματα κρυπτογραφημένα. Στέλνουν, δηλαδή, δεδομένα που έχουν μετατραπεί με τη χρήση κωδικών κατά τέτοιο τρόπο, ώστε να μπορούν να διαβαστούν μόνο από συγκεκριμένους παραλήπτες με τη χρήση ενός «κρυφού κωδικού».

Άμεσα ηλεκτρονικά μηνύματα (instant messages).

Πρόκειται για προγράμματα, τα οποία επιτρέπουν σε δύο ή παραπάνω χρήστες να στέλνουν και να λαμβάνουν γραπτά μηνύματα σε πραγματικό χρόνο, να πραγματοποιούν συνομιλίες, συνοδευόμενες συχνά από τη χρήση ψηφιακής κάμερας και την ανταλλαγή φακέλων και αρχείων. Χαρακτηριστικά τέτοια προγράμματα είναι τα MSN Messenger- Outlook, Yahoo Messenger Skype κ.α. Τα προγράμματα αυτά χρησιμεύουν επιπλέον στην επικοινωνία μεταξύ παιδόφιλων, αλλά και μεταξύ παιδόφιλων με υποψήφια θύματα, καθώς και στην ανταλλαγή και γενικότερη διακίνηση εικόνων και βίντεο πορνογραφίας ανηλίκων.

Ομάδες συζήτησης (forum)

Πρόκειται για υπηρεσίες οι οποίες προσφέρουν τη δυνατότητα καταχώρησης και ανάγνωσης μηνυμάτων σε ανοιχτά forum στο διαδίκτυο, ταξινομημένων κατά θεματικές ενότητες. Κάθε χρήστης μπορεί να γίνει συνδρομητής σε όποια κατηγορία θεμάτων επιθυμεί, για να διαβάζει μηνύματα και να απαντά σ' αυτά. Την υπηρεσία αυτή χρησιμοποιούν συχνά οι δράστες της παιδικής πορνογραφίας για να επικοινωνήσουν μεταξύ τους, να ανταλλάξουν εμπειρίες, συμβουλές και φυσικά να διακινήσουν πορνογραφικό υλικό.

Κάθε άρθρο ή μήνυμα που καταχωρείται από κάποιον χρήστη προωθείται αυτόματα σε όλους τους υπόλοιπους χρήστες της ίδια ομάδας, ενώ το υλικό που έχει σταλεί διαγράφεται αυτόματα από κάθε υπολογιστή μετά την πάροδο κάποιων ημερών, εκτός αν γίνει ειδική ρύθμιση. Οι ομάδες συζήτησης με θέμα την παιδική πορνογραφία χρησιμοποιούν κυρίως παραπλανητικά θεματικά ονόματα για να μην γίνουν αντιληπτές οι δραστηριότητές τους.

Όλα αυτά τα groups μοιράζονται τα ίδια ενδιαφέροντα, στα πλαίσια των οποίων στέλλονται και διανέμονται πορνογραφικές εικόνες, καθώς και πληροφορίες για νέες ιστοσελίδες με σχετικό περιεχόμενο. Αν και η λειτουργία των ομάδων αυτών, διακόπτεται άμεσα, όταν αυτές γίνουν αντιληπτές από τους διανομείς (servers), σύντομα επαναλειτουργούν με νέο παραπλανητικό όνομα, που αποτελεί κάλυψη στις παράνομες δραστηριότητές τους.

Δωμάτια επικοινωνία (Chat Rooms).

Τα chat rooms δεν αποτελεί πλέον το πιο διαδεδομένο μέσο διαδικτυακής επικοινωνίας τόσο για τα παιδιά όσο και για τους ενήλικους. Ωστόσο, για όσους τα χρησιμοποιούν για γνωριμίες και επικοινωνία, επιτρέπουν τη ταυτόχρονη διαδικτυακή επαφή με περισσότερους και άγνωστους χρήστες σε πραγματικό χρόνο. Παράλληλα όμως χρησιμεύει και ως μέσο ανταλλαγής υλικού πορνογραφίας, κυρίως φωτογραφιών και μικρής διάρκειας βίντεο, συνομιλίας μεταξύ των συλλεκτών παιδικής πορνογραφίας, καθώς και ως τόπος γνωριμίας μεταξύ παιδιών και παιδόφιλων ή παραγωγών τέτοιου υλικού.

Τα chat rooms (όπως θα αναλυθεί και παρακάτω) φέρνουν σε επαφή ανθρώπους, οι οποίοι συνομιλούν μεταξύ τους, διακηρύσσουν τον τρόπο ζωής τους, στηρίζουν ο ένας τον άλλον ως προς τις επιλογές τους, ανταλλάσσουν πληροφορίες και συμβουλές για την κάλυψη των δραστηριοτήτων τους και διακινούν σε πραγματικό χρόνο και δωρεάν υλικό παιδικής πορνογραφίας.

Κατέβασμα (downloading) .

Οι εικόνες και τα βίντεο με παιδικό πορνογραφικό περιεχόμενο «κατεβάζονται» από το διαδίκτυο, και είτε αποθηκεύονται στον σκληρό δίσκο ή σε κάποιο αποσπώμενο τμήμα του

υπολογιστή μετά τη διαδικασία του downloading, είτε απλά προβάλλονται χωρίς στη συνέχεια να αποθηκευτούν.

Σε κάποιες περιπτώσεις κάποιος χρήστης του internet μπορεί να παρακολουθήσει, να λάβει, ακόμα και να κατεβάσει άθελά του στον υπολογιστή του εικόνες ή βίντεο παιδικής πορνογραφίας, μέσω ανεπιθύμητων διαφημιστικών μηνυμάτων (spam advertising) στα e-mails του , με τη μορφή αναδυόμενης σύνδεσης σε κάποια άλλη εντελώς άσχετη με την πορνογραφία ιστοσελίδα (pop-up link), ή τέλος με την ακούσια παραπομπή του χρήστη σε ιστοσελίδα με πορνογραφικό υλικό, μέσω μίας λέξης- κλειδιού στη μηχανή αναζήτησης όπως η Google, λέξη, η οποία βέβαια, καμία σχέση δεν έχει με την πορνογραφία.

Τις περισσότερες φορές όμως, η προβολή και το κατέβασμα του πορνογραφικού υλικού ανηλίκων γίνεται σκόπιμα, από χρήστες οι οποίοι αναζητούν τέτοιο υλικό στις σχετικές ιστοσελίδες στο διαδίκτυο, πληρώνοντας την ανάλογη συνδρομή ή συμμετέχοντας σε ομάδες διακίνησης υλικού. Όπως αναφέρθηκε παραπάνω, εικόνες παιδικής πορνογραφίας σπάνια απαντώνται σε εύκολα και ανοιχτά προσβάσιμες περιοχές του διαδικτύου, ενώ αντίθετα αυτοί που επιθυμούν να βρουν και να κατεβάσουν τέτοιες εικόνες, γνωρίζουν με ποιον τρόπο να τις αναζητήσουν. Το μεγαλύτερο ποσοστό της παιδικής πορνογραφίας κατεβαίνει μέσα από ομάδες συζήτησης και δωμάτια ανοιχτής επικοινωνίας, με δεδομένη μάλιστα την δωρεάν τους διάθεση, αφού το downloading αυτού του υλικού από τις ιστοσελίδες τις περισσότερες φορές απαιτεί την καταβολή χρηματικής αμοιβής ή τη χρήση ειδικού κωδικού.

GROOMING

Στα πλαίσια των συζητήσεων μέσα στα chat rooms που αναφέρθηκαν παραπάνω, θα γίνει μια αναφορά στον όρο Grooming. Το grooming είναι η διαδικασία κατά την οποία, παιδόφιλοι χρήστες, χρησιμοποιούν τα chat rooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Στην πλειονότητα των περιπτώσεων οι παιδόφιλοι υιοθετούν μια διαφορετική πλασματική ταυτότητα, όπως για παράδειγμα αποτελεί συχνό φαινόμενο να προσποιούνται ότι είναι έφηβοι. Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση ο καθένας από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά και τους εφήβους ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, εξαιτίας του δημόσιου χαρακτήρα της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα παιδιά με σκοπό να αναπτύξουν αρχικά φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα τους και τις σεξουαλικές τους εμπειρίες. Αφού αναπτυχθεί η σχέση αυτή προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να κάνουν τα παιδιά να νιώσουν ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η μέθοδος αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή και επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς ή τον δάσκαλό του, αφού στο τέλος νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους υλικό.

Προφίλ των δραστών.

Δράστης συλλογής, παραγωγής και διακίνησης παιδικού πορνογραφικού υλικού μπορεί να είναι οποιοσδήποτε, καθώς το διαδίκτυο προσφέρει ανωνυμία, ταχύτητα και ευκολία για την ανάπτυξη τέτοιων δραστηριοτήτων. Είναι χαρακτηριστικό το αποτέλεσμα έρευνας που αναφέρει ότι η πλειονότητα όσων ανταλλάσουν ή διανέμουν υλικό παιδικής πορνογραφίας online δεν θα το έκαναν ποτέ offline.

Γενικά, είναι ξεκάθαρο πως όσοι εμπλέκονται σε αδικήματα σχετικά με την παιδική πορνογραφία στο διαδίκτυο, δεν είναι απαραίτητα και δράστες σεξουαλικών εγκλημάτων στην πραγματική ζωή. Πριν την εξάπλωση του διαδικτύου, είχε διαπιστωθεί ότι το ένα τρίτο με ένα πέμπτο όσων συλλαμβάνονταν για κατοχή παιδικού πορνογραφικού υλικού, είχαν ανάμειξη και σε πραγματικές κακοποιήσεις παιδιών. Το διαδίκτυο ωστόσο, διευκόλυνε την πρόσβαση σε υλικό πορνογραφίας από χρήστες, οι οποίοι ποτέ πριν δεν αναζήτησαν υλικό παιδικής πορνογραφίας σε βιντεοκασέτες ή περιοδικά. Όμως λόγω της ευκολίας και της ανωνυμίας του internet αναζητούν τέτοιου είδους εικόνες για την ικανοποίηση της περιέργειάς τους. Βέβαια, η επαφή με αυτό το υλικό ενδέχεται να καταλήξει σε συχνότερη χρήση ή ακόμα και σε εθισμό των χρηστών σε τέτοιες εικόνες. Πρέπει εδώ να αναφερθεί ότι όσοι έχουν καταδικαστεί για σεξουαλικά αδικήματα σε βάρος ανηλίκων, δεν είναι αυτονόητο ότι δείχνουν ενδιαφέρον για την αναζήτηση εικόνων παιδικής πορνογραφίας, καθώς σύμφωνα με έρευνα, το ποσοστό των δραστών σεξουαλικών αδικημάτων, με ενδιαφέρον στην παιδική πορνογραφία, κυμαίνεται μεταξύ του 10 και 24% του συνολικού αριθμού των καταδικασθέντων.

Οι εμπλεκόμενοι στην παραγωγή, κατοχή και διακίνηση παιδικής πορνογραφίας μπορεί να προέρχονται από οποιοδήποτε τμήμα του κοινωνικού συνόλου. Σύμφωνα με έρευνες, είναι πιθανότερο να έχουν μία σταθερή ερωτική σχέση, μόνιμη εργασία, υψηλότερο από τον μέσο όρο δείκτη ευφυΐας, να έχουν πανεπιστημιακή μόρφωση και να μην έχουν βεβαρυμμένο ποινικό μητρώο. Ανάμεσα σε όσους έχουν συλληφθεί για τα σχετικά αδικήματα μέχρι τώρα, τόσο στην Ελλάδα αλλά και διεθνώς, ευρίσκονται και δικαστές, δικηγόροι, καθηγητές, δάσκαλοι, διασημότητες κ.α. Από τα ελάχιστα κοινά τους χαρακτηριστικά, είναι ότι στην πλειονότητα τους, πρόκειται για λευκούς άνδρες, μεταξύ 26 και 40 ετών, συνήθεις χρήστες του διαδικτύου, γεγονός μάλιστα, το οποίο συχνά επηρεάζει την κοινωνική τους ζωή και τις διαπροσωπικές τους επαφές.

Η ηλικία των εμπλεκομένων διεθνώς για σχετικά με την παιδική πορνογραφία αδικήματα στο διαδίκτυο ποικίλει από 10 έως 65 ετών. Σύμφωνα με σχετική έρευνα γνωστού Πανεπιστημίου, ποσοστό 3% των συλληφθέντων για τις παραπάνω πράξεις είναι ηλικίας κάτω των 17 ετών, το 11% είναι ηλικίας 18 έως 25 ετών, το 45% ανήκει στην ηλικιακή ομάδα των 26 έως 39 και το 41% είναι 40 ετών και άνω. Σύμφωνα με την ίδια έρευνα, το 99% των κατηγορουμένων είναι άνδρες, στην συντριπτική τους πλειονότητα λευκοί, οι οποίοι δρουν μόνοι τους, ανήκουν στη μέση ή ανώτερη οικονομική τάξη, ενώ στις περισσότερες περιπτώσεις είναι άτομα που χαρακτηρίζονται ως «υπεράνω υποψίας», συχνά δε θεωρούντο πρότυπα για το κοινωνικό σύνολο στο οποίο διαβιούσαν.

Από το σύνολο των συλληφθέντων, το 67% απλά κατείχε σε ψηφιακή μορφή το υλικό, ενώ το 22% το διένειμε στο internet, ενώ ένας στους δέκα κατηγορουμένους για αδικήματα σχετικά με την παιδική πορνογραφία έχει συλληφθεί και παλαιότερα για κάποιο αδίκημα σεξουαλικής φύσεως εναντίον ανηλίκου. Από τους εμπλεκομένους στις παραπάνω πράξεις το 91% χρησιμοποιούσε οικιακό ηλεκτρονικό υπολογιστή, το 7% είχε πρόσβαση στο πορνογραφικό υλικό από Η/Υ ευρισκόμενο στον χώρο της εργασίας τους, ενώ το 2% χρησιμοποιούσε υπολογιστή ευρισκόμενο σε άλλο μέρος, συνήθως δημόσια βιβλιοθήκη.

Προφίλ θυμάτων.

Δεν υπάρχει μία συγκεκριμένη κατηγορία παιδιών, τα οποία αποτελούν αποκλειστικά τα θύματα εκμετάλλευσης στο διαδίκτυο και απεικονίζονται σε πορνογραφικές αποτυπώσεις. Οποιοσδήποτε ανήλικος ενδέχεται να θυματοποιηθεί, αφού σε αυτό συμβάλλουν τα ιδιαίτερα χαρακτηριστικά της νεαρής ηλικίας: η αφέλεια, η εμπιστοσύνη, η περιέργεια, η ανάγκη για προσοχή και στοργή και η επιθυμία για περιπέτεια. Όπως οι δράστες, έτσι και τα θύματα προέρχονται από οποιοδήποτε οικογενειακό ή κοινωνικό περιβάλλον και το μόνο κοινό χαρακτηριστικό τους είναι η χρήση του διαδικτύου. Υπάρχουν ωστόσο, μερικά συγκεκριμένα ατομικά χαρακτηριστικά, τα οποία μπορούν να μετατρέψουν κάποιους ανήλικους σε ευκολότερο στόχο για τους δράστες σχετικών με την online παιδική πορνογραφία εγκλημάτων.

Οι δράστες σεξουαλικών εγκλημάτων εναντίον παιδιών συνηθίζουν να στοχεύουν περισσότερο σε ανηλίκους που βρίσκονται υπό την επίβλεψη και κηδεμονία του κράτους, οι οποίοι συνήθως έχουν στερηθεί την γονική φροντίδα κι αγάπη, σε παιδιά μονογονεϊκών οικογενειών, τα οποία ο γονέας είναι δύσκολο να εποπτεύσει, σε ανήλικους που έχουν στο παρελθόν κακοποιηθεί

σωματικά, ψυχολογικά ή σεξουαλικά, σε συναισθηματικά ανώριμους ή μπερδεμένους ως προς την σεξουαλική τους ταυτότητα, σε παιδιά με μαθησιακές δυσκολίες, ή σε ανηλίκους, οι οποίοι δυσκολεύονται να αναπτύξουν φιλίες και διαπροσωπικές σχέσεις με συνομήλικούς τους.

Εξίσου εύκολους στόχους αποτελούν για τους αυτουργούς τέτοιων εγκλημάτων, παιδιά με χαμηλή αυτοπεποίθηση, παιδιά διακατεχόμενα από ισχυρό αίσθημα σεβασμού και υπακοής απέναντι στους ενηλίκους ή αντίθετα ανήλικοι οι οποίοι θέλουν να επαναστατήσουν ενάντια στη γονική επίβλεψη και τέλος παιδιά τα οποία είναι πρόθυμα να συνεργαστούν με τους δράστες έναντι υλικών ανταλλαγμάτων, όπως χρήματα ή ηλεκτρονικά παιχνίδια.

Αντιμετώπιση

Τα παιδιά χειρίζονται πλέον με μεγαλύτερη ευκολία από τους γονείς τούς τους ηλεκτρονικούς υπολογιστές, λόγω της καθημερινής και πολύωρης τριβής με αυτούς στο σχολείο και στο σπίτι. Κατά την πλοήγησή τους στον παγκόσμιο ιστό είναι πιθανό να συναντήσουν ενημερωτικές σελίδες και υλικό, ενώ παράλληλα υπάρχει περίπτωση να γνωρίσουν και να συνομιλήσουν με άγνωστα άτομα, κυρίως μέσα από ανοιχτές συζητήσεις στο διαδίκτυο. Προς αποφυγή των κινδύνων, οι οποίοι ελλοχεύουν στο διαδίκτυο, τα ίδια τα παιδιά οφείλουν να γνωρίζουν και να ακολουθούν κάποιους κανόνες κατά την πλοήγηση τους στον κυβερνοχώρο.

Επιβάλλεται, αρχικά, να μάθουν να μη απαντούν ποτέ σε πρόστυχα ή δελεαστικά online μηνύματα και να μιλούν πάντα στους γονείς τους ή σε κάποιον ενήλικο για εικόνες ή κείμενα που βρήκαν στο Διαδίκτυο και ενδέχεται να τους προκάλεσαν αισθήματα ανασφάλειας, ντροπής ή φόβου, ενώ παράλληλα θα πρέπει να τους γίνει συνείδηση ότι δε φέρουν καμία ευθύνη για όλα αυτά κι επομένως δεν πρέπει να αισθάνονται ενοχές όταν λαμβάνουν προσβλητικά μηνύματα ή μηνύματα που δεν κατανοούν ή ακόμη και απρεπείς εικόνες, οι οποίες τους είναι δυσάρεστες ή τους προκαλούν ταραχή. Θα πρέπει, επομένως, να γνωρίζουν ότι επιβάλλεται να ενημερώνουν γι' αυτές τις εικόνες ή τα μηνύματα τους γονείς τους ή τον παροχέα υπηρεσιών δικτύου.

Οφείλουν να προσέχουν όταν μιλούν στο διαδίκτυο και να διακόψουν τη συνομιλία όταν κάποιοι τα κάνουν να νιώσουν άβολα. Σε κάθε περίπτωση θα πρέπει να διαφυλάσσουν τις προσωπικές τους πληροφορίες και ποτέ να μην δίνουν το όνομα και την διεύθυνσή τους ή το όνομα και την διεύθυνση του σχολείου τους, το τηλέφωνο τους και προσωπικές φωτογραφίες τους σε αγνώστους που συναντούν σε διάφορες συνομιλίες στο διαδίκτυο ακόμη και αν τους ζητηθεί.

Προφανώς, κι αυτό ίσως είναι το σημαντικότερο, δεν πρέπει να συναντούν κάποιον που γνώρισαν για πρώτη φορά στο διαδίκτυο, χωρίς να το αναφέρουν πρώτα στους γονείς τους προκειμένου να λάβουν την έγκρισή τους και χωρίς να συνοδεύονται από κάποιον από αυτούς.

Οι ιστοσελίδες και οι ανοικτές γραμμές καταγγελίας είναι διαδικτυακοί τόποι και τηλεφωνικές γραμμές αντίστοιχα, οι οποίες λειτουργούν συνήθως σε συνεργασία με τους παροχείς υπηρεσιών internet και δίνουν στους χρήστες του διαδικτύου, τη δυνατότητα να αναφέρουν ύποπτες εικόνες που εντοπίζουν στο internet. Οι αναφορές αυτές καταγράφονται σε μία βάση δεδομένων, από την οποία προωθούνται στη συνέχεια στις αρμόδιες υπηρεσίες καταστολής ή σε ανοικτές γραμμές άλλων χωρών για τον απαραίτητο έλεγχο.

Η πρώτη γραμμή καταγγελίας για ιστοσελίδες παιδικής πορνογραφίας στο διαδίκτυο και online σεξουαλικής εκμετάλλευσης ανηλίκων εν γένει, ξεκίνησε να λειτουργεί τον Ιανουάριο του 1997 στη Νορβηγία και μέσα στα δύο πρώτα χρόνια λειτουργίας της έλαβε πάνω από 6.000 καταγγελίες.

Ανοικτές γραμμές διαδικτυακής καταγγελίας λειτουργούν σήμερα, σε πολλές Ευρωπαϊκές χώρες, αλλά και σε χώρες εκτός Ε.Ε., όπως η Αυστραλία, ο Καναδάς, η Ιαπωνία, οι Η.Π.Α. κ.α, η δράση των περισσοτέρων από τις οποίες συντονίζεται από τον Παγκόσμιο Σύνδεσμο Ανοικτών Γραμμών Internet, «INHOPE». Ορισμένες από τις πιο γνωστές ιστοσελίδες που ασχολούνται με την προστασία των παιδιών στο διαδίκτυο, πολλές από τις οποίες λειτουργούν και ως δίκτυα καταγγελίας, είναι: Childnet International, CyberAngels Internet Safety Organization, Enough is Enough, Family

Στην Ελλάδα η πιο γνωστή ιστοσελίδα και ανοικτή γραμμή καταγγελιών για διαδικτυακούς τόπους και ομάδων συζητήσεων, που περιέχουν εικόνες παιδικής πορνογραφίας σε οποιοδήποτε σημείο του κόσμου και γενικά παράνομο υλικό, είναι η «SafeLine» που λειτουργεί από τον Απρίλιο του 2003.

Πρωταρχικός της στόχος είναι η εξάλειψη από το διαδίκτυο οποιοδήποτε υλικού παιδικής πορνογραφίας. Καταγγελίες μπορούν να υποβληθούν μέσω διαδικτύου, στη διεύθυνση

www.safeline.gr, με e-mail, τηλεφωνικά ή ταχυδρομικά, ενώ ο καταγγέλλων αν το επιθυμεί μπορεί να αποκρύψει τα προσωπικά του στοιχεία, ή διαφορετικά να επιλέξει να τα αναφέρει προκειμένου να ενημερωθεί για την εξέλιξη της καταγγελίας του.

Η ιστοσελίδα SafeLine μετά την λήψη της καταγγελίας, προχωρά σε τυπική επαλήθευση της, επιβεβαιώνει δηλαδή ότι το περιεχόμενο της καταγγελίας όντως υπάρχει και μπορεί ενδεχομένως να χαρακτηριστεί παράνομο και στη συνέχεια εντοπίζει τη χώρα προέλευσης του διαδικτυακού τόπου με τη χρήση τεχνικών μέσων. Αν το περιεχόμενο προέρχεται από την Ελλάδα, ενημερώνει την ελληνική αστυνομία, διαφορετικά ενημερώνει την αντίστοιχη ανοικτή γραμμή της χώρας προέλευσης. Στην περίπτωση που τέτοια γραμμή δεν υπάρχει, ενημερώνεται η ελληνική αστυνομία, προκειμένου αυτή να ενημερώσει την Interpol.

4.4 ΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η κλοπή ταυτότητας (Identity Theft) είναι ένα από τα πλέον σοβαρά εγκλήματα του Διαδικτύου. Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς (π .χ. εμπορικούς, ιατρικούς, διαφημιστικούς). Είναι εύκολο για τον καθέναν, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών.

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δυο στάδια: Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς. Για παράδειγμα, αφαιρούν πορτοφόλια από τσάντες στα μέσα μαζικής μεταφοράς, αυτοκίνητα ή ακόμη και από την τσέπη ανυποψίαστων περαστικών. Υποκλέπτουν την αλληλογραφία, παραβιάζουν μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλουν ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών και άλλα. Επίσης, αποσπούν τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενοι τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου. Εισβάλλουν στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα. Τέλος, χρησιμοποιούν ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων στο διαδίκτυο.

Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων. Αυτή μπορεί να πραγματοποιηθεί με διάφορους τρόπους, όπως ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, οι οποίοι χρησιμοποιούνται για την αγορά αγαθών μέσω του διαδικτύου και ανοίγοντας τραπεζικούς λογαριασμούς, οι οποίοι χρεώνονται με ακάλυπτες επιταγές. Άλλοι τρόποι είναι η δημιουργία πλαστών πιστωτικών καρτών, αδειών οδήγησης, διαβατηρίων και ταυτοτήτων, χρησιμοποιώντας τα στοιχεία του θύματος και η υποβολή ψευδών φορολογικών δηλώσεων μέσω Διαδικτύου, για την είσπραξη της επιστροφής.

Πειρατεία ονομάτων διαδικτυακού χώρου

Για την πραγματοποίηση οποιασδήποτε συναλλαγής στο διαδίκτυο, κύρια προϋπόθεση αποτελεί η δημιουργία ενός διαδικτυακού χώρου, όπου θα είναι δυνατή η πρόσβαση πελατών και η πραγματοποίηση ηλεκτρονικού εμπορίου. Το μέσο για να εισαχθεί ο χρήστης στο διαδίκτυο αποτελεί το «domain name» (όνομα πεδίου ή όνομα χώρου), το οποίο στην ουσία έχει ρόλο ηλεκτρονικής

διευθύνσεως και επιτρέπει έτσι την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως.

Το «domain name» αποτελείται από σειρά μια χαρακτήρων, αριθμών αλλά και γραμμάτων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό. Επίσης, μπορεί να αποτελείται από μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία και διαιρείται σε τρία μέρη.

Το πρώτο από τα τρία μέρη είναι κοινό για όλα τα «domain names» και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο).

Το δεύτερο μέρος ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το υπάρχον όνομα και την υπάρχουσα διαδικτυακή διεύθυνση.

Το τρίτο μέρος δηλώνει το είδος της τοποθεσίας ή τη γεωγραφική προέλευση, όπως «.com» για όσους ασκούν εμπορικές συναλλαγές, «.edu» για εκπαιδευτικούς οργανισμούς, «.org» για οργανισμούς γενικά, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς και «.int» για διεθνείς οργανισμούς. Τέλος, υπάρχει και ένα σύνολο δύο ή παραπάνω γραμμάτων που αποτελούν τη χώρα αρχειακής καταχωρίσεως του «domain name», όπως για παράδειγμα το «.gr» για την Ελλάδα.

Το «domain name» δεν μπορεί να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο μια επιχείρησης καθώς και το εμπορικό σήμα της. Επιβάλλεται, ωστόσο, να αποδίδεται σ' αυτό λειτουργία, κατά έμμεσο τρόπο, όταν αυτό χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση που προσδιορίζει στο διαδίκτυο, διότι, έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία.

Η πειρατεία ονομάτων διαδικτυακού χώρου, εξαπλώθηκε ιδιαίτερα κατά τα πρώτα χρόνια του διαδικτύου. Γνώστες του αντικειμένου, εκμεταλλευόμενοι το γεγονός πως μεγάλες εταιρείες δεν είχαν κατοχυρώσει, ακόμη, ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διασήμων εταιρειών, με αποτέλεσμα να αποκτούν οι ίδιοι τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν να δράσουν με διαφορετικούς τρόπους. Έκαναν για παράδειγμα προσπάθειες να παραχωρήσουν την διεύθυνση στην εταιρεία που κατέχει το συγκεκριμένο όνομα, έναντι βέβαια σημαντικού χρηματικού ποσού. Ή ακόμη χειρότερα, υπάρχουν περιπτώσεις που οι δράστες επιχειρούν να προβούν στην ανάρτηση, στη συγκεκριμένη διεύθυνση, περιεχομένου προσβλητικού (π.χ. πορνογραφία), γεγονός που επιφέρει σημαντικές οικονομικές και όχι μόνο, συνέπειες στην εταιρεία.

Η ευκολία του να χρησιμοποιείται ελεύθερα μια ονομασία, όσο γνωστή και φημισμένη και αν είναι, από τον οποιοδήποτε, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση που καθιερώθηκε στις συναλλαγές με τη συγκεκριμένη ονομασία. Επομένως, για τη διαφύλαξη των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο «domain name», όπως αναφέρθηκε και παραπάνω, μια λειτουργία διακριτικού τίτλου και σήματος. Αυτό ενισχύεται και από το ότι οι κάτοχοι «domain names» στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους έκαναν γνωστούς στην αγορά, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, λαμβάνοντας βέβαια υπόψη τα περιορισμένα όρια παροχής «domain names» για κάθε επιχείρηση αλλά και την επιβαλλόμενη συντομία γι' αυτού του είδους την επικοινωνία.

Έννομη Προστασία:

Γνωρίζοντας, λοιπόν, όλα τα παραπάνω, μια επιχείρηση με ένα συγκεκριμένο «domain name» θα πρέπει να απολαμβάνει προστασίας αντίστοιχης με εκείνη των διακριτικών γνωρισμάτων (εφαρμοζομένων αναλόγως των σχετικών διατάξεων). Επίσης, ένα διακριτικό γνώρισμα θα πρέπει να προστατεύεται από τη χρήση ενός ονόματος διαδικτύου, παρά το γεγονός ότι προηγήθηκε χρονικά η καταχώριση αυτού στο διαδίκτυο. Κρίνεται απαραίτητο σε αυτό το σημείο, να ληφθούν υπόψη οι ιδιαιτερότητες του διαδικτύου, και συγκεκριμένα η παγκοσμιότητά του ως μέσο ενημέρωσης και επικοινωνίας, η μοναδικότητα των ηλεκτρονικών διευθύνσεων, οι λίγες επιλογές που υπάρχουν στον συνδυασμό διευθύνσεων και το ιδιαίτερο σύστημα καταχωρίσεως των ονομασιών, σύμφωνα με το οποίο η εξυπηρέτηση των αιτήσεων γίνεται με βάση την ημερομηνία άφιξής τους χωρίς διενέργεια

προληπτικού ελέγχου, αρκεί να μην έχει χορηγηθεί το συγκεκριμένο όνομα σε άλλον αιτούντα (First Come First Served).

Η καταχώριση γνωστού διακριτικού γνωρίσματος ως «domain name» ενδέχεται στην εμπορική αγορά να συνιστά και αθέμιτο παρεμποδιστικό ανταγωνισμό (άρθρο 1 Ν 146/1914), ενώ δεν αποκλείεται ότι μπορεί να συντρέχουν και οι προϋποθέσεις εφαρμογής του άρθρου 13 Ν 146/1914 , «όταν το διακριτικό γνώρισμα χρησιμοποιείται ήδη στο διαδίκτυο από άλλη εταιρεία.» Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι δημοσιεύθηκε η ΕφΠειρ 608/2009, που έκρινε μη νόμιμη την κατοχύρωση και χρήση του domain name "chattours.gr" από επιχείρηση που δραστηριοποιείται στον τομέα του τουρισμού, λόγω της προσβολής δικαιώματος της εταιρείας CHAT-TOURS ΕΠΕ, η οποία είχε ήδη προλάβει να κατοχυρώσει το domain name "chatours.gr" (με ένα 't'),και επιδίκασε συναφώς αποζημίωση.

Πειρατεία Λογισμικού

Το γεγονός ότι οι εφαρμογές του λογισμικού είναι σε ψηφιακή μορφή, καθιστά ιδιαίτερα εύκολη την αναπαραγωγή τους σε πολλά αντίγραφα. Πριν την έλευση του Διαδικτύου, το λογισμικό διακινούταν με φυσικό τρόπο (π. χ . με δισκέτες ή CD). Η άνθηση, όμως, του διαδικτύου και ιδιαίτερα των ευρυζωνικών συνδέσεων άνοιξε νέους δρόμους στην πειρατεία λογισμικού. Πλέον, η διακίνηση του λογισμικού μπορεί να γίνει μέσω διάφορων υπηρεσιών που υπάρχουν στο Διαδίκτυο, όπως ηλεκτρονικό ταχυδρομείο (e-mail), chat κ.α. και ιδιαίτερα με τις εφαρμογές ανταλλαγής αρχείων.

Πειρατεία Λογισμικού θεωρείται η χωρίς άδεια χρήση, η εγκατάσταση, αναπαραγωγή, αντιγραφή και διανομή ενός προγράμματος υπολογιστή. Η πειρατεία λογισμικού έχει πολύ μεγάλες αρνητικές συνέπειες στην εθνική οικονομία και την απασχόληση, ενώ θέτει τον χρήστη τέτοιου λογισμικού ενώπιον οικονομικών και ηθικών κινδύνων. Σημαντικοί είναι επίσης και οι κίνδυνοι ασφάλειας των ηλεκτρονικών συστημάτων του χρήστη. Οι πιθανές συνέπειες από τη χρήση μη αδειοδοτημένου λογισμικού περιλαμβάνουν ποινικές, αστικές και διοικητικές κυρώσεις. Επιπλέον, μειώνεται η φήμη και το κύρος της επιχείρησής που χρησιμοποιεί λογισμικό χωρίς άδεια και κατ' επέκταση ο προμηθευτής του παράνομου λογισμικού αδυνατεί να προβεί σε τεχνική υποστήριξη και δωρεάν αναβάθμισή του. Τέλος, είναι εξαιρετικά υψηλός ο κίνδυνος προσβολής του πληροφοριακού συστήματος από ιούς, κακόβουλο λογισμικό κ.α.

Οι εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα για να αποτρέψουν την αντιγραφή ή χρήση τους από άλλους υπολογιστές. Ωστόσο, οι hackers-crackers πάντα βρίσκουν τεχνικές για να παρακάμψουν τα μέτρα αυτά και να απενεργοποιούν τους κωδικούς, τα κλειδιά και ό,τι άλλο χρησιμοποιείται για την προστασία ενός προγράμματος. Ακόμα και αν κάποιος δεν έχει εξειδικευμένες γνώσεις για να «σπάσει» ένα πρόγραμμα, μπορεί να χρησιμοποιήσει έτοιμο λογισμικό «crack», που διατίθεται ελεύθερα στο Διαδίκτυο και μπορεί να απενεργοποιεί τα μέτρα προστασίας των εταιρειών παραγωγής λογισμικού. Σύμφωνα με τη γνωστή έρευνα Global Piracy Study 2010, της εταιρείας Business Software Alliance που παρουσιάστηκε τον Μάιο του 2011, το ποσοστό πειρατείας λογισμικού παγκοσμίως έφτασε το 42%. Χαρακτηριστική είναι η παρατήρηση ότι «για κάθε $100 γνήσιου λογισμικού που πωλήθηκε, ένα πρόσθετο ποσό αξίας $75 λογισμικού χωρίς άδεια, βγήκε στην αγορά.»

HACKING

Είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας αρχικά δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Η έννοια του hacking είναι πιο γενική. Μπορεί να περιλαμβάνει από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και εγκληματικές.

Το hacking εξελίχθηκε ιδιαίτερα και σαν όρος και σαν τεχνική-πρακτική κατά την περίοδο μετα τον Β παγκόσμιο πόλεμο. Στις μέρες μας, το νόημά του φτάνει σε τέτοιο βαθμό ώστε να συμπεριλαμβάνει εντελώς αντίθετες, συγκρουόμενες αντιλήψεις οι οποίες αναφέρονται σε πολύ διαφορετικές πραγματικότητες. Παρατηρείται ότι υπάρχει σύγκρουση ανάμεσα στον κοινωνικό και τον νομικό ορισμού του hacking. Για να καταφέρουμε να αναλύσουμε την κατάσταση και λαμβάνοντας υπόψη τα ιστορικά δεδομένα, ο κοινωνικός ορισμός είναι παλαιότερος από το νομικό ορισμό. Ο κοινωνικός ορισμός ταυτίζει το hacking με την ¨ιδέα¨, τον τρόπο σκέψης και ο νομικός ορισμός με την παραβατικότητα και την εγκληματικότητα.

Κατά τη δεκαετία του 1950 το hacking έγινε αντιληπτό ως τρόπος σκέψης. Οριοθετήθηκε ως νοοτροπία, που ασφαλώς πρέπει να έχει κάποιο όνομα από τους γνώστες-επιστήμονες ανάπτυξης της επιστήμης της πληροφορικής. Το hacking ταυτίστηκε με συγκεκριμένους ανθρώπους, όχι με συγκεκριμένες ιδέες αφού παρουσιάστηκε ως καινοτομία της εποχής. Η σύνδεση που γίνεται, πηγάζει στην άποψη ότι η καινοτομία αυτή δε μπορεί να είναι προϊόν μιας τυχαίας ανακάλυψης της στιγμής αλλά αντιθέτως, αποτελεί το αποτέλεσμα δράσεων και ενεργειών με νόημα, εξαρτημένη από το άτομο που παράγει τη δράση.

Εδώ δίδεται και ένας σύντομος και σύγχρονος ορισμός για το τι μπορεί να ορίσει ως παραγωγός της δράσης που αναφέραμε παραπάνω, hacker. Οι hackers είναι αυτοί που έχουν συνδεθεί με το έγκλημα και την παραβατικότητα στο διαδίκτυο, μάλιστα σε αρκετές περιπτώσεις δε γίνεται άστοχα. Ετυμολογικά, ούτε η κυριολεκτική έννοια της λέξης αλλά ούτε η μεταφορική, συνδέονται με παράνομες πράξεις. Η συγκεκριμένη λέξη έχει τις ρίζες της στην αγγλική λέξη hack που μεταφράζεται ως το κόψιμο και την επεξεργασία ξύλου. Έτσι λοιπόν, μπορεί να ορισθεί το άτομο αυτό το οποίο χωρίς να έχει κανένα δικαίωμα λαμβάνει πρωτοβουλία να αποκτήσει πρόσβαση σε αρχεία που υπάρχουν σε ηλεκτρονικό υπολογιστή ή σε κάποια περιφερειακή μνήμη υπολογιστή ή μεταφέρονται με κάποιο σύστημα τηλεπικοινωνιών

Ο hacker είναι άτομο πλήρως καταρτισμένο και εμφανίζει ιδιαίτερα μεγάλο ενδιαφέρον για το αντικείμενο που τον απασχολεί, όποιο και αν είναι αυτό. Επίσης, τον χαρακτηρίζει η έντονη διάθεση και πρόθεση μα βρει λύσεις τις οποίες θα μελετήσει και θα αναπτύξει ώστε να φτάσουν σε καλύτερη μορφή από τις υπάρχουσες και τις προβλεπόμενες συμβατικές. Η παραβίαση ενός δικτύου ηλεκτρονικών υπολογιστών, το λεγόμενο hacking, είναι το επικρατέστερο στοιχείο των περισσότερων διαδικτυακών εγκλημάτων. Ο χαρακτηρισμός που του αποδίδεται πλέον είναι: ¨ο εγκληματίας του 21 ου αιώνα¨.

Η είσοδος σε διαδικτυακούς τόπους που δεν επιτρέπεται ακόμα και αν δεν είναι με κακή πρόθεση, θα λέγαμε ότι εμφανίζει κακόβουλο χαρακτήρα. Αυτό επειδή αυτός που κάνει επίθεση, δηλαδή ο hacker, μπαίνοντας στο σύστημα μαθαίνει πράγματα για την ασφάλεια του, εντοπίζει οποίο αδύναμο σημείο του και έτσι μπορεί στη συνέχεια έχει φτιάξει τις προϋποθέσεις που θα του επιτρέψουν να διατελέσει, εάν το θέλει επίθεση ή ακόμα και να παραχωρήσει όποιο στοιχείο έχει σε κάποιον άλλο ώστε να μπορέσει να επιτεθεί εκείνος! Οι ενέργειες των hackers δεν κινούνται πάντα στη ζώνη της παραβατικότητας –εγκληματικότητας με την έννοια ότι θέλουν να καταστρέψουν και να βλάψουν. Είναι κι ένα κομμάτι της δράσης τους το οποίο ταυτίζεται με την ανάγκη επίδειξης, επιβεβαίωσης των δεξιοτήτων τους. Όπως γίνεται σε μια αληθινή μάχη, έτσι και στο διαδίκτυο το πιο βασικό προτού περάσει στην επίθεση ο ¨δράστης¨ είναι να συλλέξει πληροφορίες για τον ¨εχθρό¨. Αυτό είναι βασικό για να φτάσει και στο στόχο του αργότερα.

Υπάρχουν τρεις κατηγορίες hacker:

A) White hat - Hackers:

Στόχος τους είναι να καταπολεμούν το ηλεκτρονικό έγκλημα και τους black hat – hackers . Οι grey hats τους παραλληλίζουν με αυτούς που είναι ειδικοί για την ασφάλεια και διαχειρίζονται συστήματα. Το ηλικιακό διάστημα στο οποίο κινούνται είναι τα 25 με 40 έτη. Η εξέλιξη των grey hats είναι οι white hats.

Β) Black hat- Hackers:

Το ηλεκτρονικό έγκλημα είναι συνώνυμο του ονόματος τους. Εκμεταλλεύονται τις γνώσεις τους για να δράσουν ομαδικά δημιουργώντας προγράμματα που δεν είναι νόμιμα, όπως ηλεκτρονικούς ιούς προγράμματα κατασκοπείας. Εισχωρούν σε δίκτυα και τα παρακολουθούν με σκοπό να τα καταστρέψου, σπάνε κωδικούς, καταστρέφουν ιστοσελίδες. Αυτό που τους ωθεί σε τέτοιου είδους συμπεριφορές , αν όχι όλες , τις πιο πολλές φορές είναι το οικονομικό κίνητρο.

Γ) Grey hat-Hackers:

Εδώ βρισκόμαστε στην γκρίζα ζώνη του διαδικτύου. Στους grey hat-hackers συμπεριλαμβάνονται οι hackers που παραβαίνουν τον νόμο χωρίς φραγμούς αλλά παρόλα αυτά δεν υπάρχει κακόβουλη πρόθεση. Αντλούν τα κίνητρα τους από το ότι πειραματίζονται για να αποκτήσουν γνώση πάνω σε ότι έχει να κάνει με τα ηλεκτρονικά συστήματα.
Μπορούν να ανακαλύπτουν κενά ώστε να παραβιάζουν ξένα δίκτυα ή ηλεκτρονικά συστήματα για να αποδείξουν την ύπαρξη αδυναμιών. Η ηλικία αυτών των hackers δεν ξεπερνάει τα 18 έτη. Είναι επίσης άτομα τα οποία φτάνουν στο απόγειο των γνώσεων τους ως φοιτητές. Από αυτή την εισχώρησή τους σε ξένα δίκτυα δεν προκαλείται καταστροφή, το μόνο που συμβαίνει είναι η αποκάλυψη κενών και αδυναμιών γι αυτό, δεν θεωρείται από τους ίδιους ότι παραβαίνουν το νόμο και ότι ασκούν εγκληματικές πράξεις. Πιστεύουν ότι είναι ερευνητές της επιστήμης αυτής που σχετίζεται με το δίκτυο, τα συστήματα κτλ.

Η παραβίαση ενός δικτύου υπολογιστών από ένα hacker, αποβλέπει στο να μπορεί αυτός που επιτίθεται, ο hacker δηλαδή, να διαχειρίζεται το όλο σύστημα από απόσταση. Ανάλογα με την πρόσβαση, που έχει μετά την επίθεση ο hacker στον στόχο του, υπάρχουν οι δύο κυριότερες κατηγορίες.

α) η παραβίαση του συστήματος και στη συνέχεια η χρήση του ως διαχειριστής (πλήρη δικαιώματα στην πρόσβαση και στη διαχείριση) και

β) η απλή προσβασιμότητα και χρήση του συστήματος.

Η πρώτη είναι κι αυτή που είναι και η πιο επικίνδυνη, επειδή ο εισβολέας-hacker μπορεί να προκαλέσει σοβαρές αλλαγές στην όλη λειτουργία του συστήματος που προσβάλει, ως διαχειριστής του. Ενώ στην άλλη περίπτωση ο κίνδυνος σίγουρα είναι σοβαρός αλλά ταυτόχρονα και πιο μικρός.

Οι τρόποι, που χρησιμοποιούν οι hackers για να εισχωρούν στα δίκτυα ηλεκτρονικών υπολογιστών συμβαδίζουν με την ανάπτυξη της τεχνολογίας των συστημάτων ηλεκτρονικών υπολογιστών.
Οι πιο συχνοί τρόποι εισχώρησης είναι:

Η εκμετάλλευση των cookies:

Ο όρος cookie χρησιμοποιείται για να περιγράψει πολύ μικρά αρχεία κειμένου, των οποίων η χρησιμότητα βρίσκεται στο ότι προστίθενται στον ηλεκτρονικό υπολογιστή από τους διάφορους ιστοχώρους τους οποίους επισκέπτεται ο χρήστης του δικτύου και συμπεριλαμβάνουν πληροφορίες σχετικές με τα στοιχεία του χρήστη, κάθε δραστηριότητα του κ.α. Όταν λοιπόν, σ' ένα cookie περιέχονται πληροφορίες, π.χ. usernames και passwords για υπηρεσίες στις οποίες έχει πρόσβαση ο χρήστης, ο hacker μπορεί εύκολα να τις εντοπίσει αξιοποιώντας την όποια αδράνεια του φυλλομετρητή ή του Λειτουργικού Συστήματος.

Ανίχνευση δικτυακών υπηρεσιών των συστημάτων:

Από τις βασικότερες κινήσεις των hackers είναι το να εντοπίζουν πληροφορίες για το σύστημα στο οποίο θέλουν να κάνουν επίθεση. Για να καταφέρουν το στόχο τους μπαίνουν σε

διαδικασία να εφαρμόσουν τη λεγόμενη ως τεχνική σάρωσης θυρών. Αφορά μια διαδικασία κατά την οποία αποστέλλονται ερωτήματα σε οποιοδήποτε διακομιστή, με κύριο στόχο να λάβει ο επιτιθέμενος τις πληροφορίες που του είναι χρήσιμες για τις υπηρεσίες που προσφέρει, καθώς και για το επίπεδο ασφαλείας που υπάρχει. Η συλλογή αυτών των πληροφοριών έχει ιδιαίτερη σημασία, επειδή κάνει παιχνιδάκι για το hacker το να εισχωρήσει στο σύστημα παραβιάζοντας την ασφάλεια του.

Ανιχνευτές πακέτων δικτύου:

Η ανίχνευση πακέτων δικτύου, γίνεται με εφαρμογές για το λογισμικό, που έχουν προγραμματιστεί ώστε να βρίσκουν κάθε πακέτο, που κυκλοφορεί στο διαδίκτυο. Αν, το πακέτο δεν είναι κρυπτογραφημένο, τότε υπάρχει δυνατότητα, να αποσπαστούν πληροφορίες, όπως usernames, passwords, αριθμοί πιστωτικών καρτών και τα λοιπά.

Επιπρόσθετα, ο δράστης αποκτά πληροφορίες που έχουν σχέση με τη μορφή που συνδέονται οι κόμβοι ενός δικτύου, το που βρίσκεται, το πόσοι υπολογιστές βρίσκονται στο δίκτυο αλλά και τι υπηρεσίες παρέχονται. Υπάρχει δυνατότητα, μέσω των πακέτων που διακινούνται για την διεξαγωγή καθημερινών δραστηριοτήτων, να ληφθούν όλες οι απαιτούμενες πληροφορίες. Το να ανιχνευτούν τέτοιου είδους επιθέσεις είναι πάρα πολύ δύσκολο.

Πλαστές διευθύνσεις IP:

Σε επιθέσεις τύπου IP Spoofing, οι hackers επεμβαίνουν στις επικεφαλίδες των πακέτων που διακινούνται στο δίκτυο και τις αλλάζουν έτσι ώστε το μήνυμα να μοιάζει ότι έφτασε από πηγή την οποία εμπιστεύεται ο χρήστης. Με τον τρόπο αυτό, καταφέρουν να κάνουν χρήση μιας IP διεύθυνσης μέσα στο πλήθος των διευθύνσεων που είναι αξιόπιστες και να αποκτούν προσβασιμότητα σε υπηρεσίες του διαδικτύου, που αφορούν αξιόπιστους χρήστες του δικτύου. Η μέθοδος IP Spoofing εφαρμόζεται κυρίως συνδυαστικά με άλλες μεθόδους επίθεσης.

SPAMMING

Το spamming είναι η μαζική αποστολή πολλών μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται αρκετούς παραλήπτες του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον συγκεκριμένο αποστολέα. Ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου. Ωστόσο, χρησιμοποιείται επιπρόσθετα για να προσδιορίσει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως ενοχλητικό για τον παραλήπτη.

Η ανεπιθύμητη αυτή αλληλογραφία θα μπορούσε να χαρακτηριστεί ενοχλητική, καθώς ο χρήστης χωρίς την οποιαδήποτε έμπρακτη εκδήλωση ενδιαφέροντος, γίνεται παραλήπτης διαφημίσεων από διάφορες εταιρίες, οι οποίες γνωρίζουν με νόμιμο ή παράνομο τρόπο την ηλεκτρονική του διεύθυνση.

Τα πιο σημαντικά χαρακτηριστικά του spamming είναι ότι είναι:

• Απρόκλητο: Δεν υπάρχει η οποιαδήποτε σχέση μεταξύ αποδέκτη και αποστολέα, η οποία θα δικαιολογούσε τη συγκεκριμένη αλληλογραφία.

• Εμπορικό: Το spamming κυρίως αφορά την αλληλογραφία με εμπορικό σκοπό. Συνήθως, δηλαδή, στοχεύει στην προβολή και διαφήμιση προϊόντων και υπηρεσιών και επιπλέον, στη διεύρυνση πελατολογίου και πραγματοποίηση περισσότερων πωλήσεων.

• Μαζικό: Το spamming συνήθως αναφέρεται στη μαζική αποστολή μηνυμάτων από τον αποστολέα σε πολλούς παραλήπτες.

Ο χρήστης μπορεί να προστατευτεί από την ανεπιθύμητη αλληλογραφία, εγκαθιστώντας στον υπολογιστή του ενημερωμένα φίλτρα κατά των μηνυμάτων spam. Θα πρέπει, επίσης, να μη

γνωστοποιεί την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει, ούτε να την συμπληρώνει σε έτοιμες φόρμες στο διαδίκτυο, σε αμφίβολες σελίδες. Σε κάθε περίπτωση, όταν ο χρήστης λάβει τέτοιου είδους μηνύματα, θα πρέπει να τα διαγράψει άμεσα, χωρίς να τα ανοίξει, γιατί υπάρχει κίνδυνος μόλυνσης του υπολογιστή με κακόβουλο λογισμικό ή ορισμένες φορές, κίνδυνος απάτης.
Επομένως, για την προστασία του χρήστη από spam, θα πρέπει να:
-Μη δημοσιεύει την διεύθυνση ηλεκτρονικού ταχυδρομείου του σε σελίδες κοινωνικής δικτύωσης και αλλού. .
-Μη δίνει την διεύθυνση ηλεκτρονικού ταχυδρομείου του σε οργανισμούς που δεν είναι της εμπιστοσύνης του.
-Μην απαντάει στα μηνύματα spam, ούτε να προσπαθεί να τα διαβάσει.
-Αναφέρει κάθε μήνυμα spam που δέχεται στα εισερχόμενά του.
-Διαδώσει τη γνώση και την εμπειρία του σχετικά με τα μηνύματα spam και σε άλλους χρήστες. .

ΔΙΑΚΙΝΗΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Ιοί

Οι ιοί είναι ένα πρόγραμμα υπολογιστή που έχει δημιουργηθεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφα του εαυτού του που κατασκευάζει. Επιπλέον, επειδή μπορεί να δημιουργεί συνεχώς αντίγραφα του εαυτού του, μεταδίδεται από ένα σύστημα σε ένα άλλο, με σκοπό να κάνει αυτό για το οποίο δημιουργήθηκε. Η αποστολή του, λοιπόν, περιλαμβάνει την δυσλειτουργία ή ακόμα και την καταστροφή ολόκληρων συστημάτων, την διαγραφή συγκεκριμένων αρχείων ή όλου του συνόλου των σκληρών δίσκων ενός υπολογιστή. Ουσιαστικά, πρόκειται για έναν κακόβουλο εκτελέσιμο κώδικα, ο οποίος επιβιώνει με το να «κολλάει» σε ένα άλλο πρόγραμμα ή αρχείο ή να περιέχεται μέσα σε αυτό. Ο ιός δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα, γι' αυτό λέγεται ότι παρουσιάζει παρασιτική συμπεριφορά. Όπως και ένας κανονικός ιός, επιζεί με το να μολύνει άλλα αρχεία, αντιγράφοντας όσο πιο πιστά γίνεται τον τρόπο ζωής και πολλαπλασιασμού του. Ο πιο διαδεδομένος τρόπος μετάδοσης των ιών, σήμερα, είναι η διανομή τους μέσω των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.

Οι πιο συνηθισμένες κατηγορίες ιών που συναντά ο χρήστης κατά την πλοήγησή του στο διαδίκτυο είναι οι εξής:
1. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, που επηρεάζουν άμεσα την εκκίνηση του υπολογιστή.
2. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα.
3. Ιοί που προσβάλλουν προγράμματα υπολογιστή και κρύβονται μέσα σε εκτελέσιμα αρχεία. Αυτού του είδους οι ιοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει.
4. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την προστασία τους έναντι των διαφόρων προγραμμάτων καταπολέμησης ιών.
5. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος.
6. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus που χρησιμοποιεί ο χρήστης για την προστασία του.
7. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών.

Δούρειοι ίπποι (Trojan Horses).

Ο Δούρειος Ίππος είναι ένα είδος βλαβερού λογισμικού που προσβάλει έναν υπολογιστή και επιτρέπει στον χάκερ την πρόσβαση σε όλα του τα προγράμματα. Ένας δούρειος ίππος αποτελείται από δύο μέρη, το server και το client. Για να επιφέρει τη μόλυνση στον υπολογιστή, ένα πρόγραμμα δούρειου ίππου θα πρέπει κάπως να εγκατασταθεί και να εκτελεστεί σε αυτόν τον υπολογιστή το μέρος server. Έπειτα, αφού εκτελεστεί αυτό το μέρος του δούρειου ίππου στον υπολογιστή του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του είναι πλέον εύκολο πράγμα. Οι δούρειοι ίπποι μεταφέρονται στον ηλεκτρονικό υπολογιστή με συγκεκριμένα προγράμματα, τα οποία ονομάζονται droppers. Ο τρόπος που επικοινωνούν με τον client είναι μέσω διαφόρων θυρών του υπολογιστή, τις οποίες όμως μπορεί ο χρήστης να απενεργοποιήσει με τη χρήση κάποιου τοίχους προστασίας firewall.

Οι δούρειοι ίπποι έχουν ένα ιδιαίτερο χαρακτηριστικό. Ενώ είναι προγράμματα που φαίνονται να λειτουργούν κανονικά, παράλληλα εκτελούν και άλλες εργασίες, μη επιτρεπόμενες. Με αυτόν τον τρόπο, ένα τέτοιο λογισμικό μπορεί να έχει τη μορφή κάποιου παιχνιδιού, ωστόσο, στην πραγματικότητα, συλλέγει ονόματα και προσωπικούς κωδικούς των χρηστών που εκείνη τη στιγμή απολαμβάνουν το παιχνίδι τους. Πολλές φορές, ένα λογισμικό τέτοιου τύπου χρησιμοποιεί ένα μυστικό πέρασμα που έχει δημιουργήσει ο δράστης, για να συνδεθεί στον υπολογιστή του χρήστη. Αυτό το μυστικό σημείο εισόδου επιτρέπει στον επιτιθέμενο να αποκτήσει άμεση πρόσβαση στο σύστημα, προσπερνώντας πολλές φορές τις συνηθισμένες διαδικασίες ελέγχου που χρησιμοποιεί ένας υπολογιστής.

Σκουλήκια

Τα σκουλήκια είναι και αυτά προγράμματα που χρησιμοποιούνται για να μεταφέρουν άλλα προγράμματα στον υπολογιστή του χρήστη. Επομένως, γι' αυτόν τον λόγο αυτό, χρησιμοποιούν το διαδίκτυο και τις δυνατότητες που αυτό παρέχει, με σκοπό να μεταφέρουν κάποιο βλαβερό πρόγραμμα όπως για παράδειγμα έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Τα σκουλήκια διαφέρουν από τους ιούς στο γεγονός ότι δεν είναι απαραίτητη η ανθρώπινη παρεμβολή για να ενεργοποιηθούν, κάτι που συμβαίνει στην εξάπλωση των ιών.

Υπάρχουν βέβαια κι άλλα είδη κακόβουλου λογισμικού που χρησιμοποιούνται για τη μόλυνση του υπολογιστή. Παρακάτω αναφέρονται κάποια από αυτά.

Dialers

Οι dialers, παρότι δημιουργήθηκαν για τις συνδέσεις μέσω τηλεφώνου, είναι μια υποκατηγορία κακόβουλων προγραμμάτων που προσβάλουν άμεσα τον ηλεκτρονικό υπολογιστή. Αυτά τα προγράμματα είναι σχεδιασμένα να υποκλέπτουν σημαντικές πληροφορίες του χρήστη, όπως οι κωδικοί πρόσβασης, οι αριθμοί πιστωτικών καρτών και τα στοιχεία λογαριασμών του, χωρίς τη γνώση και έγκρισή του. Αυτού του είδους το λογισμικό δημιουργήθηκε με σκοπό το εύκολο και γρήγορο κέρδος.

Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου, ώστε να αναγκάσουν τον χρήστη να καλεί έναν συγκεκριμένο αριθμό, άγνωστο σε αυτόν. Αυτός ο αριθμός συνήθως είναι μια διεθνής κλήση με υψηλό για τον καλούντα κόστος. Έπειτα, γίνεται η διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και αντικαθίσταται με τον πάροχο του επιτιθέμενου. Έτσι, όταν ο χρήστης συνδέεται στο διαδίκτυο μέσω τηλεφωνικής πάντα σύνδεσης, χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου.

Λογική βόμβα.

Οι λογικές βόμβες είναι μικρά προγράμματα που εγκαθίστανται σε κάποιο ήδη υπάρχον πρόγραμμα ή αλλάζουν κάποιον υπάρχοντα κώδικα. Οφείλουν το όνομά τους στον τρόπο με τον

οποίο δρουν. Είναι δηλαδή σχεδιασμένες να «εκραγούν» ηλεκτρονικά, με ορισμένες προϋποθέσεις φυσικά. Κάποιος γνώστης του προγράμματος μπορεί να προσθέσει τη λογική βόμβα στο σύστημα και να την εγκαταστήσει. Το πιο σημαντικό είναι ότι ο κίνδυνος είναι μεγαλύτερος με τις λογικές βόμβες, απ' ότι με τους ιούς ή τα σκουλήκια. Αυτό στηρίζεται στο γεγονός ότι η κατασκευή τους είναι πολύ πιο εύκολη και η ζημιά που μπορεί να προκαλέσουν είναι αρκετά μεγαλύτερη. Για την ακρίβεια, έχουν τη δυνατότητα να καταστρέψουν ήδη αποθηκευμένα αρχεία, ακόμη και ολόκληρο το λογισμικό του υπολογιστή.

Rootkits.

Πρόκειται για ένα σύνολο εργαλείων και υπηρεσιών που ο επιτιθέμενος μπορεί να χρησιμοποιήσει για να διατηρήσει την πρόσβαση του στο σύστημα που έχει προσβάλει από τη στιγμή που θα εισβάλει σε αυτό. Τα εργαλεία αυτά θα επιτρέψουν στον χάκερ να συλλέξει τα ονόματα των χρηστών καθώς και τους κωδικούς πρόσβασής του. Επιπλέον, θα τον βοηθήσει να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να καλύψει τις ενέργειές του, αποκρύπτοντας αρχεία και διαγράφοντας κάθε δραστηριότητά του από το αρχείο καταγραφής. Μέσω αυτού του εργαλείου, ο χάκερ αποκτά πλήρη πρόσβαση στο σύστημα, κάτι που του επιτρέπει να το διαχειρίζεται όπως αυτός επιθυμεί. Μπορέι για παράδειγμα, να ελέγξει την πληκτρολόγηση, μπορεί να κάνει επιθέσεις σε άλλους υπολογιστές που είναι συνδεμένοι στο δίκτυο καθώς και να δημιουργεί μυστικά σημεία εισόδου για τη διευκόλυνση άλλων εισβολέων.

Ransomware.

Το Ransomware είναι ένα λογισμικό το οποίο μπορεί από οποιαδήποτε απόσταση να αποκρυπτογραφήσει τα δεδομένα των χρηστών. Το κακόβουλο αυτό λογισμικό προχωράει στην αποκρυπτογράφηση, αφού πρώτα, λάβει τα λύτρα που έχει απαιτήσει.

Bots – zombies.

Πρόκειται για ένα κακόβουλο λογισμικό που επιτρέπει σε όποιον κάνει επίθεση να έχει πλήρη έλεγχο στον ηλεκτρονικό υπολογιστή που έχει πληγεί. Οι ηλεκτρονικοί υπολογιστές που έχουν πληγεί από τα bot αποκαλούνται στον κόσμο της τεχνολογίας, «ζόμπι». Στην πραγματικότητα, υπάρχουν πάρα πολλοί υπολογιστές στο δίκτυο που έχουν πληγεί από αυτό το λογισμικό, αλλά δεν το γνωρίζουν ακόμα. Πολλές φορές, ο χρήστης δεν ξέρει ότι έχει κολλήσει ιό ή ότι έχει εγκαταστήσει έναν δούρειο ίππο πράγμα. Αυτό, βέβαια, σημαίνει ότι ο ηλεκτρονικός υπολογιστής μπαίνει στη διαδικασία να δουλέψει όπως λειτουργεί ένα ζόμπι. Αυτός που εισβάλει μπορεί να επιτίθεται με το μολυσμένο ηλεκτρονικό υπολογιστή ή μπορεί να στείλει μηνύματα spam σε διαφορετικούς υπολογιστές χωρίς να το γνωρίζουν οι κάτοχοι τους.

Scareware.

Το scareware ή fraudware είναι πρόγραμμα που έχει ως στόχο την εξαπάτηση των χρηστών. Τις πιο πολλές φορές εμφανίζεται με τη μορφή παραθύρου τρομοκρατώντας όσους χρήστες το συναντήσουν. Στη συνέχεια, τους καθησυχάζει ότι το πρόβλημα που έχει προκληθεί στον ηλεκτρονικό τους υπολογιστή θα λυθεί αφού αγοράσουν και εγκαταστήσουν ένα συγκεκριμένο λογισμικό, που τους προτείνει και που θα τους προστατεύει από επιθέσεις κάθε τύπου.

Βακτήρια

Τα βακτήρια είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να «τρέχει» ταυτόχρονα δύο αντίγραφά του σε ένα σύστημα. Ενδέχεται επίσης, να δημιουργεί δύο νέα αρχεία, τα οποία είναι αντίγραφα του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να δημιουργήσουν δύο αντίγραφα του εαυτού τους και ούτω καθεξής. Με αυτόν τον τρόπο τα βακτήρια αναπαράγονται καταλαμβάνοντας τελικά όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του σκληρού δίσκου του υπολογιστή, στερώντας τους πόρους αυτούς από τον χρήστη.

4.5 ΜΕΘΟΔΟΙ ΑΠΑΤΗΣ ΣΤΑ ATM

Οι μηχανές ATM ενεργοποιούνται με μια μαγνητική λωρίδα που βρίσκεται πάνω στην κάρτα μετρητών του πελάτη και την πληκτρολόγηση του προσωπικού του κωδικού αριθμού PIN. Οι μηχανές ATM επιτρέπουν να γίνουν οι παρακάτω συναλλαγές :

• Αναλήψεις και καταθέσεις χρημάτων

• Μεταφορά χρηματικών ποσών από ένα λογαριασμό σε άλλο

• Ενημέρωση υπολοίπου λογαριασμού

• Ανάληψη χρημάτων με πιστωτικές κάρτες

• Πληρωμές λογαριασμών πιστωτικών καρτών

• Πληρωμές καταναλωτικών δανείων

• Πληρωμές λογαριασμών ΔΕΚΟ .

Η παράνομη ανάληψη χρημάτων από ATM δεν επιβαρύνει την τράπεζα αλλά το λογαριασμό κάποιου τυχαίου πελάτη της. Η εκτεταμένη εφαρμογή των μεθόδων αυτών εμφανίστηκε στην Ευρώπη στα μέσα της δεκαετίας του '80. Χαρακτηριστικό παράδειγμα αποτελεί ένα πρωτότυπο «πείραμα» από τον Sieber: Το Σεπτέμβριο του 1985, δυο δημοσιογράφοι της τηλεόρασης από το Αμβούργο κατάφεραν να χρησιμοποιήσουν τις μαγνητικές τους κάρτες με σκοπό τη δημιουργία υπερβάσεων σε τραπεζικούς λογαριασμούς τρίτων. Η εν λόγω διαδικασία έλαβε χώρα μέσω της χρήσης μιας συσκευής ανάγνωσης και αναγνώρισης μαγνητικών καρτών , ενός προσωπικού υπολογιστή και ενός προγράμματος που είχαν δημιουργήσει οι ίδιοι. Μαγνητοσκόπησαν αυτήν την πράξη τους και στις 27 Οκτωβρίου του 1985 πρόβαλαν το φιλμ στην δυτικογερμανική τηλεόραση.

Η παραπάνω υπόθεση ενέπνευσε δυο άνεργα άτομα από την Κολονία να αναπτύξουν την ακόλουθη τεχνική: Εισήγαγαν ένα κενό αντίγραφο μαγνητικής κάρτας μέσα σε ένα μηχάνημα ATM και, κατόπιν, προσάρμοσαν στη συσκευή ανάγνωσης και αναγνώρισης έναν ειδικό βοηθητικό μηχανισμό. Όταν κάποιος πελάτης εισήγαγε την κάρτα του μέσα στον βοηθητικό μηχανισμό, το

αρχικό κενό αντίγραφο έμπαινε στη συσκευή ανάγνωσης και αναγνώρισης της τράπεζας. Από τη στιγμή που ο προσωπικός κωδικός αριθμός του πελάτη δεν ταίριαζε με αυτόν της ειδικά προετοιμασμένης κενής κάρτας, το μηχάνημα «παρακρατούσε» την τελευταία και απέρριπτε μόνιμα την κάρτα του πελάτη, ο οποίος έφευγε απογοητευμένος. Οι δράστες έβγαζαν την κάρτα του πελάτη από τον βοηθητικό μηχανισμό και προσπαθούσαν να εντοπίσουν τον κωδικό της αναλύοντας τα κουμπιά του πληκτρολογίου, τα οποία είχαν προηγουμένως ευαισθητοποιηθεί με μικρές σταγόνες πετρελαίου. Όταν ανακάλυπταν τους τέσσερις κωδικούς αριθμούς, προσπαθούσαν να εξακριβώσουν τη σωστή τους σειρά μέσα από τον έλεγχο 24 συνδυασμών: Η αυτοάμυνα του μηχανήματος - που θα έπρεπε να δεσμεύσει την κάρτα μετά από τρεις λαθεμένες εισαγωγές - παρακαμπτόταν με την αντιγραφή της κάρτας και την αλλαγή του αυτόματου μετά από δυο λαθεμένες εισαγωγές, ή με τον επιδέξιο χειρισμό του μετρητή ασφαλείας της κάρτας, ο οποίος κατέγραφε τον αριθμό λαθεμένων εισαγωγών. Οι δράστες καταχράστηκαν ποσό της τάξης των 80 χιλιάδων γερμανικών μάρκων. Πιάστηκαν στις 16 Ιανουαρίου του 1986, μετά από συστηματική παρακολούθηση και καταγραφή τους με κρυμμένες βιντεοκάμερες.

4.6. ΕΠΙΘΕΣΗ ΣΤΑ SOCIAL MEDIA

Τα social media, ή αλλιώς τα κοινωνικά δίκτυα είναι υπηρεσίες επικοινωνίας των χρηστών, καθώς και γνωριμίας με νέα άτομα, μέσω λογαριασμών. Τα τελευταία χρόνια, παρατηρείται ανάπτυξη των κοινωνικών δικτύων, τα οποία μετρούν εκατομμύρια χρήστες ανά τον κόσμο. Τέτοια είναι το facebook, το twitter και άλλα. Ωστόσο, η ανάπτυξη αυτή έχει οδηγήσει στην αύξηση του ηλεκτρονικού εγκλήματος, το οποίο στοχεύει στα κοινωνικά αυτά δίκτυα. Σύμφωνα με το Κέντρο Διαδικτυακών Παραπόνων των ΗΠΑ, από το 2006, περίπου 3.200 λογαριασμοί χρηστών έχουν δεχτεί επίθεση σε διάφορες μορφές. Η επίθεση ξεκινάει με τη λήψη μηνύματος από κάποιον φιλικό χρήστη, ή ένα φαινομενικά αθώο link για κάποιο βίντεο. Εάν ο χρήστης το ανοίξει, οδηγείται σε ψεύτικες ιστοσελίδες, στις οποίες του ζητείται να δώσει τα προσωπικά του στοιχεία και τους κωδικούς (phishing).

Όταν οι χρήστες ανοίξουν τα μηνύματα αυτά, οι απατεώνες πραγματοποιούν την ίδια επίθεση σε όλους τους χρήστες που βρίσκονται στις λίστες διευθύνσεων. Σύμφωνα με μελέτη του πανεπιστημίου της Ιντιάνα, οι επιθέσεις phishing στα κοινωνικά δίκτυα έφταναν το 2005 ποσοστά 70%. Οι λόγοι για τους οποίους γίνονται αυτές οι επιθέσεις είναι πολλοί. Συχνά οι δράστες επιχειρούν να οδηγήσουν τους χρήστες σε ιστοσελίδες, στις οποίες το κέρδος, καθορίζεται από τον αριθμό των κλικαρισμάτων, δηλαδή των επισκέψεων. Ταυτόχρονα προσπαθούν να αποσπάσουν πληροφορίες από τον χρήστη, όπως προσωπικούς κωδικούς πρόσβασης σε τραπεζικούς λογαριασμούς, με στόχο το κέρδος.

Στόχος των επίδοξων hackers είναι συνήθως υψηλόβαθμα στελέχη εταιρειών ή σημαντικά πρόσωπα. Μέσω των δημόσιων ηλεκτρονικών εργαλείων, επιχειρούν να συλλέξουν πληροφορίες γι' αυτούς και να τις χρησιμοποιήσουν εναντίον τους. Με τα δεδομένα που δημοσιεύονται σε σελίδες κοινωνικής δικτύωσης, μαθαίνουν τις ηλεκτρονικές διευθύνσεις. Έπειτα, στέλνουν ηλεκτρονικά μηνύματα, τα οποία περιέχουν ιούς που προσβάλουν τον υπολογιστή. Δημιουργείται έτσι μια σύνδεση, η οποία είναι κρυφή και δύσκολα εντοπίζεται, με αποτέλεσμα, οι hackers να παραμένουν για αρκετό καιρό στο δίκτυο και να συλλέγουν πληροφορίες.

Οι κύριοι τύποι των σελίδων κοινωνικής δικτύωσης είναι οι εξής: σελίδες που περιέχουν κατηγορίες, τρόπους σύνδεσης με φίλους και ένα σύστημα προτάσεων που έχει να κάνει με την

εμπιστοσύνη. Τα πιο διαδεδομένα τέτοια μέσα είναι το Facebook, το Youtube και το Twitter και χρησιμοποιούνται ευρέως σε όλο τον κόσμο. Κάποια άλλα είναι περισσότερο ανεπτυγμένα σε συγκεκριμένες περιοχές, όπως το MySpace και το LinkedIn που είναι πιο γνωστά στη Βόρεια Αμερική.

Οι υπηρεσίες κοινωνικής δικτύωσης έχουν, ωστόσο, πολλές παγίδες και κινδύνους. Μετά από έρευνες, έχει διαπιστωθεί ότι οι περισσότεροι χρήστες που συμμετέχουν σε αυτές τις σελίδες περιλαμβάνουν στο προφίλ τους άκρως προσωπικές πληροφορίες, όπως, φωτογραφίες, ενδιαφέροντα, τον τόπο και την ψυχολογική κατάσταση στην οποία βρίσκονται τη δεδομένη στιγμή ενώ κάποιοι δημοσιεύουν ακόμα και τον αριθμό τηλεφώνου τους ή τη διεύθυνσή τους.

Σαφώς, ο μεγαλύτερος κίνδυνος είναι για τους ανήλικους, εφόσον είναι δύσκολη η ταυτοποίηση του πραγματικού προσώπου που κρύβεται πίσω από ένα διαδικτυακό προφίλ. Επιπλέον, με τα παιδιά, είναι πιο εύκολη η αλίευση περισσότερων πληροφοριών από αυτές που ήδη υπάρχουν στα προφίλ. Αυτό το «ψάρεμα» πληροφοριών στοχεύει στην ψυχολογική, κοινωνική ή και κοινωνική πίεση του χρήστη από τους δράστες. Σε πιο ακραίες περιπτώσεις, επιχειρούν τον εκφοβισμό, τον εκβιασμό και την παρενόχληση του παιδιού.

Κάθε συμμετέχων στα μέσα κοινωνικής δικτύωσης θα πρέπει να εστιάζει την προσοχή του στην ασφάλεια του ηλεκτρονικού του προφίλ, τα δευτερεύοντα δεδομένα που αποκαλύπτει, στην ταυτοποίηση προσώπων από διάφορους λογαριασμούς, στον εντοπισμό του ατόμου στον φυσικό κόσμο, το μαρκάρισμα του προσώπου του σε φωτογραφίες, τη μη ολοκληρωτική διαγραφή του προφίλ του, τα μηνύματα spam, το psishing, την παρενόχληση και το βλαβερό λογισμικό.

Ψηφιακοί φάκελοι προσωπικών δεδομένων:

Στις ιστοσελίδες κοινωνικής δικτύωσης, ο κάθε χρήστης δημιουργεί το προσωπικό του ηλεκτρονικό προφίλ. Τα ηλεκτρονικά αυτά προφίλ μπορούν εύκολα να αποθηκευτούν από διάφορους χάκερς και να αποτελέσουν, έτσι, μέρος ψηφιακών φακέλων προσωπικών δεδομένων. Είναι τόσο εύκολη αυτή η αποθήκευση των πληροφοριών, ώστε κάποιες φορές, μπορούν να βρεθούν ακόμη και με μια απλή αναζήτηση. Για να αποφευχθεί αυτό από τους χρήστες, θα πρέπει μετά τη δημιουργία του προφίλ, να αλλάζονται οι προεπιλεγμένες ρυθμίσεις ασφαλείας.

Δευτερεύοντα δεδομένα:

Οι χρήστες που συμμετέχουν σε τέτοιου είδους σελίδες, αναρτούν διάφορες πληροφορίες σχετικές με την προσωπική τους ζωή. Εκτός όμως από αυτές τις πληροφορίες που δημοσιεύουν με τη θέλησή τους, αποκαλύπτουν κι άλλα δευτερεύοντα δεδομένα, αυτόματα. Αποκαλύπτουν, για παράδειγμα, στοιχεία που αφορούν τις επισκέψεις τους σε προφίλ άλλων μελών της υπηρεσίας, μηνύματα που έχουν στείλει μέσω διαδικτύου και πολλές άλλες πληροφορίες.

Οι γνωστές ιστοσελίδες κοινωνικής δικτύωσης, στις πολιτικές απορρήτου που διαθέτουν, δε διευκρινίζουν σαφώς ποιος ενδέχεται να μπορεί να έχει πρόσβαση στα προσωπικά δεδομένα του χρήστη. Επίσης, δεν καθορίζεται με σαφήνεια τι αποτελεί προσωπικό δεδομένο και τι όχι. Όλα τα παραπάνω είναι παρατηρήσεις και συμπεράσματα του Ελληνικού Κόμβου Ασφαλούς Διαδικτύου, ο οποίος επισκέφτηκε τις πιο διαδεδομένες ιστοσελίδες τέτοιου τύπου. Επιπλέον, είναι γνωστό, ότι τα δεδομένα που συλλέγονται από τους χρήστες, με αυτόν τον τρόπο, είναι πιθανό να χρησιμοποιηθούν με στόχο το οικονομικό όφελος, από την πώλησή τους σε άλλους χρήστες.

Αναγνώριση προσώπου:

Οι χάκερς χρησιμοποιούν τις φωτογραφίες των χρηστών που δημοσιεύονται στα προφίλ τους. Οι φωτογραφίες αποτελούν μια ψηφιακή ταυτότητα του εκάστοτε χρήστη. Πλέον, μέσω των εξελιγμένων τεχνολογιών αναγνώρισης προσώπου αυτές οι φωτογραφίες μπορούν να ταυτιστούν με πληροφορίες από άλλες σελίδες κοινωνικής δικτύωσης. Εκεί, ο ίδιος χρήστης ενδέχεται να έχει δημοσιεύσει άλλα προσωπικά του στοιχεία, κάτι που οδηγεί φυσικά στη συλλογή περισσότερων δεδομένων προσωπικού χαρακτήρα από αυτά που θεωρούσε ο χρήστης ότι μοιράζεται στο διαδίκτυο.

Εντοπισμός στο φυσικό κόσμο:

Μέσω νέων προηγμένων τεχνολογιών, από τις φωτογραφίες που αναρτά ο χρήστης στο προφίλ του, είναι δυνατή η συλλογή δεδομένων που μαρτυρούν τον τόπο στον οποίο βρίσκεται, όπως για παράδειγμα μια φωτογραφία προφίλ, μπροστά από το σπίτι στο οποίο κατοικεί. Ο εντοπισμός του χρήστη στον πραγματικό κόσμο, εγκυμονεί κινδύνους για την ασφάλειά του. Είναι, επομένως, πολύ σημαντικό, ο χρήστης να μην κοινοποιεί φωτογραφίες, στις οποίες είναι εύκολα αντιληπτός ο τόπος κατοικίας.

Μεταδιδόμενα:

Σε πολλές σελίδες κοινωνικής δικτύωσης δίνεται η δυνατότητα στους χρήστες τους να μαρκάρουν τις φωτογραφίες τους με μεταδιδόμενα (metadata). Τα μεταδιδόμενα είναι συνήθως, σύνδεσμοι σε προφίλ ή διευθύνσεις ηλεκτρονικού ταχυδρομείου. Αυτό είναι πολύ επικίνδυνο, καθώς επιτρέπει στον δράστη, να συνδέσει φωτογραφίες του χρήστη, με προσωπικά δεδομένα του, χωρίς τη θέλησή του. Το περίεργο είναι ότι, αν και οι χρήστες μπορεί να τηρούν όλα τα απαραίτητα μέτρα ασφάλειας για τις φωτογραφίες τους, οι ιστοσελίδες κοινωνικής δικτύωσης επιτρέπουν στους χρήστες να μαρκάρουν τις φωτογραφίες άλλων χρηστών, χωρίς να τους ρωτούν αν το επιθυμούν ή όχι. Και σε αυτή την περίπτωση, κινδυνεύει η ιδιωτική ζωή του χρήστη.

Αδυναμία πλήρους διαγραφής του προφίλ:

Όταν ένας χρήστης επιθυμεί να διαγράψει τον λογαριασμό του από μια σελίδα κοινωνικής δικτύωσης, αυτή του επιτρέπει απλά να τον απενεργοποιήσει. Δε δύναται να διαγράψει πλήρως το προφίλ του, ούτε μπορεί να διαγράψει δευτερεύοντα δεδομένα, που συνδέονται με τον λογαριασμό του.

Ανεπιθύμητα Μηνύματα – μηνύματα spam:

Τα μηνύματα spam είναι ένα πολύ διαδεδομένο φαινόμενο στο διαδίκτυο. Τα μηνύματα αυτά, προωθούνται στους χρήστες μέσω διάφορων εφαρμογών που υπάρχουν στις ιστοσελίδες κοινωνικής δικτύωσης. Υπάρχουν, για παράδειγμα, ολόκληροι μηχανισμοί που αποστέλλουν μαζικά στους χρήστες αιτήματα φιλίας, ώστε να τους επιτρέπεται να σχολιάζουν στο προφίλ τους, σε αναρτήσεις γενικού ενδιαφέροντος. Ωστόσο, τα μηνύματα αυτά συχνά κρύβουν διαφημίσεις ή είναι σύνδεσμοι ιστοσελίδων πορνογραφικού περιεχομένου.

Εξειδικευμένη Επίθεση - phishing:

Πολλοί επιτήδειοι αντλούν πληροφορίες από τα προσωπικά προφίλ των χρηστών, ειδικά όταν εκείνοι δεν έχουν απαγορεύσει μέσω ρυθμίσεων, την πρόσβαση σε τρίτους. Η συλλογή των δεδομένων είναι πολύ εύκολη, και οι έγκυρες πληροφορίες χρησιμοποιούνται από τους επιτιθέμενους για phishing. Στην εξειδικευμένη αυτή επίθεση, ο χρήστης λαμβάνει ένα παραπλανητικό μήνυμα, στο οποίο κάνει κλικ πάνω στον σύνδεσμο και προκειμένου να συμμετάσχει, συμπληρώνει τα προσωπικά του στοιχεία σε μια εικονική φόρμα μιας ιστοσελίδας. . Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες, το 70% όσων έλαβαν τέτοιο μήνυμα, πάτησε το σύνδεσμο και έγραψε τα στοιχεία του στην ιστοσελίδα.

Παρενόχληση:

Οι επιτήδειοι μέσα από τις σελίδες κοινωνικής δικτύωσης, έχουν τη δυνατότητα να επικοινωνούν επανειλημμένα με τα θύματά τους, μέσω προσωπικών μηνυμάτων ή σχολίων σε διάφορες αναρτήσεις. Αυτό καλλιεργεί και διευκολύνει περιστατικά παρενόχλησης των συμμετεχόντων. Από τα πιο συνηθισμένα, είναι η δημιουργία ψεύτικου λογαριασμού, ο οποίος στοχεύει στην προσωπική προσβολή ή τον εξευτελισμό δημόσια του χρήστη. Ακόμα, δημιουργούνται εικονικά προφίλ, τα οποία υιοθετούν ονόματα και σύμβολα γνωστών εταιρειών ή και διάσημων προσωπικοτήτων. Οι δράστε αυτοί εκμεταλλεύονται τη φήμη των παραπάνω, με σκοπό φυσικά το κέρδος.

Βλαβερό Λογισμικό:

Τέλος, οι ιστοσελίδες κοινωνικής δικτύωσης περιλαμβάνουν διάφορες εφαρμογές «widgets». Ωστόσο, οι δημιουργοί αυτών των εφαρμογών δεν είναι πάντα πιστοποιημένοι επαρκώς. Επομένως, αυτές οι εφαρμογές υπάρχει περίπτωση να περιέχουν κακόβουλο λογισμικό και ιούς.

cyber bullying

Ο εκφοβισμός μέσω του Διαδικτύου είναι οποιαδήποτε πράξη επιθετικότητας, παρενόχλησης και εκφοβισμού που πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών επικοινωνίας και συγκεκριμένα μέσω του Διαδικτύου και των κινητών τηλεφώνων. Στον ορισμό του cyber bullying θα πρέπει να προστεθεί και η συστηματικότητα του φαινομένου, το οποίο επαναλαμβάνεται ανά χρονικά διαστήματα.

Ο όρος cyber bullying πρωτοειπώθηκε από τον Καναδό Bill Belsey και σχετίζεται με τον παραδοσιακό σωματικό ή ψυχολογικό εκφοβισμό, κατά τον οποίο ο θύτης προσπαθεί να προκαλέσει ζημιά ή να βλάψει το θύμα του.

Υπάρχουν διάφορες μορφές εκφοβισμού μέσω του διαδικτύου. Οι πιο διαδεδομένες είναι οι ακόλουθες:

- Πειράγματα που έχουν στόχο τη διασκέδαση
- Διάδοση ψευδών προσβλητικών φημών online
- Αποστολή ανεπιθύμητων μηνυμάτων στα θύματα (υβριστικά- προσβλητικά)
- Παρενόχληση μέσω διαδικτύου
- Δυσφήμηση σε τρίτους με μηνύματα, φωτογραφίες και βίντεο μέσω του ηλεκτρονικού ταχυδρομείου, μέσω κινητού, σε ιστοσελίδες, μπλογκς, chat rooms και άλλα.

Το φαινόμενο του cyber bullying, έχει σήμερα πάρει άλλες διαστάσεις. Παρότι αφορά το πρόβλημα της παρενόχλησης μαθητών και παιδιών μέσα από το ίντερνετ, είναι πλέον πιο περίπλοκο. Μπορεί το bullying να έχει "αντικαταστήσει", ίσως, τον παλιό "τσαμπουκά" στο σχολικό χώρο, ωστόσο, έχει πιο επικίνδυνα στοιχεία.

Οι ειδικοί αναζητούν τα αίτια της εξάπλωσης του φαινομένου στην οικογένεια. Συγκεκριμένα, ο κυριότερος λόγος είναι η έλλειψη επικοινωνίας ανάμεσα στα παιδιά και τους γονείς τους. Επιπλέον, απουσιάζει και η επιμέλεια καθώς και η επίβλεψη των παιδιών στη διάρκεια της ημέρας. Τα παιδιά ουσιαστικά οδηγούνται σε βίαια ξεσπάσματα και τελικά σε ακραίες συμπεριφορές, όπως το cyber bullying.

Αυτή η έλλειψη επικοινωνίας μέσα στην οικογένεια, μπορεί να προκαλέσει επίσης, στα παιδιά τη βίωση έντονων συναισθημάτων, όπως είναι ο θυμός, η απόγνωση, η ζήλια και άλλα. Γονείς που δεν έρχονται σε ουσιαστική επαφή με τα παιδιά τους, λόγω του σημερινού τρόπου ζωής, συνήθως τους προκαλούν ένα συναισθηματικό κενό, το οποίο έρχονται να καλύψουν άλλα συναισθήματα, όπως αυτά που προαναφέρθηκαν. Τέλος, η δημιουργία τέτοιων συναισθημάτων, μπορεί να προκληθεί και από παθογένεια του επιτιθέμενου. Άλλωστε, έχουν παρατηρηθεί περιστατικά, όπου ο δράστης νιώθει ικανοποίηση και ψυχαγωγείται με τον τρόπο που βλέπει να αντιδρούν τα θύματά του.

4.7. ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Το ξέπλυμα χρήματος είναι η διαδικασία «εξαφάνισης» χρημάτων, τα οποία έχουν προέλθει από παράνομες δραστηριότητες. Οι δράστες επιχειρούν το ξέπλυμα σε τρία στάδια. Στο πρώτο στάδιο, γίνεται η προσπάθεια μετατροπής των παράνομων χρημάτων σε μια μορφή πιο «αθώα» για τις διωκτικές αρχές. Έτσι, λοιπόν, τα χρήματα που προέρχονται από μη νόμιμες δραστηριότητες, καταλήγει σε διάφορα οικονομικά ιδρύματα ή στο λιανεμπόριο, πράγμα που το καθιστά λιγότερο ύποπτο. Στο δεύτερο στάδιο, πραγματοποιείται ο διαχωρισμός του χρήματος από την παράνομη πηγή του, με διάφορες οικονομικές συναλλαγές, ώστε να γίνει απόκρυψη του χρήματος. Στο τρίτο στάδιο, πραγματοποιείται η μετατροπή του παράνομου χρήματος σε μια άλλη μορφή, αυτή του εισοδήματος, το οποίο έχει προέλθει από νόμιμες επαγγελματικές εργασίες.

Πλέον, το ξέπλυμα βρώμικου χρήματος δε γίνεται σε καζίνο ή με δελτία στοιχήματος όπως συνέβαινε μέχρι τώρα. Σήμερα, υπάρχουν περισσότερες δυνατότητες για τους δράστες κι όλα αυτά μέσω ίντερνετ. Οι πιο συνηθισμένες μέθοδοι είναι οι εξής:

Ψηφιακά νομίσματα

Μια πολύ γνωστή μέθοδος είναι αυτή της μετατροπής μέσω ψηφιακών νομισμάτων τύπου Bitcoin, WebMoney κλπ. Η μετατροπή γίνεται με τον εξής τρόπο: ο χρήστης αγοράζει ψηφιακά νομίσματα χρησιμοποιώντας παράνομο χρήμα και έπειτα πληρώνει σε άλλον χρήστη, ο οποίος μετατρέπει το ψηφιακό νόμισμα σε πραγματικό. Με εξαίρεση ορισμένες υπηρεσίες που έχουν αναγνώριση ταυτότητας του χρήστη, στις υπόλοιπες, η παραπάνω διαδικασία πραγματοποιείται πολύ εύκολα και γρήγορα.

Online Gaming

Πλέον, στους λάτρεις των online παιχνιδιών συγκαταλέγονται και οι «επαγγελματίες». Στα παιχνίδια αυτά, καθώς και σε ψηφιακούς κόσμους, ο χρήστης έχει τη δυνατότητα να αγοράσει με πραγματικά χρήματα, διάφορα ψηφιακά αγαθά που τον βοηθάνε στο παιχνίδι. Στη συνέχεια, όσα από αυτά δε χρησιμοποιηθούν από τον χρήστη, τα ξαναμετατρέπει σε φυσικό χρήμα, το οποίο αυτή τη φορά είναι νόμιμο.

Παραπλανητικά e-mail

Πολύ συχνά, στέλνονται στους χρήστες διάφορα spam mails, τα οποία τους προτείνουν συμμετοχή σε επιχειρηματικές κινήσεις, με σκοπό το κέρδος. Αυτό γίνεται, μεταφέροντας χρηματικά ποσά από το λογαριασμό μας, επενδύοντας φυσικά σε αυτήν την υποτιθέμενη κερδοφόρα επιχείρηση. Τις περισσότερες φορές, τέτοιου είδους μηνύματα σκοπό έχουν την εξαπάτηση και το άδειασμα των λογαριασμών του χρήστη. Ωστόσο, σε κάποιες περιπτώσεις γίνονται πραγματικά μεταφορές χρημάτων και ο χρήστης φαίνεται να έχει κέρδος. Βέβαια, αυτό συμβαίνει γιατί ο χρήστης έχει ουσιαστικά μετατραπεί σε συνεργός του εκάστοτε επιχειρηματία, που θέλει να κάνει το ξέπλυμα.

Προσφορά εργασίας από το σπίτι

Με παρόμοιο τρόπο ο χρήστης μπορεί να εξαπατηθεί, αυτή τη φορά μέσω αγγελιών για εύρεση εργασίας. Σε αυτές τις αγγελίες, προσφέρεται εργασία από το σπίτι, με άμεσο και γρήγορο κέρδος. Ο χρήστης που θα καταπιαστεί με τέτοιου είδους εργασίες, προβαίνει και στη μεταφορά χρημάτων, μέσω του λογαριασμού του, δηλαδή σε ξέπλυμα χρήματος.

Online υπηρεσίες στοιχημάτων

Πρόκειται για την πιο διαδομένη μέθοδο ξεπλύματος χρήματος στην Ελλάδα. Άλλωστε, έχουν ακουστεί πολλά για το στοίχημα και τους αγώνες ποδοσφαίρου στην Ελλάδα. Σε αυτή την περίπτωση, αρκεί ο επιχειρηματίας να γνωρίζει καλά τους κατάλληλους συνεργάτες, όπως προέδρους αθλητικών ομάδων, ποδοσφαιριστές ή διαιτητές. Στη συνέχεια, τοποθετεί τα χρήματα που θέλει να ξεπλύνει σε συγκεκριμένους αγώνες και έπειτα μπορεί να εισπράξει το κέρδος ως νόμιμο χρήμα. Προφανώς, θα πρέπει να υπάρχει και η ανάλογη συνεννόηση με την online εταιρεία στοιχημάτων, η οποία θα εισπράξει, στο τέλος, το ισοζύγιο κερδών.

4.8. ΔΙΑΚΙΝΗΣΗ ΝΑΡΚΩΤΙΚΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Σύμφωνα με έρευνα πανεπιστημίου της Αυστραλίας, μέσω του διαδικτύου, διακινούνται πλέον και ναρκωτικά. Η έρευνα έδειξε ότι διακινούνται «νόμιμα» ναρκωτικά, με ουσίες που τα καθιστούν επικίνδυνα και κατ' επέκταση παράνομα. Φυσικά, μέσω του διαδικτύου γίνεται και η συνηθισμένη διακίνηση των παράνομων ναρκωτικών, καθώς το διαδίκτυο δυσκολεύει τις διωκτικές αρχές στον εντοπισμό τους.

Τα ναρκωτικά στο διαδίκτυο δεν μεταφέρονται μόνο στη γνώριμη στους περισσότερους μορφή, δηλαδή σε χάπια, ενέσεις ή εισπνοές, αλλά εντοπίζονται σε ψηφιακά αρχεία, που οι χρήστες κατεβάζουν εύκολα και γρήγορα από το Διαδίκτυο στον υπολογιστή τους. Η επικίνδυνη «δόση» έχει τη μορφή ηχητικών κυμάτων, τα οποία έχουν ενσωματωθεί με ειδική επεξεργασία σε απλά μουσικά αρχεία mp3 και πωλούνται ως αρχεία drg. Σύμφωνα με τους εδικούς, πρόκειται για συγκεκριμένα ηχητικά κύματα συχνότητας 3 έως 30 Hertz (τα λεγόμενα υποηχητικά κύματα) που έχουν την ικανότητα να επηρεάζουν τη λειτουργία του εγκεφάλου προκαλώντας διάφορες δυσάρεστες αντιδράσεις. Υπάρχουν κύματα που έχουν χαλαρωτική δράση, καθώς και κύματα που προκαλούν υπερδιέγερση και ευφορία.

Έχει γίνει ήδη, εντοπισμός τέτοιων σελίδων από τις διωκτικές αρχές, στις οποίες απευθύνονται οι χρήστες για τη λήψη της «δόσης» τους. Χαρακτηριστικό είναι το γεγονός ότι, αναφέρεται από τους ειδικούς, η ύπαρξη ιστοσελίδας όπου παρέχονται οδηγίες χρήσης του ναρκωτικού αυτού για τους αρχάριους και στην οποία πωλούνται CD's με τραγούδια-«δόσεις». Επιπλέον, στέλνονται e-mail σε ανήλικους με τραγούδια τα οποία βρίσκονται στις συχνότητες που προαναφέρθηκαν, με σκοπό των εθισμό τους.

Κεφάλαιο 5: ΠΡΟΛΗΨΗ ΚΑΙ ΠΡΟΣΤΑΣΙΑ

5.1 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η προστασία των προσωπικών δεδομένων του ατόμου θεωρείται το πιο σημαντικό και σοβαρό κομμάτι της χρήσης του διαδικτύου. Για αυτό το λόγο, έχουν παρθεί πολλά μέτρα καθώς και νόμοι που εξασφαλίζουν την ασφάλεια των χρηστών.

Οι περισσότερες χώρες της Ευρωπαϊκής Ένωσης διαθέτουν νομοθεσία, η οποία φροντίζει για την προστασία των προσωπικών δεδομένων του ατόμου. Συγκεκριμένα, η Σύμβαση της 28 Ιανουαρίου 1981 του Συμβουλίου της Ευρώπης αφορά «την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα » και η Οδηγία 95/46/ ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24 Οκτωβρίου 1995 αναφέρεται «στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και στην ελεύθερη κυκλοφορία των δεδομένων αυτών». Όλα αυτά, λοιπόν, υποχρεώνουν τα κράτη - μέλη της Ευρωπαϊκής Ένωσης να λάβουν τα απαραίτητα μέτρα.

Η εφαρμογή της Ευρωπαϊκής Οδηγίας προστατεύει τον χρήστη του διαδικτύου από επεμβάσεις στην ιδιωτική του σφαίρα. Συγκεκριμένα, τον προστατεύει από:

- την δημιουργία αρχείων με προσωπικά του δεδομένα, τα οποία θα μπορούν να λαμβάνονται από τον οποιοδήποτε τρόπο μέσω Διαδικτύου,
- την μεταφορά αρχείων με προσωπικά δεδομένα μέσω του Διαδικτύου,
- την συλλογή και διασύνδεση αρχείων προσωπικού χαρακτήρα, τα οποία βρίσκονται σε διαφορετικούς υπολογιστές συνδεδεμένους στο Διαδίκτυο.

Το άρθρο 9 Α, το οποίο προστέθηκε στο Σύνταγμα της Ελλάδος, αναφέρει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως ο νόμος ορίζει.» Ο Νόμος 2472/1997 που αφορά στην Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, έχει ως αντικείμενο τη θέσπιση των προϋποθέσεων για την επεξεργασία αυτών των δεδομένων. Συγκεκριμένα, στο άρθρο 2 επεξηγεί ορισμούς που αφορούν το θέμα αυτό. Έτσι, λοιπόν, «δεδομένα προσωπικού χαρακτήρα νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.» Αν το υποκείμενο των δεδομένων δεν μπορεί να προσδιοριστεί στο Διαδίκτυο, τότε τα δεδομένα αυτά δεν προστατεύονται.

Επίσης ο νόμος δεν εφαρμόζεται, αν η επεξεργασία των δεδομένων γίνεται «από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών» (άρθρο 3 παρ. 2). Ο νόμος δεν εφαρμόζεται τέλος στην περίπτωση που η επεξεργασία εκτελείται από άτομο «εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο» (βλ. άρθρο 3 παρ. 3).

Με βάση το άρθρο 4 τα δεδομένα προσωπικού χαρακτήρα του χρήστη, για να επεξεργαστούν νόμιμα θα πρέπει να «Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς». Αυτό, φυσικά προϋποθέτει ότι δε γίνεται η οποιαδήποτε παραβίαση του απορρήτου ή ύποπτη εισχώρηση (hacking). «Τα δεδομένα πρέπει να είναι ακριβή και να υποβάλλονται σε ενημέρωση» σύμφωνα με τους όρους του άρθρου 4(παράγραφος 1γ). Σαφώς, θεωρείται δεδομένο ότι η επεξεργασία επιτρέπεται μόνο όταν ο χρήστης έχει δώσει τη συγκατάθεσή

του (π.χ. απάντηση στα «cookies»). Η συγκατάθεση του χρήστη είναι, επίσης, απαραίτητη όταν μια εταιρεία με πρόσβαση στο Διαδίκτυο συγκεντρώνει δεδομένα για ένα χρήστη, στον οποίο σκοπεύει να υποβάλει πρόταση κατάρτισης σύμβασης.

Με βάση το άρθρο 6 «Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας» (παράγραφος 1). Το άρθρο 7 απαγορεύει τη «συλλογή και την επεξεργασία ευαίσθητων δεδομένων». Επομένως, δεν μπορεί κάποιος να συλλέγει δεδομένα για τις επισκέψεις οποιαδήποτε χρήστη σε σελίδες με άσεμνο περιεχόμενο ή σε σελίδες πολιτικών κομμάτων ή θρησκευτικών οργανώσεων και άλλα., (εκτός αν ο χρήστης έχει δώσει τη συγκατάθεσή του γι' αυτή τη συλλογή στοιχείων ή γενικά αν συντρέχουν οι προϋποθέσεις του άρθρου 7 παράγραφος 2).

Συνεχίζοντας, ιδιαίτερη σημασία έχει το άρθρο 8 που επιτρέπει τη διασύνδεση αρχείων μόνο υπό συγκεκριμένους όρους. Η διασύνδεση αρχείων στο διαδίκτυο είναι μια σχετικά εύκολη διαδικασία, ειδικά αν σκεφτεί κανείς ότι ολόκληρα αρχεία μπορούν να μεταφέρονται μέσω του πρωτοκόλλου μεταφοράς αρχείων ή του ηλεκτρονικού ταχυδρομείου. Παρόλο που κάτι τέτοιο θα ήταν υπερβολικά δύσκολο, επιβάλλεται να γίνει δεκτό ότι όλες οι διασυνδέσεις αρχείων μέσω του Διαδικτύου πρέπει να γνωστοποιούνται στην Αρχή. Θα ήταν ορθό «Η άδεια διασύνδεσης … να χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων» (άρθρο 8 παρ. 4).

Με βάση το άρθρο 10, «η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη» (άρθρο 10, παράγραφος 1). Συμπεραίνεται, επομένως, ότι ο υπεύθυνος επεξεργαστής πρέπει να λάβει τα αναγκαία μέτρα για τη θωράκισή της επεξεργασίας από πιθανή πρόσβαση. Δεν πρέπει, προφανώς, να ανακοινώνει το αποτέλεσμα της επεξεργασίας των προσωπικών δεδομένων μέσω του Διαδικτύου. Ο χρήστης των δεδομένων έχει δικαίωμα α) ενημέρωσης, β) πρόσβασης, γ) αντίρρησης και δ) προσωρινής δικαστικής προστασίας, σύμφωνα με τα άρθρα 11, 12, 13 και 14 αντίστοιχα. Τέλος, επιβάλλονται κυρώσεις στους υπεύθυνους επεξεργασίας, καθώς και στους χρήστες που παραβιάζουν τον παρών Νόμο στο διαδίκτυο. Αυτές οι κυρώσεις αναφέρονται αναλυτικά στο Κεφάλαιο Ε', στα άρθρα 21 ως 23.

Σαφώς και η σύνταξη του προαναφερθέντα νόμου δεν έχει σε καμία περίπτωση, σκοπό να νομιμοποιήσει τη διαδικασία συλλογής προσωπικών δεδομένων του χρήστη. Ο βασικός σκοπός του είναι να ξεκαθαρίσει σε ποιες περιπτώσεις, η συλλογή αυτή επιτρέπεται για λόγους ασφαλείας. Αυτό που απασχολεί τους ειδικούς, είναι να εξασφαλιστεί η μη συλλογή δεδομένων προσωπικού χαρακτήρα του ατόμου. Αν, παρόλα αυτά, αυτό συμβεί, να εξασφαλιστεί επίσης, το δικαίωμα του χρήστη να γνωρίζει ότι κάποιος συλλέγει τα προσωπικά του δεδομένα και με ποιον σκοπό. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η ανωνυμία του χρήστη στο διαδίκτυο για την αποφυγή οποιουδήποτε κινδύνου.

Σύμφωνα με όλα τα παραπάνω, η έμφαση πρέπει δοθεί πλέον, όχι στην συνηθισμένη νομική κίνηση (να απευθύνεται δηλαδή το άτομο στη δικαιοσύνη για τη λήψη νομοθετικών μέτρων), αλλά στην ανάπτυξη της τεχνολογίας. Θα πρέπει, δηλαδή, να πέσει όλο το βάρος στην εύρεση τρόπων μέσω της τεχνολογίας, με τα οποία ο χρήστης θα έχει την απαραίτητη προστασία. Με αυτά τα μέσα, ο χρήστης θα μπορεί ο ίδιος να ελέγχει και να καθορίζει ότι αφορά τη συλλογή των προσωπικών του δεδομένων. Θα μπορεί για παράδειγμα, να ελέγχει ποιος έχει πρόσβαση στα δεδομένα του και επιπλέον να τσεκάρει ο ίδιος ποιος και για ποιους λόγους συλλέγει τα προσωπικά του δεδομένα. Η ανάπτυξη αυτού του είδους της τεχνολογίας, όμως, θα πρέπει να συνδυαστεί με ενσωμάτωσή της στα προϊόντα της πληροφορικής. Επίσης, θα πρέπει να συνταχθούν ειδικοί κανόνες για να εξασφαλιστεί η ανωνυμία του χρήστη. Μόνο με τους προαναφερθέντες όρους αυτή η τεχνολογία θα είναι πραγματικά προστατευτική για τον χρήστη.

Είναι γνωστό και μη αμφισβητήσιμο ότι ζούμε στην κοινωνία της πληροφορίας και της γνώσης. Ωστόσο, αυτό κρύβει και επικίνδυνα παρακλάδια, καθώς ορισμένες φορές παραβιάζονται αυστηρά προσωπικά ζητήματα. Η ανάγκη του ατόμου και όλο και μεγαλύτερη αναζήτηση πληροφοριών για κάθε θέμα, ξεπερνά τα όρια της απλής ενημέρωσης και αγγίζει την αδιακρισία. Με δεδομένο, λοιπόν, ότι ζούμε σε μια δημοκρατική κοινωνία, θα πρέπει να πέσει το βάρος στην προστασία των ατόμων από τέτοιες ενέργειες. Αυτό θα επιτευχθεί μόνο αν κατοχυρωθεί το απαραβίαστο των δεδομένων του χρήστη, σύμφωνα πάντα και με την προσωπική του βούληση, η οποία θα εκφράζεται νομικά και θα προστατεύεται από το δικαστήριο και από την επιτροπή προστασίας του χρήστη.

Τέλος, όλες οι γενικές και ασαφείς διατάξεις που αφορούν τα παραπάνω ζητήματα, θα πρέπει άμεσα να αντικατασταθούν από άλλες, πιο λεπτομερείς. Όταν υπάρχουν κανόνες οι οποίοι δεν καθορίζουν με ευκρίνεια τις περιπτώσεις που προστατεύεται ο πολίτης, οδηγούν ίσως στην παραβίαση των προσωπικών του δεδομένων και κατ' επέκταση σε αίσθημα ανασφάλειας από μεριάς του. Στην κοινωνία της πληροφορίας που ζούμε, επιβάλλεται άμεσα να υπάρχουν λεπτομερείς διατάξεις, οι οποίες θα αναφέρουν σαφώς, ποιος χρήστης θα έχει δικαίωμα πρόσβασης, σε ποια δεδομένα και φυσικά για ποιο σκοπό. Με αυτό θα ανακουφιστεί ο χρήστης, καθώς δε θα υπάρχουν «παραθυράκια» της νομοθεσίας που θα τον αφήνουν ακάλυπτο σε τέτοιες περιπτώσεις

5.2. ΜΕΤΡΑ ΠΡΟΦΥΛΑΞΗΣ

Είναι γνωστό, όπως θα αναφερθεί και παρακάτω, ότι η πρόληψη, σε όλους τους τομείς είναι πιο επιθυμητή και πιο αποτελεσματική από τη θεραπεία. Ισχύει στον τομέα της ιατρικής, ισχύει και στη χρήση του διαδικτύου. Όσο αφορά, επομένως, την προφύλαξη του τερματικού από τους κινδύνους του διαδικτύου, η πρόληψη είναι ίσως το ισχυρότερο όπλο του χρήστη. Βασικός σκοπός της πρόληψης και η μεγάλη της διαφορά από τη θεραπεία είναι η αποτροπή εκδήλωσης μιας επίθεσης στο διαδίκτυο, αποθαρρύνοντας τον δράστη και η έγκαιρη αντίδραση του θύματος από το αρχικό στάδιο που εκδηλώνεται μια επίθεση.

Τα πιο γνωστά μέτρα που μπορεί να πάρει ένας χρήστης για να προλάβει μια επίθεση στο διαδίκτυο, είναι οι κωδικοί πρόσβασης στα δεδομένα του, η χρήση λογισμικού ασφαλείας (antivirus, firewalls) και η κρυπτογραφία, που εφαρμόζεται κυρίως στην επικοινωνία.

Α. ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Σε αρκετά συστήματα του διαδικτύου, η είσοδος του χρήστη, πραγματοποιείται μόνο με την εισαγωγή κωδικών. Τα συστήματα αυτά, που χρησιμοποιούν κωδικούς , απαιτούν από το χρήστη την εισαγωγή ενός ονόματος χρήστη (user ID, user name) και ενός κωδικού πρόσβασης (password) για να επιτρέψουν την είσοδό του. Αφού ο χρήστης εισάγει το όνομα και τον κωδικό, το σύστημα τα συγκρίνει με τη βάση δεδομένων από κωδικούς, στην οποία είναι αποθηκευμένοι όλοι οι κωδικοί από τη στιγμή που ο χρήστης δημιουργεί λογαριασμό, και εφόσον διαπιστωθεί ταύτιση του επιτρέπεται η είσοδος.

Αυτό το μέτρο, είναι από τα πιο παλιά και εξαιτίας της απλότητάς του και της μεγάλης ασφάλειας που προσφέρει, αποτελεί την πιο συχνά εφαρμόσιμη μέθοδο προστασίας. Πλέον, οι κωδικοί πρόσβασης είναι ένα μεγάλο και αναπόσπαστο κομμάτι όλων των λειτουργικών συστημάτων.

Το σπουδαιότερο ζήτημα στην εφαρμογή των κωδικών πρόσβασης, όσο αφορά την αξιοπιστία του συστήματος που τους χρησιμοποιεί, είναι το κατά πόσο αυτοί μπορούν να διατηρήσουν τη μυστικότητά τους. Άλλωστε, υπάρχουν άπειροι τρόποι με τους οποίους οι κωδικοί πρόσβασης μπορούν να πάψουν να μένουν μυστικοί για τον χρήστη. Επιπλέον, ο ίδιος ο χρήστης με λάθος χειρισμούς ή με παραλείψεις μπορεί να αποκαλύψει τους κωδικούς του, χωρίς να το θέλει

Οι κυριότεροι κίνδυνοι που αντιμετωπίζει ένα σύστημα που χρησιμοποιεί κωδικούς πρόσβασης είναι

η σωστή επιλογή του κωδικού, το να μοιράζεται κάποιος τον κωδικό του, η παρακολούθηση πακέτων στο διαδίκτυο και η πρόσβαση του δράστη στο αρχείο αποθήκευσης των κωδικών.

Η επιλογή των κωδικών πρόσβασης: Η σωστή επιλογή του κωδικού πρόσβασης είναι ίσως το πιο σημαντικό κομμάτι της πρόληψης. Στις περισσότερες περιπτώσεις, ζητείται από τον χρήστη να επιλέξει τον κωδικό πρόσβασης που επιθυμεί. Τότε, εκείνος, συνήθως επιλέγει κωδικό που είναι εύκολος, ώστε να μην τον ξεχάσει. Τα πιο συνηθισμένα passwords που επιλέγονται από τους χρήστες είναι ονόματα ή ημερομηνίες γέννησης. Σε αυτή την περίπτωση, είναι αρκετά εύκολο για τον επιτιθέμενο να μαντέψει τον κωδικό, βλέποντας ποιο πρόσωπο κρύβεται πίσω από τον εκάστοτε λογαριασμό. Όταν η επιλογή των κωδικών δεν ζητείται από τους χρήστες, αλλά πραγματοποιείται από τους διαχειριστές του συστήματος, τότε επιτυγχάνεται μεγαλύτερη ασφάλεια. Βέβαια, και σε αυτή την περίπτωση εγκυμονούν κίνδυνοι, όταν ο χρήστης αναγκαστεί να γράψει τον δύσκολο κωδικό σε χαρτί ή σε σημειωματάριο, για να τον θυμάται και αυτός θα διαρρεύσει από μια ενδεχόμενη κλοπή ή απώλεια των προσωπικών του αντικειμένων.

Διαμοιρασμός των κωδικών πρόσβασης: Με αυτόν τον τρόπο, κάποιος χρήστης μπορεί να αποκαλύψει τον κωδικό του σε κάποιον άλλον, προκειμένου να τον διευκολύνει σε κάποια εργασία, ειδικά αν είναι σε απόσταση από τον υπολογιστή. Αυτός ο κωδικός στη συνέχεια μπορεί να αποκαλυφθεί αλλού ή να σημειωθεί από τον χρήστη σε ένα κομμάτι χαρτί και στη συνέχεια να διαδοθεί σε κάποιον τρίτο και ούτω κάθε εξής. Αυτός ο διαμοιρασμός των κωδικών πρόσβασης είναι αρκετά επικίνδυνος, όση κι αν είναι η εμπιστοσύνη που έχει ο ένας χρήστης στον άλλον, καθώς, δεν είναι σίγουρο σε ποια χέρια θα καταλήξουν οι κωδικοί και επομένως, ποιος θα έχει πρόσβαση στα προσωπικά αρχεία του χρήστη.

Παρακολούθηση πακέτων: Η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο, μπορεί να έχει ως αποτέλεσμα τη λήψη των κωδικών πρόσβασης από κάποιο άλλο πρόσωπο. Όταν για παράδειγμα, συνδέεται ένας κεντρικός υπολογιστής με έναν απομακρυσμένο υπολογιστή, απαιτείται από τον χρήστη να γράψει τους κωδικούς πρόσβασης. Αυτοί οι κωδικοί θα διακινηθούν μέσω διαδικτύου, από ένα προστατευμένο σύστημα στον απομακρυσμένο υπολογιστή.

Πρόσβαση στο αρχείο αποθήκευσης των κωδικών: Όλοι οι κωδικοί πρόσβασης των χρηστών του διαδικτύου αποθηκεύονται σε ένα αρχείο του διακομιστή, προκειμένου, να είναι δυνατή η διαδικασία ταυτοποίησης, όταν αυτοί εισαχθούν από τον χρήστη στο σύστημα. Στην περίπτωση που το αρχείο αυτό δεν είναι καλά φυλαγμένο ή δεν είναι κρυπτογραφημένο με μία hash function (θα αναλυθεί παρακάτω), ο δράστης μπορεί να το ανακτήσει και να έχει, πλέον, πρόσβαση σε όλους τους κωδικούς ενός οργανισμού.

Β. ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

Πρωταρχικός στόχος των συστημάτων είναι η χρήση συγκεκριμένου λογισμικού, το οποίο θα φροντίζει για την ασφάλεια στο διαδίκτυο. Οι διαχειριστές ενός συστήματος, πλέον, μεριμνούν για αυτό τον σκοπό, χρησιμοποιώντας διάφορες εφαρμογές. Οι πιο διαδεδομένες είναι τα antivirus και firewalls.

Λογισμικό Antivirus

Ο πιο συχνός τρόπος για να πραγματοποιηθεί μια επίθεση στο διαδίκτυο, είναι με ιούς. Οι ιοί μεταδίδονται στο σύστημα μέσω πακέτων δεδομένων. Δυστυχώς, σε καθημερινή βάση, κατασκευάζονται πολλοί ιοί, οι οποίοι διασπείρονται και απειλούν το υπολογιστικό σύστημα. Ο βασικός τρόπος αντιμετώπισης αυτής της επίθεσης είναι τα προγράμματα antivirus. Η χρήση

αντιβιοτικών προγραμμάτων προστατεύει τον υπολογιστή από επιθέσεις ιών. Ωστόσο, τέτοιου είδους λογισμικά είναι πολύ περίπλοκα, λόγω της συνεχούς δημιουργίας νέων ιών. Τα λογισμικά antivirus επιτελούν, ουσιαστικά, τρεις βασικές λειτουργίες: την ανίχνευση, την αναγνώριση και τον καθαρισμό των ιών.

Ανίχνευση των ιών: Η ανίχνευση των ιών πραγματοποιείται για να εξακριβωθεί, εάν έχει μολυνθεί το σύστημα από ιούς. Η διαδικασία αυτή, μπορεί να γίνει με δύο τρόπους. Ο πρώτος τρόπος είναι όταν ο χρήστης επιλέγει να γίνει έλεγχος του σκληρού του δίσκου, μέσω του λογισμικού που του επιτρέπει τέτοιες ενέργειες. Ο δεύτερος τρόπος και ο πιο συχνός πλέον είναι με αυτόματο έλεγχο που κάνει το λογισμικό. Συγκεκριμένα, το λογισμικό φορτώνεται στη μνήμη RAM του συστήματος και κάνει αυτόματα έλεγχο σε όλες τις εφαρμογές που εκτελούνται.

Προσδιορισμός της ταυτότητας των ιών: Αυτή η διαδικασία γίνεται προκειμένου να αναγνωριστεί ο ιός. Όταν, λοιπόν, το σύστημα έχει προσβληθεί από κάποιο ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητά του. Αυτή είναι μια πολύ σημαντική ενέργεια, καθώς επιτρέπει να εκτιμηθεί το μέγεθος της ζημιάς που έχει προκαλέσει ο ιός. Επιπλέον, φροντίζει ώστε να γίνουν οι απαραίτητες ενέργειες, για την διόρθωση της ζημιάς και για την αποκατάσταση της ομαλής λειτουργίας του συστήματος.

Καθαρισμός των ιών: Στην τελευταία φάση, μετά τον εντοπισμό και την αναγνώριση των ιών, πρέπει να γίνει και η αφαίρεσή τους. Συνήθως, όταν το λογισμικό εντοπίσει τον ιό, δίνει συγκεκριμένες προτάσεις στον χρήστη, ώστε να μπορέσει να τον καταπολεμήσει. Το πιο σύνηθες είναι να του προτείνει:

- να επιδιορθώσει το αρχείο που έχει τον ιό,
- να περιορίσει το αρχείο, ώστε να μην μπορεί να χρησιμοποιηθεί και επομένως να μην διατρέχεται κίνδυνος,
- να διαγράψει το αρχείο, που έχει μολυνθεί.

Firewalls

Στην πληροφορική, ο όρος Firewall αναφέρεται σε μια συσκευή ή εργαλείο λογισμικού (ή και συνδυασμό των δύο), που ελέγχει τα πακέτα που προσπαθούν να εισέλθουν ή και να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Πρόκειται για λογισμικά που έχουν την ικανότητα να ξεχωρίζουν ένα «ασφαλές» δίκτυο (π.χ. το δίκτυο μιας εταιρείας), από ένα μη ασφαλές δίκτυο.

Τα πιο πολλά λογισμικά αυτού του τύπου επιτελούν δυο βασικές λειτουργίες για την ασφάλεια του συστήματος:
Α) Φιλτράρισμα πακέτων. Ειδικεύεται, δηλαδή, στο να φιλτράρει τα πακέτα που διακινούνται μέσω διαδικτύου. Έτσι, μπορεί να επιτρέπει ή να απαγορεύει την όποια κίνηση των πακέτων, με βάση την υπάρχουσα πολιτική ασφαλείας και
Β) Πύλες εφαρμογών. Σε αυτή τη λειτουργία τα λογισμικά προσφέρουν υπηρεσίες στους χρήστες που βρίσκονται μέσα στο δίκτυο και ταυτόχρονα προστατεύουν τους εξωτερικούς χρήστες που επισκέπτονται μια σελίδα από εξωτερικές απειλές.

Γ. ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ

Η κρυπτολογία είναι η επιστήμη που ασχολείται με την ασφάλεια στην επικοινωνία, μέσω του διαδικτύου. Περιλαμβάνει δύο κλάδους: Την κρυπτογραφία και την κρυπτανάλυση. Η κρυπτανάλυση ασχολείται με την ανάλυση και το σπάσιμο των αλγορίθμων κρυπτογράφησης. Η κρυπτογραφία «είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.» (ορισμός Βικιπαίδεια) Η κρυπτογραφία επιτελεί τέσσερεις βασικές λειτουργίες: την εμπιστευτικότητα, τη μη άρνηση της αυθεντικότητας, την ακεραιότητα και την εξακρίβωση του είδους της εισερχόμενης πληροφορίας.

Η κρυπτογράφηση είναι μια διαδικασία, με την οποία επιχειρείται η μετατροπή μιας πληροφορίας, από μια κατανοητή μορφή σε ένα γρίφο, ο οποίος δε θα γίνεται κατανοητός. Με την αντίθετη διαδικασία, δηλαδή την αποκρυπτογράφηση, ο ακατανόητος γρίφος επανέρχεται στην αρχική του μορφή και η πληροφορία μπορεί πλέον, ξεκάθαρα να αναγνωστεί.

Υπάρχουν τέσσερα βασικά στοιχεία, τα οποία απαρτίζουν ένα σύστημα κρυπτογράφησης, όπως το γνωρίζουμε σήμερα.

α) Το αρχικό μήνυμα.

β) Το σύστημα κρυπτογράφησης το οποίο αποτελείται από έναν αλγόριθμο κρυπτογράφησης και έναν αποκρυπτογράφησης.

γ) Το κρυπτογραφημένο κείμενο, το οποίο είναι το αποτέλεσμα της κρυπτογράφησης στο αρχικό μήνυμα, πριν γίνει η αποστολή του στον παραλήπτη και

δ) Ένα κλειδί, το οποίο είναι μια σειρά από σύμβολα, που χρησιμοποιείται από τους αλγόριθμους στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος.

Πρακτικά, η κρυπτογραφία διαιρείται σε δύο βασικές κατηγορίες:

- Την συμμετρική κρυπτογραφία, στην οποία χρησιμοποιείται ένα ιδιωτικό κλειδί και
- Την ασύμμετρη κρυπτογραφία, στην οποία χρησιμοποιούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό.

Συμμετρική κρυπτογραφία

Η συμμετρική κρυπτογράφηση, χαρακτηρίζεται από το γεγονός ότι χρησιμοποιείται το ίδιο κλειδί, τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση του μηνύματος. Σαφώς, προϋποθέτεται, το κλειδί αυτό να είναι γνωστό στους χρήστες, που θέλουν να επικοινωνήσουν, συνήθως τους έχει σταλεί μέσω ενός ασφαλούς καναλιού επικοινωνίας. Η διαδικασία επικοινωνίας σε αυτού του είδους την κρυπτογραφία έχει ως εξής: Το αρχικό μήνυμα κρυπτογραφείται με το μυστικό κλειδί του αποστολέα, όπως προαναφέρθηκε και έπειτα, αποστέλλεται στον παραλήπτη μέσω του

καναλιού επικοινωνίας, με ασφάλεια. Ο παραλήπτης παραλαμβάνει το κρυπτογραφημένο μήνυμα και στη συνέχεια, το αποκρυπτογραφεί με το ίδιο μυστικό κλειδί, που έγινε η κρυπτογράφησή του.

Ασύμμετρη κρυπτογραφία

Η ασύμμετρη κρυπτογράφηση χαρακτηρίζεται από τη χρήση δύο διαφορετικών μυστικών κλειδιών. Ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση. Κύριο γνώρισμα των κλειδιών αυτών είναι, ότι αν και αφορούν τα ίδια δεδομένα, η γνώση του ενός δεν μπορεί να οδηγήσει στην αποκάλυψη του άλλου, εξασφαλίζοντας έτσι, μεγαλύτερη ασφάλεια. Το κλειδί, που χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος, ονομάζεται δημόσιο και είναι γνωστό σε όλους, ενώ το κλειδί με το οποίο γίνεται η αποκρυπτογράφηση, ονομάζεται ιδιωτικό και το γνωρίζει μόνο αυτός που πρόκειται να πραγματοποιήσει την αποκρυπτογράφηση.

Η προστασία, που προσφέρεται με αυτήν την κρυπτογράφηση, είναι σαφώς πιο ισχυρή από την συμμετρική. Επιπλέον, δεν είναι απαραίτητη και η εξασφάλιση του ασφαλούς διαύλου επικοινωνίας για την αποστολή του μυστικού κλειδιού. Όταν, λοιπόν, ένας χρήστης επιθυμεί να λάβει ένα κρυπτογραφημένο μήνυμα δίνει στον αποστολέα το δημόσιο κλειδί του, με το οποίο γίνεται η κρυπτογράφηση του μηνύματος και στη συνέχεια, προχωράει στην αποκρυπτογράφηση, με το ιδιωτικό κλειδί που μόνο αυτός κατέχει. Το μειονέκτημα της διαδικασίας αυτής είναι, ότι απαιτούνται μεγαλύτερα κλειδιά απ’ ότι στην συμμετρική κρυπτογράφηση.

Αν χρησιμοποιηθεί η ασύμμετρη κρυπτογραφία αντίστροφα, μπορεί να γίνει αναγνώριση του αποστολέα ενός μηνύματος. Πιο αναλυτικά, ο αποστολέας, αρχικά, κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Το μήνυμα, τότε, δύναται να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί, το οποίο όμως είναι γνωστό σε περισσότερους του ενός χρήστες. Ωστόσο, η αρχική κρυπτογράφηση του μηνύματος με ιδιωτικό κλειδί, προσδιορίζει τον αποστολέα του. Αυτή η συγκεκριμένη κρυπτογράφηση, με ιδιωτικό κλειδί, συνηθίζεται να λέγεται ψηφιακή υπογραφή και έχει την ικανότητα να πραγματοποιεί την ταυτοποίηση του αποστολέα του μηνύματος.

Διαχείριση δημοσίων κλειδιών – πιστοποιητικά

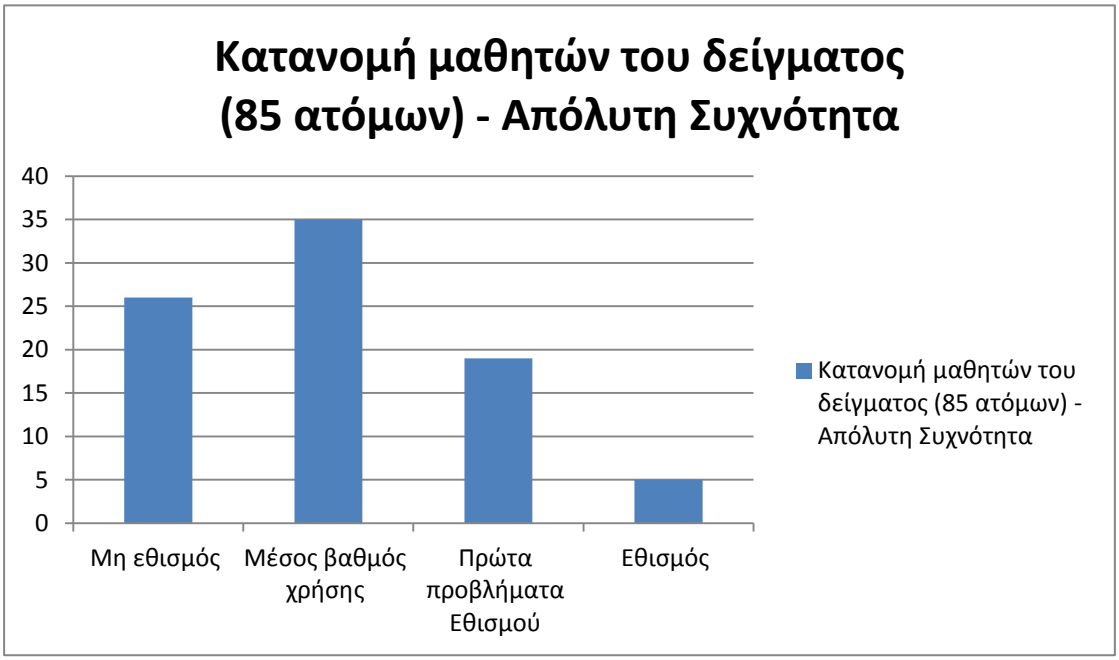
Σε αυτό το σημείο, προκύπτει κι ένα άλλο ζήτημα, αυτό της αυθεντικότητας των κλειδιών. Είναι πολύ δύσκολο να εξακριβωθεί με ασφάλεια ότι το δημόσιο κλειδί, που λαμβάνει ένας χρήστης, είναι πράγματι αυθεντικό. Η εξακρίβωση αυτή, ωστόσο, είναι πολύ σημαντική, διότι κατά την επαλήθευση μιας ψηφιακής υπογραφής, ο χρήστης πρέπει να είναι σίγουρος, ότι το δημόσιο κλειδί που κατέχει, είναι πραγματικά το δημόσιο κλειδί του αποστολέα. Επομένως, θα πρέπει κάθε χρήστης να εξακριβώνει την αυθεντικότητα του δημόσιου κλειδιού, πριν προχωρήσει στη χρήση του.

Αυτό το πρόβλημα έρχεται να λύσει η αρχή πιστοποίησης. Πρόκειται για έναν τρίτο παράγοντα, ο οποίος έχει τη δυνατότητα εξακρίβωσης της αυθεντικότητας των δημόσιων κλειδιών και χαίρει της εμπιστοσύνης και των δύο πλευρών. Η συγκεκριμένη αρχή υπογράφει με το δικό της ιδιωτικό κλειδί, τα δημόσια κλειδιά, προσθέτοντας κάποια επιπλέον στοιχεία, π.χ. περίοδο εγκυρότητας. Το τμήμα αυτό των δεδομένων, που έχει λάβει την υπογραφή από την αρχή πιστοποίησης, ονομάζεται πιστοποιητικό. Το πιστοποιητικό μπορεί με τη σειρά του να επαληθευτεί, χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης.

ΚΕΦΑΛΑΙΟ 6. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

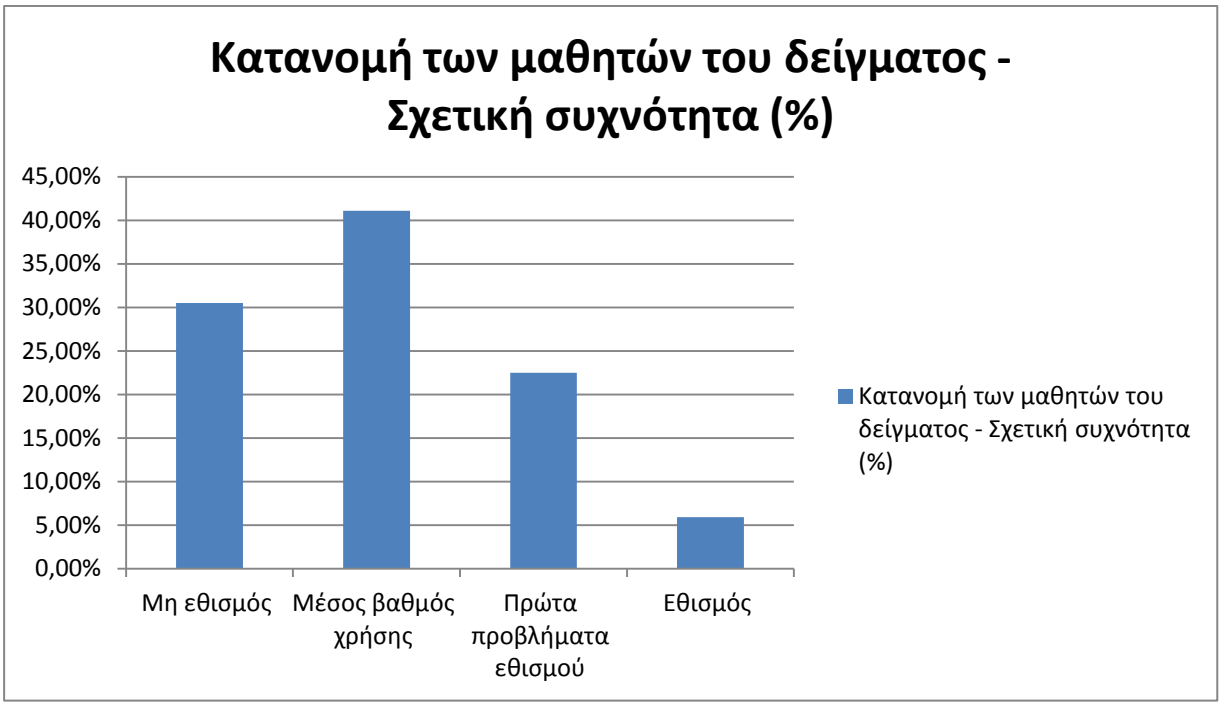
6.1. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

Σε δείγμα 85 μαθητών έγινε έρευνα με τη μέθοδο των ερωτηματολογίων. Μελετήθηκε ο βαθμός Εθισμού των μαθητών στο Διαδίκτυο με βάση τις απαντήσεις τους. Επιπλέον, έγινε διαχωρισμός σύμφωνα με το φύλο για πιο λεπτομερή μελέτη των παρατηρήσεων. Τα αποτελέσματα της έρευνας φαίνονται παρακάτω στα σχετικά γραφήματα.



Κατανομή των μαθητών του δείγματος ως προς τον βαθμό Εθισμού στο Διαδίκτυο.

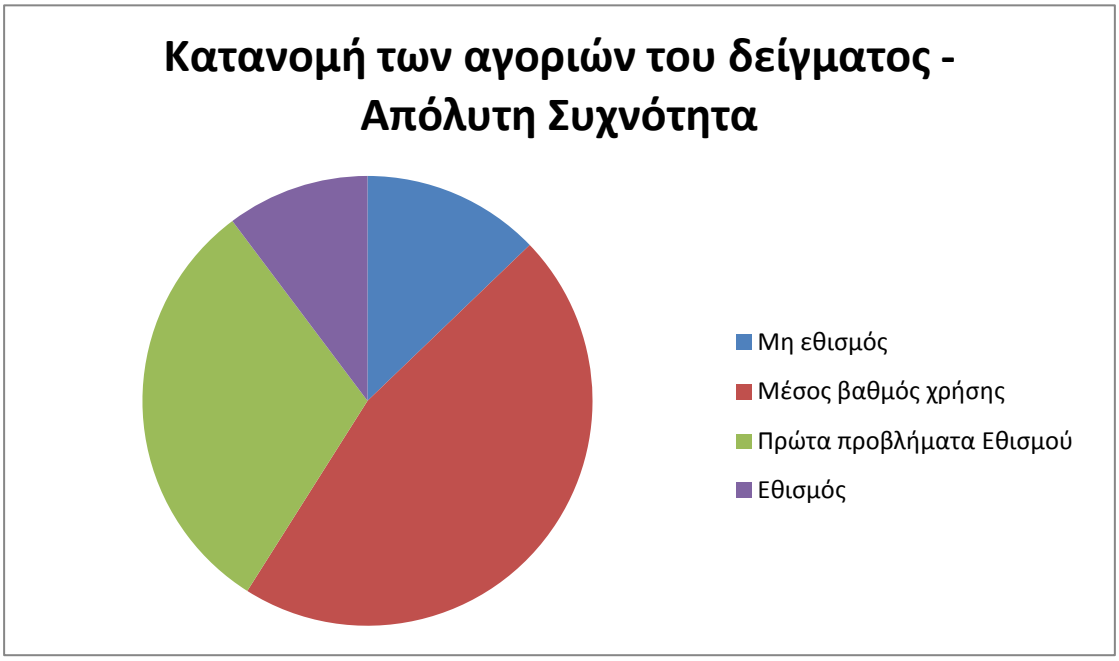
Σύνολο: 85 μαθητές



Κατανομή των μαθητών του δείγματος ως προς τον βαθμό Εθισμού στο Διαδίκτυο.

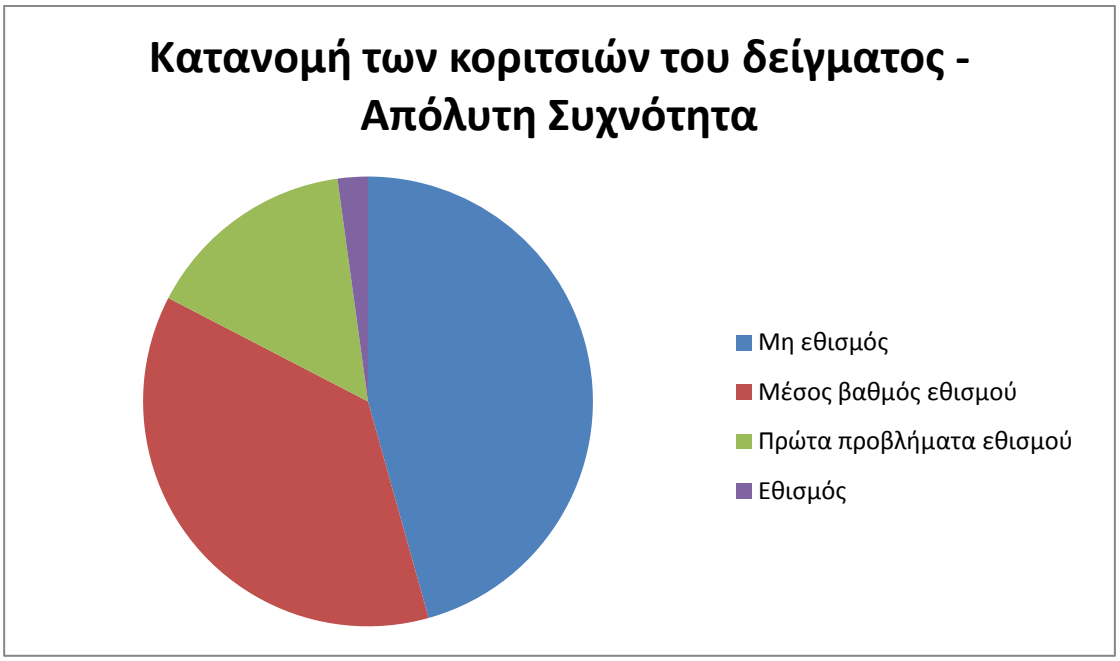
Σχετική Συχνότητα %.

Σύνολο: 100



Κατανομή των αγοριών του δείγματος ως προς τον βαθμό Εθισμού στο Διαδίκτυο

(Σε σύνολο 85 μαθητών, 39 αγόρια)



Κατανομή των κοριτσιών του δείγματος ως προς τον βαθμό εθισμού

(Σε σύνολο 85 μαθητών, 46 κορίτσια)

6.2. ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΡΕΥΝΑΣ

Παρατηρώντας τα παραπάνω αποτελέσματα της έρευνας σε 85 μαθητές, παρατηρούμε ότι το ποσοστό των ατόμων με μέσο βαθμό χρήσης του διαδικτύου είναι αρκετά μεγαλύτερος από το αντίστοιχο ποσοστό των μαθητών που δεν έδειξαν κανένα δείγμα εθισμού. Παρατηρείται, επίσης, ότι ο αριθμός των μαθητών του δείγματος που παρουσιάζουν τα πρώτα συμπτώματα για μετέπειτα εθισμό στο διαδίκτυο είναι αρκετά υψηλός. Ωστόσο, σε αυτό το στάδιο, με την κατάλληλη παρέμβαση, τα παιδιά αυτά μπορούν να ξεπεράσουν τον σκόπελο του εθισμού κι αυτό είναι παρήγορο.

Μη ικανοποιητικά χαμηλό είναι το ποσοστό των μαθητών που έχουν παρουσιάσει δείγματα εξάρτησης από τον ηλεκτρονικό υπολογιστή και το διαδίκτυο. Λαμβάνοντας υπόψη, όπως διεξοδικά αναφέραμε παραπάνω, όλες τις προσπάθειες τόσο του κρατικού όσο και του μη κυβερνητικού μηχανισμού, για πρόληψη του εθισμού ειδικά στους νέους, θα περίμενε κανείς, το συγκεκριμένο ποσοστό να βρίσκεται πολύ χαμηλότερα.

Όσο αφορά τον διαχωρισμό των νέων του δείγματος ως προς το φύλο, τα δεδομένα εδώ μας δίνουν σημαντικά στοιχεία που πρέπει να ληφθούν υπόψη από τους υπεύθυνους. Συγκεκριμένα, παρατηρείται ότι τα αγόρια είναι πιο επιρρεπή από τα κορίτσια στο να παρουσιάσουν κάποια στιγμή δείγματα εθισμού στο διαδίκτυο. Χαρακτηριστικό είναι το συντριπτικό ποσοστό των αγοριών έναντι των κοριτσιών (4 προς 1) που έχουν ήδη εθιστεί. Αξιοσημείωτος είναι επίσης και ο αριθμός των αγοριών που δείχνουν τα πρώτα σημάδια εθισμού. Σε σύνολο 19 ατόμων, τα κορίτσια είναι μόλις 7, με τα αγόρια να έχουν κι εδώ την πρωτιά.

Παρόμοια δεδομένα παρατηρούνται και στα δείγματα των μαθητών που δεν παρουσιάζουν κανένα εθισμό. Εδώ, βέβαια, τα ποσοστά αντιστρέφονται, καθώς ο αριθμός των αγοριών είναι μόλις στο 5, ενώ τα κορίτσια φτάνουν τα 21. Σημαντικό είναι επίσης, ότι όταν μιλάμε για ορθή χρήση του διαδικτύου, τα ποσοστά και των δύο φύλων ισοσταθμίζονται.

Προσπαθώντας να ερμηνευτούν τα παραπάνω δεδομένα της έρευνας, φτάνει κανείς στο συμπέρασμα, ότι η βασική και ίσως η μόνη αιτία αυτού του διαχωρισμού των δύο φύλων, είναι η τάση των αρσενικών κάθε ηλικίας για ενασχόληση με ηλεκτρονικά παιχνίδια. Όπως παρατηρείται, αυτή η ενασχόληση των αρσενικών μπορεί να ξεκινήσει από πολύ μικρές ηλικίες και να σταματήσει πολύ αργότερα. Είναι, επομένως, προφανές ότι παρουσιάζουν περισσότερες πιθανότητες να εθιστούν στο διαδίκτυο, σε σχέση με τα θηλυκά.

ΚΕΦΑΛΑΙΟ 7. ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ- ΑΞΙΟΛΟΓΗΣΗ

7.1. ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΡΓΑΣΙΑΣ

Ολοκληρώνοντας την παρούσα πτυχιακή εργασία για τον Εθισμό στο Διαδίκτυο, θα γίνει σε αυτό το σημείο μια προσπάθεια να παρατεθούν τα συμπεράσματα της έρευνας. Μέσα από τη μελέτη του όρου Εθισμός, έγινε κατανοητό ότι δεν πρέπει να συγχέεται η έννοια αυτή με την πολύωρη απασχόληση του ατόμου με τον ηλεκτρονικό υπολογιστή. Ο Εθισμός είναι ένα φαινόμενο που έχει αρκετά παρακλάδια. Σημαντικό ρόλο φαίνεται να παίζουν η προσωπικότητα του χρήστη καθώς και ο κοινωνικός περίγυρος. Κάνοντας αναφορά στον κοινωνικό περίγυρο, καλό είναι να αναφερθεί ότι νοείται η οικογένεια, το σχολείο και φυσικά οι παρέες του ατόμου, χωρίς να γίνεται διαχωρισμός των ηλικιών. Οι φιλικές σχέσεις επηρεάζουν τόσο τους ανήλικους όσο και τους ενήλικες παίζοντας καθοριστικό ρόλο στις συμπεριφορές που θα αναπτύξει το άτομο. Επομένως, ο εθισμός στο διαδίκτυο θα πρέπει να μελετάται μέσα στο κοινωνικό περιβάλλον του χρήστη.

Ο αριθμός των χρηστών του διαδικτύου αυξάνεται με γοργούς ρυθμούς τα τελευταία χρόνια. Αυτή η αλόγιστη χρήση ενισχύεται από πολλούς παράγοντες. Η ανωνυμία, η εύκολη, γρήγορη και ανέξοδη πρόσβαση καθώς και το αίσθημα ικανοποίησης και κοινωνικοποίησης που νιώθει ο χρήστης είναι μόνο κάποιοι από αυτούς τους παράγοντες.

Αδιαμφισβήτητα, ο ηλεκτρονικός υπολογιστής και το διαδίκτυο είναι ένα ισχυρό μέσο στα χέρια των χρηστών. Θα πρέπει όμως να γίνεται και σωστή χρήση τους, χωρίς να παραμελούνται άλλες πρωταρχικές προτεραιότητες. Οι δυνατότητες αυτών των μέσων είναι άπειρες και αυτό προφανώς είναι που συνέβαλε στην γρήγορη εξάπλωσή του.

Όσο αφορά τον Εθισμό των μικρών παιδιών στο Διαδίκτυο, είναι προφανές ότι καθοριστικό ρόλο παίζει η οικογένεια, οι φιλικές σχέσεις και το σχολείο. Οι γονείς, έχοντας τόσο μεγάλο μερίδιο ευθύνης, θα πρέπει πρώτα απ' όλα να γνωρίζουν τα μέτρα προστασίας και πρόληψης και έπειτα να τα εφαρμόζουν. Θα πρέπει να δώσουν ιδιαίτερη έμφαση στην ενημέρωση των παιδιών και στη δημιουργία ευχάριστου κλίματος στο σπίτι. Άλλωστε, όση περισσότερη ατομικότητα εμφανίζεται, τόσο πιο πιθανή γίνεται η εμφάνιση διαφόρων ειδών εξαρτήσεων. Γενικά, πρέπει να γίνει κατανοητό από όλους ότι το διαδίκτυο αποτελεί ένα σημαντικό εργαλείο για αναζήτηση πληροφοριών, ψυχαγωγία και επικοινωνία. Πρέπει, ωστόσο, να λαμβάνεται υπόψη και το γεγονός ότι η κακή χρήση του μπορεί να επιφέρει σοβαρές επιπτώσεις στο άτομο. Σημαντικό μέσο προστασίας αποτελεί η γνώση για την ύπαρξη του φαινομένου καθώς και η παρατήρηση από τη μεριά του χρήστη.

Χαρακτηριστικό φαινόμενο της σύγχρονης εποχής είναι η καθημερινή επαφή με το διαδίκτυο, από τον υπολογιστή, το τάμπλετ και το κινητό. Ο καθένας μπορεί να κάνει αγορές on line, να ακούσει μουσική από το διαδίκτυο, να παίξει ένα online παιχνίδι ακόμη και να ξεφυλλίσει ηλεκτρονικά βιβλία. Τα μέσα κοινωνικής δικτύωσης είναι πλέον τόσα πολλά, με αποτέλεσμα ο κάθε χρήστης να διαθέτει αντίστοιχους λογαριασμούς. Μέσα από τον λογαριασμό του, μπορεί να ανεβάσει φωτογραφίες και να τις μοιραστεί με τους διαδικτυακούς του φίλους, να δηλώσει τον τόπο που βρίσκεται τη δεδομένη χρονική στιγμή, να «ποστάρει» αυτό που τον εκφράζει και φυσικά να σχολιάσει αυτά που έχουν κοινοποιήσει οι άλλοι. Όλα τα παραπάνω οδηγούν το άτομο στην ανάγκη για σύνδεση στο διαδίκτυο ανά πάσα στιγμή οπουδήποτε κι αν βρίσκεται. Η συμμετοχή, επομένως, στα μέσα αυτά, καταλαμβάνει άπειρο χρόνο από την καθημερινότητα και ορισμένες φορές αγγίζει τα όρια της εξάρτησης.

Η εξάρτηση, αρχικά, αντιμετωπίστηκε πολύ επιφανειακά, ωστόσο στην πορεία της εξέλιξης της πληροφορικής κοινωνίας, έγινε ένας νέος τρόπος έκφρασης. Καθοριστικό ρόλο σ' αυτή την πορεία έπαιξε η βαρύτητα που ρίχνει στο διαδίκτυο ο χρήστης. Πλέον, είναι γνωστό ότι ο καθένας κάνει αναζητήσεις στο διαδίκτυο για τα πάντα, από συνταγές μαγειρικής μέχρι και ιατρικές πληροφορίες. Χαρακτηριστική είναι επίσης η άποψη ορισμένων ότι αν κάτι δε βρίσκεται στο internet δεν ισχύει.

Από τη μια πλευρά η χρήση του διαδικτύου είναι δικαίωμα, και από την άλλη είναι επίσης δικαίωμα του χρήστη να προστατεύεται από κακόβουλες ενέργειες στο διαδίκτυο. Στη σημερινή κοινωνία, τα ηλεκτρονικά εγκλήματα αποτελούν τον υπ' αριθμόν ένα κίνδυνο για τους χρήστες. Το χακάρισμα προσωπικών λογαριασμών, η κλοπή προσωπικών στοιχείων και οι ιοί που λαμβάνονται

μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ορισμένα μόνο από τα συνηθισμένα εγκλήματα που λαμβάνουν χώρα στο διαδίκτυο.

Κάποια από τα κυβερνοεγκλήματα, χαρακτηρίζονται από τους ειδικούς και από την αστυνομία ως σοβαρότερα από τα αντίστοιχα εγκλήματα στην πραγματική ζωή. Συγκεκριμένα, υπάρχει μεγάλη διαφορά ανάμεσα σε έναν τσαντάκια και σε κάποιον χάκερ που εισβάλλει σε προσωπικούς λογαριασμούς τραπέζης και αφαιρεί χρηματικά ποσά. Όπως επίσης, υπάρχει διαφορά ανάμεσα στο ψηφιακό bullying και στον κλασικό εκφοβισμό. Αυτό που διαφοροποιεί τις δύο αυτές περιπτώσεις είναι η ανωνυμία που προστατεύει τον δράστη και η μη άμεση επαφή με το θύμα. Είναι, επιπλέον, σοβαρότερο γιατί συνήθως προκαλείται μεγαλύτερης έκτασης ζημιά. Τα κακόβουλα μηνύματα, οι υποκλοπές και η παραβίαση προσωπικών δεδομένων πραγματοποιούνται γρήγορα και «ταξιδεύουν» σε μακρινές αποστάσεις, εύκολα και ανέξοδα. Εξάλλου, όσο αφορά το cyber bullying με το διαδίκτυο είναι πολύ πιο εύκολο να εξαπλωθεί μια πληροφορία και να διαδοθούν ταπεινωτικές φήμες για κάποιον.

Η Αρχή Προστασίας Προσωπικών Δεδομένων έχει αναρτήσει εργαλεία για επαγγελματίες και το κοινό, που αφορούν την προστασία και την ασφαλή πλοήγηση, τα οποία είναι εύκολα προσβάσιμα από την ιστοσελίδα της. Βέβαια, η ανωνυμία που αναφέρθηκε παραπάνω, και η μη ιδιωτικότητα δυσκολεύουν την εφαρμογή των νόμων περί διαδικτύου και κατ' επέκταση και την προστασία των θυμάτων.

Δεδομένου ότι το διαδίκτυο μπορεί να συμβάλει αρκετά στον τομέα της στοχευμένης πρόληψης σε ένα κομμάτι του πληθυσμού, ειδικά για άτομα τα οποία δυσκολεύονται στη συμβατική πρόσβασή τους σε υπηρεσίες συμβουλευτικής, κρίνεται ως μεγάλης σημασίας να στηριχθούν online παρεμβάσεις, σε ξεχωριστές σελίδες ή ακόμα και μέσα στις ίδιες τις εφαρμογές (παιχνίδια, σελίδες κοινωνικής δικτύωσης). Με αυτόν τον τρόπο εξασφαλίζεται και η προσέγγιση ατόμων τα οποία παρουσιάζουν εθισμό στο διαδίκτυο.

Το γενικότερο συμπέρασμα που βγαίνει, επομένως, με βάση όλα τα παραπάνω είναι ότι η γνώση και η ενημέρωση είναι τα δύο σημαντικότερα όπλα των χρηστών για πρόληψη και αντιμετώπιση εγκλημάτων που τελούνται στο διαδίκτυο. Τα άτομα που γνωρίζουν πως πρέπει να προφυλαχτούν, δεν αντιμετωπίζουν κινδύνους κατά την πλοήγησή τους στο διαδίκτυο και επομένως μπορούν να απολαύσουν όλα τα θετικά που αυτό προσφέρει.

7.2. ΑΞΙΟΛΟΓΗΣΗ

Επιχειρώντας μια αυτοαξιολόγηση της παρούσας πτυχιακής εργασίας, θα πρέπει να ειπωθεί ότι καλύφθηκε πλήρως και αναπτύχθηκε επαρκώς το θέμα της έρευνας. Η δομή της εργασίας είναι άκρως ικανοποιητική, καθώς ο τρόπος που διαιρέθηκαν τα κεφάλαια συμβάλει άριστα στην ευκολότερη μελέτη των επιμέρους θεμάτων. Τέλος, τα συμπεράσματα της έρευνας, κάποια από τα οποία βασίστηκαν σε βιβλιογραφική μελέτη και κάποια άλλα σε απλή παράθεση προσωπικής γνώμης, μπορούν να χαρακτηριστούν ιδιαιτέρως χρήσιμα.

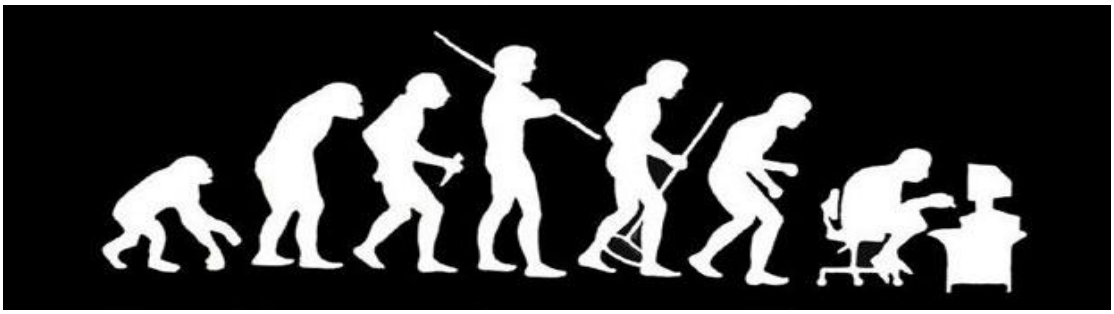
ΒΙΒΛΙΟΓΡΑΦΙΑ

1. **Εθισμός, [2013, Δεκέμβριος] [online]: www.inpsyche.gr**
2. **Β' τάξη 2ου ΓΕΛ Σερρών, Ερευνητική Εργασία για τον Εθισμό στο διαδίκτυο, [2012-2013] [online]: http://netaddiction.site90.net/**
3. **Α' τάξη 2ου ΓΕΛ Αλίμου, Διαδίκτυο, [2014-2015] [online]: http://diadiktio.wikispaces.com/**
4. **Χριστίνα Ιωάννου, Εθισμός-Διαδίκτυο-Πρόληψη, [2015, Ιούνιος 02] [online]: http://www.paidiatros.com/efivos/psyxologia/internet-use-abuse-addiction**
5. **Θ. Τσώλη, Εθισμός στο Internet, [2008, Νοέμβριος 30] [online]: http://www.tovima.gr/science/article/?aid=244780#ixzz0oGBQhNit**
6. **Διαδίκτυο, Ορισμός, [online]: https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF**
7. **Πλοήγηση στο διαδίκτυο, Έγκλημα, [2015, Φεβρουάριος 18] [online]: www.e-crime.gr**
8. **Γ. Κόκουβα, Εθισμός στο διαδίκτυο, e-εξάρτηση, [2012, Αύγουστος 28] [online]: www.in2life.gr/everyday/modernlife/article/241932/ethismos-sto-diadiktyo-eho-pathei-e-xarthsh.html**
9. **Συνέδριο « Έρευνα, πρόληψη και αντιμετώπιση των κινδύνων στη χρήση του Διαδικτύου», 2009, [online]: www.hasiad.gr/index.php/index.php?option=com_content&view=article&id=31%3A2011-04-09-13-42-03&catid=1&Itemid=21&lang=el**
10. **Φίλτρα προστασίας, [2007, Σεπτέμβριος 10] [online]: www.ethnos.gr/article.asp?catid=22733&subid=2&pubid=131453**
11. **Ηλεκτρονικό Έγκλημα, [online]: www.astynomia.gr**
12. **ΚΕ Σιώμος-ΝΒ Αγγελόπουλος, Διαταραχή εθισμού στο διαδίκτυο, Ψυχιατρική,[2008] [online]: http://www.psych.gr/documents/psychiatry/19.1-GR-2008-52.pdf**
13. **Σιώμος ΚΕ-Μουζάς Ο- Σκεντέρης Ν-Θεοδώρου Κ-Αγγελόπουλος ΝΒ, Χαρακτηριστικά και τρόπος ζωής των εθισμένων στο διαδίκτυο Ελλήνων εφήβων μαθητών, Ψυχιατρική, [2008, Μάιος]**
14. **Σιώμος ΚΕ, Εθισμός των εφήβων στους Η/Υ και το διαδίκτυο: Ψυχιατρικά συμπτώματα και διαταραχές ύπνου, Διδακτορική Διατριβή, Ιατρική Σχολή, Πανεπιστήμιο Θεσσαλίας [2008][online]: http://thesis.ekt.gr/thesisBookReader/id/26207#page/1/mode/2up**
15. **ΚΕ Σιώμος-ΓΔ Φλώρος-ΟΔ Μουζάς-ΝΒ Αγγελόπουλος, Στάθμιση κλίμακας μέτρησης του εθισμού των εφήβων στους Ηλεκτρονικούς Υπολογιστές, Ψυχιατρική [2009] [online]: http://www.psych.gr/documents/psychiatry/20.3-GR-2009-222.pdf**
16. **Σιώμος Κ. , Σφακιανάκης Ε. , Φλώρος Γ. , Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου, Εκδόσεις Λιβάνη, [2012]**
17. **Κ Σιώμος, Γ Φλώρος, Το Διαδίκτυο ως παράγοντας ενίσχυσης των ψυχιατρικών συμπτωμάτων σε εφήβους μαθητές. Αναρτημένη ανακοίνωση στο 6ο Πανελλήνιο Παιδοψυχιατρικό Συνέδριο, [2009, Μάιος 15-17]**
18. **Γατσάς Βασίλης, Κίνδυνοι στο Ίντερνετ - Εγκλήματα στο Διαδίκτυο [online]: http://www.psixologikosfaros.gr/article_det.asp?artid=4777**
19. **Μονάδα Απεξάρτησης 18 ΑΝΩ, Ψυχιατρικό Νοσοκομείο Αττικής [online]: http://www.18ano.gr/internet.html**

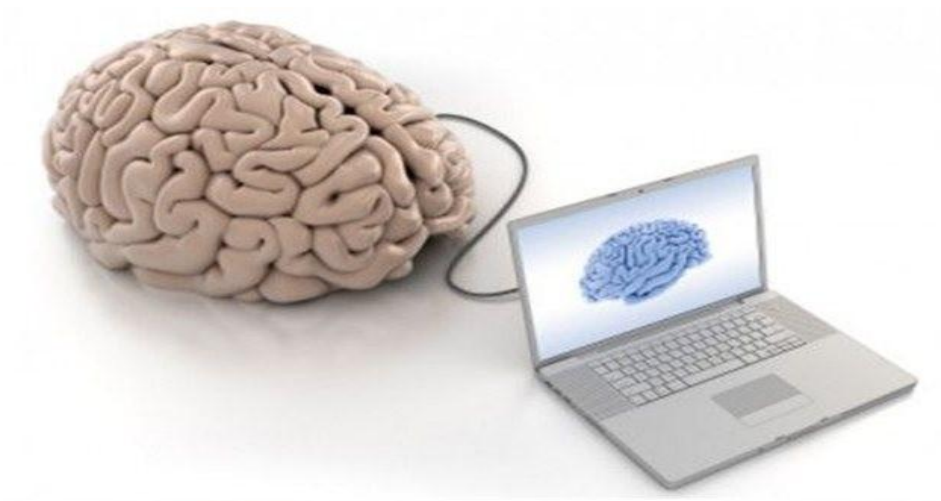
20. **Διασπορά κακόβουλου λογισμικού μέσω του διαδικτύου, [2015, Φεβρουάριος 14] [online]: http://www.mylefkada.gr/alles-eidiseis/diaspora-kakovoulou-logismikou-meso-tou-diadiktiou-51389/**
21. **Εξάρτηση, [2011, Μάιος 07] [online]: http://eprl.korinthos.uop.gr/BlogsPortal/group11/category**
22. **Αγγούσης Ιωάννης, Το ηλεκτρονικό έγκλημα με έμφαση στο οικονομικό-ηλεκτρονικό έγκλημα, [2008]**
23. **Lion Hearts Point Of View, Internet-Ηλεκτρονικό Έγκλημα-Δίωξη Ηλεκτρονικού Εγκλήματος, [2007, Αύγουστος 27] [online]: http://dide.flo.sch.gr/Plinet/Tutorials/Internet-ElectronicCrime-LionHeart.pdf**
24. **Στούρη Βασιλική, Έγκλημα στο διαδίκτυο-Εναλλακτικοί τρόποι εκδήλωσης, Αντιμετώπισης και Διεύρυνσης τους, [2010 Ιούλιος] [online]: http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4093/1/Stouri.pdf**
25. **Συμβουλές της Δίωξης Ηλεκτρονικού Εγκλήματος για μηνύματα-παγίδες στο διαδίκτυο, [2014, Αύγουστος 18] [online]: http://www.aftodioikisi.gr/ipourgeia/simvoules-tis-dioxis-ilektronikou-egklimatos-gia-minimata-pagides-sto-diadiktio**
26. **Η ψηφιακή εγκληματικότητα στο πλαίσιο της καθημερινής δραστηριότητας, [online]: http://www.dikseo.teimes.gr/spoudastirio/**

ΠΑΡΑΡΤΗΜΑ

ΕΙΚΟΝΕΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ



Εικόνα 1 Η εξέλιξη του ανθρώπου, με βάση τα δεδομένα της σύγχρονης εποχής της Πληροφορικής και της Τεχνολογίας.

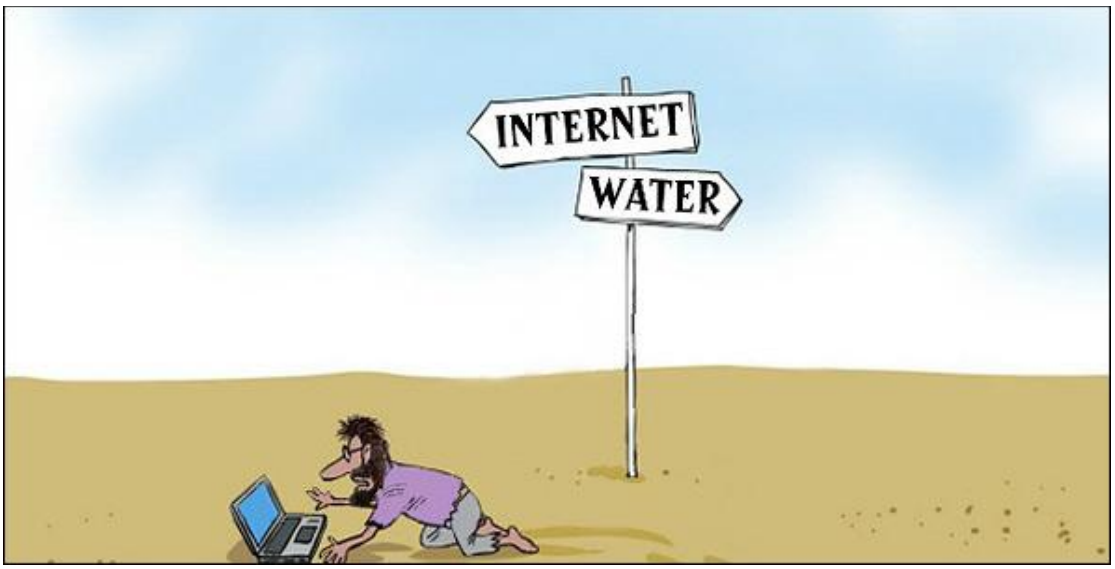


Εικόνα 2 Ο σημερινός άνθρωπος χρησιμοποιεί έναν άλλον τρόπο σκέψης και λειτουργίας, για όλες τις δραστηριότητές του, ο οποίος συνδέεται άμεσα με τη λειτουργία του ηλεκτρονικού υπολογιστή και του διαδικτύου.

Εικόνα 3 Ο Εθισμός στο διαδίκτυο απασχολεί πλέον ένα αρκετά μεγάλο κομμάτι των παιδιών και εφήβων.

Εικόνα 4 Τα μέσα κοινωνικής δικτύωσης καθώς και άλλες εφαρμογές του διαδικτύου, παίρνουν τη μορφή ενέσιμης δόσης για τον εθισμένο χρήστη.

Εικόνα 5 Η ταυτοποίηση των προσωπικών δεδομένων του χρήστη μέσω διαδικτύου, αποτελεί ένα από τα ισχυρότερα όπλα του «κυβερνοεγκλήματος».



Εικόνα 6 Η ανάγκη του σύγχρονου ανθρώπου για σύνδεση στο διαδίκτυο, φαίνεται να αφήνει πίσω άλλες πιο σημαντικές προσωπικές ανάγκες.

Εικόνα 7 Ο εθισμένος χρήστης του διαδικτύου αρχίζει να έχει όμοια χαρακτηριστικά με αυτά ενός φυλακισμένου στην πραγματική ζωή.

Εικόνα 8 Η προστασία των νέων από τον εθισμό στο διαδίκτυο καθώς και η διαπαιδαγώγησή τους για σωστή χρήση του μέσου αυτού, αποτελούν κύριο μέλημα για τους ειδικούς.

Εικόνα 9 Στα πλαίσια της ορθής χρήσης του διαδικτύου, περιλαμβάνεται η γνώση των κινδύνων που κρύβει αυτό, όπως και η προστασία από κάθε είδους διαδικτυακό έγκλημα.

Εικόνα 10 Οι χάκερς χρησιμοποιούν κακόβουλο λογισμικό για να πλήξουν τον υπολογιστή του χρήστη, με στόχο την αλίευση προσωπικών του κωδικών, και απώτερο σκοπό το κέρδος.

Εικόνα 11 Τα εγκλήματα μέσω διαδικτύου αποτελούν σήμερα την πιο συχνή, εύκολη, ανέξοδη και ασφαλής μορφή εγκλημάτων.

Εικόνα 12 Η ανωνυμία που προσφέρει το διαδίκτυο μπορεί να φέρει τον χρήστη σε δύσκολη θέση και να τον οδηγήσει σε καταστάσεις ψυχολογικής πίεσης και εκφοβισμού.