Τεχνολογικο Εκπαιδευτικο Ιδρυμα Πελοποννησου
Σχολη Τεχνολογικων Εφαρμογων
Τμημα Μηχανικων Πληροφορικης Τ.Ε.

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Πτυχιακη Εργασια

του

ΒΑΣΙΛΕΙΟΥ Π. ΜΑΥΡΙΑ

Επιβλέπουσα: Ελένη Κουτσούκου

Σπάρτη, Νοέμβριος 2015

Τεχνολογικο Εκπαιδευτικο Ιδρυμα Πελοποννησου
Σχολη Τεχνολογικων Εφαρμογων
Τμημα Μηχανικων Πληροφορικης Τ.Ε.

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Πτυχιακη Εργασια

του

ΒΑΣΙΛΕΙΟΥ Π. ΜΑΥΡΙΑ

Επιβλέπουσα: Ελένη Κουτσούκου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την .....

(Υπογραφή) *(Υπογραφή)* *(Υπογραφή)*

....

Σπάρτη, Νοέμβριος 2015

Τεχνολογικο Εκπαιδευτικο Ιδρυμα Πελοποννησου
Σχολη Τεχνολογικων Εφαρμογων
Τμημα Μηχανικων Πληροφορικης Τ.Ε.

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.
(Υπογραφή)

.....
Βασίλειος Μαυριάς

Περίληψη

Ο ηλεκτρονικός υπολογιστής στην σημερινή εποχή αποτελεί ένα αναπόσπαστο κομμάτι της καθημερινότητάς μας. Καθημερινά πολλοί είναι οι χρήστες του διαδικτύου και πολλοί πέφτουν θύματα κάποιου είδους ηλεκτρονικού εγκλήματος. Στην εργασία αυτή παρουσιάζεται η θεωρητική μελέτη που πρέπει να γνωρίζεται για το ηλεκτρονικό έγκλημα. Αυτό περιλαμβάνει τον ορισμό του ηλεκτρονικού εγκλήματος και τα χαρακτηριστικά του, τις μορφές κυβερνοεγκλήματος και τους τρόπους αντιμετώπισής του. Επίσης αναλύεται η συμβολή της δίωξης ηλεκτρονικού εγκλήματος στην αντιμετώπισή του και παραθέτονται συμβουλές για την ασφάλεια και την προστασία των παιδιών στο διαδίκτυο. Επιπροσθέτως παρουσιάζεται η εφαρμογή cyberkid της ελληνικής αστυνομίας μέσω της οποίας ενημερώνονται καθημερινά οι χρήστες του διαδικτύου για την ασφαλή πλοήγησή τους στο διαδίκτυο και πού πρέπει να απευθυνθούν σε περίπτωση παραβίασης της ιδιωτικότητάς τους.

Λέξεις Κλειδιά

Ασφάλεια στο Διαδίκτυο, Δίωξη Ηλεκτρονικού Εγκλήματος, Ηλεκτρονικό Έγκλημα, Ιδιωτικότητα.

Abstract

The computer in the current season constitutes a integral piece of everyday routine. Daily many are the users of internet and many fell victims of some type of electronic crime. In this project is presented the theoretical report that must be known for the electronic crime. This includes the definition of electronic crime and his characteristics, the forms of cybercrime and his ways of confrontation. Also is analyzed the contribution of prosecution of electronic crime in his confrontation and mentioned advices for the safety and the protection of children in the internet. In addition, it is presented the application Cyberkid of Greek police which are informed daily internet users about safe surfing on the Internet and where to go in case of violation of their privacy.

Keywords

Cyber Crime, Cyberkid, Electronic Crime, Internet Security, Privacy.

στους γονείς μου

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω την καθηγήτριά μου κ. Ελένη Κουτσούκου για την επίβλεψη αυτής της πτυχιακής εργασίας και για τα εποικοδομητικά σχόλια που μου έδωσε για την συγγραφή της. Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική συμπαράσταση που μου προσέφεραν όλα αυτά τα χρόνια.

Τρίπολη, Μάιος 2015

Βασίλειος Μαυριάς

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Εικόνων

1.1 Ιστορική Αναδρομή

Ο όρος *ηλεκτρονικό έγκλημα* [3] έχει να κάνει με όλες εκείνες τις εγκληματικές πράξεις που γίνονται είτε με την χρήση ηλεκτρονικών υπολογιστών, είτε με την χρήση συστημάτων επεξεργασίας δεδομένων και τιμωρούνται σύμφωνα με τον νόμο. Διαχωρίζονται σε δύο κατηγορίες ανάλογα με τον τρόπο που έχουν διαπραχθεί: α) Εγκλήματα με την χρήση ηλεκτρονικών υπολογιστών (computer crime), β) Κυβερνοεγκλήματα τα οποία έχουν διαπραχθεί μέσω του διαδικτύου (cyber crime).

Στις αρχές της δεκαετίας του 1980 είχαμε την έλευση του πρωτοκόλλου X.25 [1] σύμφωνα με το οποίο οι υπολογιστές της εποχής εκείνης είχαν την δυνατότητα μέσω μιας συσκευής (modem) καθώς και με το ανάλογο δίκτυο να επικοινωνούν μεταξύ τους. Έπειτα άρχισαν να μοιράζονται πληροφορίες μέσω των λεγομένων BBSs (Bulletin Board Service).[2] Η διαδικασία ήταν απλή: γινόταν ένα τηλεφώνημα από το modem σε έναν συγκεκριμένο αριθμό. Απαντούσε το modem του άλλου υπολογιστή και γινόταν η σύνδεση. Έπειτα όταν ο χρήστης είχε συνδεθεί στην BBSs μπορούσε να κατεβάσει, να διαβάσει αλλά και να ανεβάσει οτιδήποτε πληροφορίες ήθελε. Αυτές τις υπηρεσίες τις χρησιμοποιούσαν μερικά πανεπιστήμια, διάφορες εμπορικές εταιρείες αλλά και πολλοί ιδιώτες.

Καθώς κατά τα έτη 1983 -1985 τα μέτρα ασφαλείας είχανε πολλές ελλείψεις εμφανίστηκαν και οι πρώτες επιθέσεις που είχαν σκοπό την πρόκληση ζημιών στα συστήματα των πανεπιστημίων. Το 1989 γίνεται σε Πανευρωπαϊκό επίπεδο η πρώτη προσπάθεια για να αντιμετωπιστούν νομικά τα ηλεκτρονικά εγκλήματα.

Στο δεύτερο μισό της δεκαετίας του '90 εμφανίζεται ένας ιός ο οποίος προσβάλλει μη εκτελέσιμα αρχεία, όπως π.χ. αρχεία κειμένου. Ο ιός αυτός έγινε γνωστός με το όνομα Melissa. Προκάλεσε πάρα πολλές ζημιές που κόστισαν εκατομμύρια δολάρια σε πάρα πολλά υπολογιστικά συστήματα σε παγκόσμιο επίπεδο.

1.2 Ορισμός Εγκλήματος

Με τον όρο *έγκλημα* εννοούμε μία πράξη άδικη η οποία τιμωρείται σύμφωνα με τον νόμο. Υπάρχουν πολλά είδη εγκλημάτων, ένα από αυτά είναι και το *ηλεκτρονικό έγκλημα*. Κύριο στοιχείο του *ηλεκτρονικού εγκλήματος* αποτελεί ο ηλεκτρονικός υπολογιστής μέσω του οποίου διαπράττονται πάρα πολλά εγκλήματα στην σημερινή εποχή. Τα εγκλήματα στον κυβερνοχώρο [4] διαπράττονται πολύ γρήγορα αλλά απαιτούνται εξειδικευμένες γνώσεις.

[1] Υποστηρίζει επικοινωνία με σύνδεση, έπρεπε να αντιμετωπίσει τους υψηλούς ρυθμούς λαθών εκείνης της εποχής. Ενσωματώνει μηχανισμούς ανίχνευσης και διόρθωσης λαθών οι οποίοι καθυστερούν την επικοινωνία. Στόχος του είναι η επικοινωνία με συστήματα διαφορετικής ταχύτητας αλλά επιβαρύνεται σημαντικά η λειτουργία του δικτύου. Χρησιμοποιείται για χαμηλές απαιτήσεις ασύγχρονες εφαρμογές πολυμέσων και έχει σταματήσει η εξέλιξή της.

[2] Είναι ένας server που χρησιμοποιεί λογισμικό και επιτρέπει στους χρήστες να συνδέονται στο σύστημα χρησιμοποιώντας ένα πρόγραμμα τερματικού. Μόλις συνδεθεί ο χρήστης μπορεί να πραγματοποιήσει αποστολή και λήψη λογισμικού και δεδομένων. Εκτιμάτε ότι υπήρχαν 60.000 συστήματα BBSs από τις αρχές της δεκαετίας του 1990 που εξυπηρετούσαν 17 εκατομμύρια χρήστες μόνο στις ΗΠΑ το 1994.

Μπορούν να πραγματοποιηθούν από οποιοδήποτε μέρος χωρίς να χρειάζεται να μετακινηθεί ο δράστης.

1.3 Ορισμός Κυβερνοεγκλήματος

Με τον όρο *κυβερνοέγκλημα* [5] εννοούμε το έγκλημα εκείνο το οποίο ο δράστης χρησιμοποιεί εξειδικευμένες γνώσεις μέσα από τον κυβερνοχώρο. Σύμφωνα με τον Donn Parker [6] ο οποίος είναι βετεράνος ασφαλείας με πάνω από τριάντα έτη πείρα στα ηλεκτρονικά εγκλήματα διαχωρίζει το ηλεκτρονικό έγκλημα από το κυβερνοέγκλημα θεωρώντας πώς το *κυβερνοέγκλημα* απαιτεί ειδικές γνώσεις πάνω στην τεχνολογία των υπολογιστών.

1.4 Χαρακτηριστικά Ηλεκτρονικού Εγκλήματος

Το *ηλεκτρουικό έγκλημα* [7] περιέχει ορισμένα χαρακτηριστικά γνωρίσματα τα οποία το ξεχωρίζουν από το παραδοσιακό έγκλημα. **α)** Η τέλεση του εγκλήματος πραγματοποιείται σε γρήγορο χρόνο. **β)** Οι ηλεκτρονικοί εγκληματίες δεν εμφανίζουν την κανονική τους ταυτότητα αλλά στέλνουν ορισμένα ηλεκτρονικά μηνύματα (e-mails) με ψεύτικα στοιχεία. **γ)** Δύσκολα αλλά όχι ακατόρθωτα μπορεί να εντοπιστεί ο δράστης. **δ)** Η διερεύνησή του είναι αρκετά δύσκολη και χρειάζεται άρτια εξειδικευμένο προσωπικό. **ε)** Χρειάζεται συνεργασία τουλάχιστον δύο κρατών έτσι ώστε να ανταλλάσσουν στοιχεία για να ανακαλύψουν τους πραγματικούς δράστες. **στ)** Χαρακτηρίζεται ως έγκλημα χωρίς πατρίδα παρόλο που οι επιπτώσεις που δημιουργεί μπορούν να γίνουν αισθητές σε πολλούς στόχους. **ζ)** Πάρα πολύ λίγες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται όχι μόνο στον ελληνικό αλλά και στον διεθνή χώρο. Αυτό συμβαίνει διότι πάρα πολλά από τα εγκλήματα αφορούν εταιρείες οι οποίες δεν θέλουν να φανούν αναξιόπιστες στην κοινωνία.

1.5 Μορφές Ηλεκτρονικού Εγκλήματος

Οι μορφές ηλεκτρονικού εγκλήματος [8] στην σημερινή εποχή όπου έχουμε συνεχή ανάπτυξη της τεχνολογίας των υπολογιστών είναι πάρα πολλές. Μπορούμε να τις χωρίσουμε στις παρακάτω κατηγορίες:

1.5.1 Κακόβουλο Λογισμικό

Το *κακόβουλο λογισμικό* αποτελεί ένα σημαντικό πρόβλημα στον τομέα της ασφάλειας πληροφοριακών συστημάτων. Χαρακτηρίζεται ως κακόβουλο όταν έχει δημιουργηθεί κατά τέτοιο τρόπο έτσι ώστε να βλάψει κάποιο υπολογιστικό σύστημα. Το λογισμικό αυτό διακρίνεται στις παρακάτω κατηγορίες:

1. **Ιός (virus)**
   Ένας ιός είναι ένα κακόβουλο λογισμικό το οποίο εξαπλώνεται γρήγορα μέσα σε χρήσιμα προγράμματα ενός ξένου υπολογιστή. Έχει την δυνατότητα να αντιγράφει αλλά και να μολύνει τα αρχεία του υπολογιστή χωρίς την γνώση του χρήστη. Μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους υπολογιστές μέσω του διαδικτύου, τοπικού δίσκου ή

με την μεταφορά κάποιον αρχείων με έναν οπτικό δίσκο ή με κάποιο άλλο φορητό μέσο αποθήκευσης όπως π.χ. (μία δισκέτα, ένα Usb Flash Drive, ένας εξωτερικός σκληρός δίσκος). Ένας ιός μπορεί να δημιουργήσει αρκετά προβλήματα σε έναν υπολογιστή. Αρχικά μπορεί να αρχίσει να διαγράφει αρχεία από τον υπολογιστή. Θα επιβαρύνει σημαντικά την λειτουργία του συστήματος, ο υπολογιστής θα αργεί να ανοίξει ή και να φορτώσει κάποιο πρόγραμμα. Πιθανόν να οδηγήσει και σε κατάρρευση ολόκληρου του συστήματος. Ο πρώτος ιός που πρωτοεμφανίστηκε στους ηλεκτρονικούς υπολογιστές ήταν ο ιός Brain [9] ο οποίος δημιουργήθηκε το 1986 και προσέβαλε τον τομέα εκκίνησης του σκληρού δίσκου. Οι περισσότεροι ιοί έχουν γραφτεί για λειτουργικά συστήματα (Windows) διότι χρησιμοποιούνται από εκατοντάδες χρήστες σε ολόκληρο τον πλανήτη και επίσης διότι παρουσιάζουν αρκετά κενά ασφαλείας.

2. **Δούρειος Ίππος (trojan)**

   Ο Δούρειος Ίππος αποτελεί ένα κακόβουλο πρόγραμμα το οποίο δημιουργεί την εντύπωση στον χρήστη ενός υπολογιστή ότι εκτελεί κάποια χρήσιμη λειτουργία του συστήματος ενώ παράλληλα εγκαθιστά χωρίς να το γνωρίζει ο χρήστης άλλα προγράμματα στον υπολογιστή. Η ονομασία του *δούρειος ίππος* προέρχεται από την Ιλιάδα του Ομήρου όπου ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου για να καταφέρει να εισέλθει στην Τροία. Στην τεχνολογία των υπολογιστών ο όρος *δούρειος ίππος* χρησιμοποιήθηκε αρχικά από τον Κεν Τόμσον σε ομιλία του το 1983. Παρατήρησε ότι με την εντολή login του Unix [10] μπορεί να γίνει υποκλοπή κωδικών πρόσβασης. Την ανακάλυψη αυτή την ονόμασε *δούρειο ίππο*. Υποστήριξε ακόμη ότι σε οποιονδήποτε μεταγλωττιστή[3] σε γλώσσα C [11] μπορεί να προστεθεί κακόβουλος κώδικας. Με αυτόν τον τρόπο θα γίνει ακόμα πιο δύσκολος ο εντοπισμός του κακόβουλου κώδικα.

   Χωρίζονται σε δύο κύριες κατηγορίες: α) Στην πρώτη κατηγορία εντάσσονται οι δούρειοι ίπποι οι οποίοι αποτελούνται από κανονικά προγράμματα μέσα από τα οποία μπορούν διάφοροι χάκερ[4] να προσθέσουν *κακόβουλο κώδικα*. β) Η δεύτερη κατηγορία περιλαμβάνει μεμονωμένα προγράμματα τα οποία ξεγελούν τους χρήστες και τους προτρέπουν να εκτελέσουν κάποιο αρχείο το οποίο όμως θα μολύνει έπειτα τον υπολογιστή χωρίς να το γνωρίζουν π.χ. (οι διάφορες κινούμενες εικόνες που παρουσιάζουν είτε κάποιο παιχνίδι, είτε κάποια διαφήμιση και υπάρχουν σε πολλές ιστοσελίδες στο διαδίκτυο).

3. **Σκουλήκι (worm)**

   Ένα σκουλήκι (worm) είναι ένα κακόβουλο πρόγραμμα το οποίο διαδίδεται από υπολογιστή σε υπολογιστή. Χρησιμοποιεί δηλαδή ένα δίκτυο υπολογιστών μέσω του οποίου στέλνει αντίγραφα του εαυτού του σε άλλους υπολογιστές χωρίς να το γνωρίζουν οι χρήστες. Μεταδίδεται με τον εξής τρόπο: Με την αποστολή ενός e - mail το οποίο περιέχει κάποιο συνημμένο αρχείο το οποίο είναι μολυσμένο. Μόλις ανοιχτεί

[3] Μεταγλωττιστής ή αλλιώς μεταφραστής λέγεται ένα πρόγραμμα το οποίο μετατρέπει το κείμενο μιας γλώσσας προγραμματισμού σε μία άλλη γλώσσα προγραμματισμού. Περιλαμβάνει τις εξής λειτουργίες: α) λεκτική ανάλυση, β) συντακτική ανάλυση, γ) παραγωγή κώδικα, δ) βελτιστοποίηση κώδικα.

[4] Είναι το άτομο εκείνο το οποίο προσπαθεί να εισβάλει μέσα σε υπολογιστικά συστήματα και να υποκλέψει δεδομένα. Έχει τις κατάλληλες γνώσεις και μπορεί να διαχειρίζεται πλήθος υπολογιστικών συστημάτων.

το αρχείο προσθέτει έναν βλαβερό κώδικα σε όλα τα αρχεία που βρίσκει μέσα στον υπολογιστή. Οι ζημιές όμως που θα προκαλέσει εξαρτώνται από τον τρόπο που δρα το σκουλήκι. Μπορούν να αρχίσουν να μετατρέπουν τα αρχεία ενός υπολογιστή αλλά μπορούν να πραγματοποιήσουν την καταστροφή και την διαγραφή ολόκληρων των αρχείων του Η/Υ.

1.5.2 Ανεπιθύμητη Αλληλογραφία

Με τον όρο *ανεπιθύμητη αλληλογραφία* (spam) ορίζουμε την μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε πάρα πολλούς αποδέκτες. Κύριος λόγος ύπαρξης της *ανεπιθύμητης αλληλογραφίας* είναι η εξοικονόμηση χρημάτων. Μέσω του διαδικτύου βρίσκουν από τους καταλόγους των εταιρειών αλλά και από δωμάτια συζητήσεων (chat rooms) πάρα πολλές ηλεκτρονικές διευθύνσεις στις οποίες στέλνουν διάφοροι επιτήδειοι πάρα πολλά (e - mails) τα οποία στοχεύουν στην αποκομιδή κέρδους. Από την στιγμή που θα δούμε ότι κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου έχει καταχωρηθεί ως (spam) πρέπει να το διαγράψουμε από τον υπολογιστή μας για να μην το μπερδέψουμε με την αλληλογραφία μας και το ανοίξουμε. Σε καμία περίπτωση δεν πρέπει να απαντήσουμε σε κάποιο τέτοιο μήνυμα διότι με αυτόν τον τρόπο θα αποκαλύψουμε στους ηλεκτρονικούς εγκληματίες ότι η ηλεκτρονική μας διεύθυνση είναι ενεργή. Παρατηρούμε ακόμη ότι η πρακτική του (spamming) εμφανίζεται και σε άλλες περιπτώσεις ηλεκτρονικής επικοινωνίας όπως: α) σε μηνύματα που στέλνονται μέσω κινητής τηλεφωνίας π.χ. (SMS, MMS), β) στις υπηρεσίες fax, γ) σε διάφορες ηλεκτρονικές υπηρεσίες ανταλλαγής μηνυμάτων όπως π.χ. Facebook, Twitter.

1.5.3 Ηλεκτρονική Πειρατεία

Με τον όρο ηλεκτρονική πειρατεία *(hacking)* εννοούμε τη μη εξουσιοδοτημένη πρόσβαση σε συστήματα ηλεκτρονικού υπολογιστή σκοπός της οποίας είναι η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας αλλά και η επιβεβαίωση των δεξιοτήτων τους ότι μπορούν να εισβάλλουν σε κάποιο υπολογιστικό σύστημα.[5] Η εισβολή σε κάποιο δίκτυο εμπεριέχει κακόβουλο χαρακτήρα διότι ο επιτιθέμενος η αλλιώς (hacker) αφού εισβάλλει στο σύστημα αποκτά γνώσεις για αυτό, εντοπίζει κάποια αδύνατα σημεία του συστήματος, ορισμένα κενά ασφαλείας και έτσι μπορεί στην συνέχεια να διαπράξει κάποια κακόβουλη επίθεση ή να δώσει τις πληροφορίες σε κάποιο άλλο πρόσωπο για να διαπράξει αυτό την επίθεση. Υπάρχουν ορισμένες τεχνικές που χρησιμοποιούν για την είσοδό τους σε ένα υπολογιστικό σύστημα.

1. **Εκμετάλλευση των Cookies**
   Τα cookies είναι κάποια μικρά αρχεία κειμένου τα οποία αποθηκεύονται σε κάθε Η/Υ από τις δικτυακές τοποθεσίες που επισκέπτεται ένας χρήστης. Τα αρχεία αυτά περιέχουν πολλές πληροφορίες όπως π.χ. προσωπικά στοιχεία του χρήστη, τις δραστηριότητές του, τις συνήθειές του κ.λπ. Όταν σε ένα αρχείο cookie περιέχονται

[5]Υπολογιστικό σύστημα λέγεται μία ολοκληρωμένη υπολογιστική συσκευή. Αυτό περιλαμβάνει και το υλικό και το λογισμικό της. Αναφέρεται σε υπερυπολογιστή ο οποίος διαφέρει πολύ από τους υπολογιστές που χρησιμοποιούν οι απλοί χρήστες λόγω των υπολογισμών που μπορεί να εκτελέσει ανά δευτερόλεπτο, αλλά και σε έναν κεντρικό υπολογιστή οι οποίοι είναι μια κατηγορία υπολογιστών που χρησιμοποιούνται από μεγάλες εταιρείες για την δημιουργία κρίσιμων εφαρμογών όπως π.χ. η μαζική επεξεργασία των συναλλαγών.

πληροφορίες όπως κάποιο όνομα χρήστη (username) και κάποιος κωδικός (password) για μια υπηρεσία ο επιτιθέμενος έχει την δυνατότητα αφού αρχικά έχει εντοπίσει τις αστάθειες του συστήματος να ανακτήσει αυτές τις πληροφορίες και να προκαλέσει την ζημιά που θέλει.

2. **Ανίχνευση Δικτυακών Υπηρεσιών Συστημάτων**
   Σε αυτή την περίπτωση ο επιτιθέμενος εντοπίζει πληροφορίες για το σύστημα στο οποίο θέλει να επιτεθεί. Χρησιμοποιεί την τεχνική σάρωσης των θυρών (port scanning) μέσω τις οποίας γίνεται μία έρευνα των θυρών ενός υπολογιστή. Εφόσον από κάποια θύρα port εισέρχονται και εξέρχονται διάφορες πληροφορίες στο σύστημα το port scanning αναγνωρίζει τις ανοικτές θύρες ενός υπολογιστή. Έτσι ο επιτιθέμενος μπορεί να εισβάλλει στο σύστημα και να δημιουργήσει προβλήματα στον χρήστη του Η/Υ. Υπάρχουν διάφορα προγράμματα λογισμικού μέσω των οποίων μπορούν οι χρήστες ενός υπολογιστή να ενημερωθούν εάν έχει γίνει κάποια απόπειρα πρόσβασης μέσω κάποιας θύρας στον ηλεκτρονικό τους υπολογιστή. Σε περίπτωση κάποιας επίθεσης στο σύστημα προειδοποιούν τον χρήστη και καταγράφουν την διεύθυνση με την οποία ήταν συνδεδεμένος ο επιτιθέμενος.

3. **Ανίχνευση Δικτυακών Πακέτων**
   Υπάρχουν ορισμένες εφαρμογές λογισμικού που ονομάζονται packet sniffers [12] σύμφωνα με τις οποίες δίνεται η δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Η εφαρμογή αυτή εντοπίζει όλα τα πακέτα που κυκλοφορούν στο διαδίκτυο. Εάν σε κάποιο από τα πακέτα δεν έχει γίνει κρυπτογράφηση [6] μπορεί να γίνει απόσπαση πληροφοριών όπως κλοπή αριθμού πιστωτικής κάρτας, κλοπή κωδικών πρόσβασης κ.α. Δίνεται η δυνατότητα σε αυτή την εφαρμογή να κάνει λήψη πληροφοριών σχετικά με την τοπολογία του δικτύου και των αριθμό των υπολογιστών που είναι στο δίκτυο. Η ανίχνευση τέτοιου είδους επιθέσεων είναι αρκετά δύσκολη.

4. **Πλαστές Διευθύνσεις IP (IP Spoofing)**
   Στην επιστήμη των υπολογιστών ο όρος ip spoofing αναφέρεται σε πακέτα IP [13] τα οποία έχουν ψεύτικη διεύθυνση προέλευσης έτσι ώστε να μην εμφανίζεται η αληθινή ταυτότητα του αποστολέα και ο παραλήπτης να νομίζει ότι ήρθε από αξιόπιστη πηγή. Χρησιμοποιείται κυρίως σε επιθέσεις άρνησης υπηρεσιών. Τέτοιου είδους επιθέσεις έχουν ως στόχο να γεμίσουν τον υπολογιστή με πάρα πολλά πακέτα ώστε να μην μπορεί να εξυπηρετήσει σωστά τους χρήστες του.

1.5.4 Διακίνηση - Πειρατεία Λογισμικού

Ο όρος *πειρατεία λογισμικού* αναφέρεται στην αναπαραγωγή και διακίνηση προγραμμάτων Η/Υ που προστατεύονται από πνευματικά δικαιώματα. Θεωρείται η χωρίς άδεια χρήση ενός προγράμματος η οποία περιλαμβάνει την εγκατάσταση αλλά και την αντιγραφή του. Έχει σημαντικές επιπτώσεις στην οικονομία μιας χώρας και θέτει στον χρήστη που

[6] Κρυπτογράφηση είναι η διαδικασία μετασχηματισμού κάποιου μηνύματος σε μη κατανοητή μορφή. Υπάρχουν πολλοί αλγόριθμοι κρυπτογράφησης όπως π.χ. ο αλγόριθμος του Καίσαρα, ο αλγόριθμος PlayFair, Des, Triple-Des, Aes κ.α

χρησιμοποιεί κάποιο πρόγραμμα λογισμικού χωρίς την απαιτούμενη άδεια, ποινικές, αστικές και διοικητικές κυρώσεις. Υπολογίζεται ότι υπάρχουν εκατομμύρια ιστοσελίδες στο διαδίκτυο που πωλούν παράνομο λογισμικό. Για να μπορούμε να είμαστε σίγουροι ότι το λογισμικό που αγοράσαμε είναι γνήσιο θα πρέπει κάθε φορά που προμηθευόμαστε κάποιο λογισμικό να ελέγχουμε ότι συνοδεύεται από κάποια άδεια χρήσης που ονομάζεται πιστοποιητικό αυθεντικότητας. Τα τελευταία χρόνια πάρα πολλοί κατασκευαστές προγραμμάτων λογισμικού προσφέρουν δωρεάν προγράμματα λογισμικού στην παγκόσμια κοινότητα. Τα λογισμικά αυτά που δίνονται για δωρεάν χρήση ονομάζονται δωρεάν λογισμικά.
Υπάρχουν αρκετές μορφές πειρατείας λογισμικού. Οι κυριότερες είναι οι εξής: **α)** Η χρήση ενός προγράμματος σε περισσότερους από έναν υπολογιστές κάτι το οποίο παραβιάζει την άδεια χρήσης του. **β)** Με την πλαστογράφηση του προϊόντος. Για παράδειγμα αντιγράφεται το λογισμικό και η συσκευασία ενός προϊόντος και πηγαίνει προς πώληση.

1.5.5 Πειρατεία Ονομάτων Χώρου

Η επίθεση αυτή ήταν πιο έντονη στα πρώτα χρόνια του *διαδικτύου* όταν οι μεγάλες εταιρείες δεν είχαν κατοχυρώσει ονόματα για τους δικτυακούς τους τόπους. Έτσι διάφοροι επιτήδειοι προέβαιναν στην κατοχύρωση ονομάτων μεγάλων εταιρειών και οργανισμών με στόχο να έχουν αυτοί τα δικαιώματα της νέας διεύθυνσης. Έπειτα η τακτική που ακολουθούσαν ήταν: α) Με την καταβολή κάποιου σημαντικού χρηματικού ποσού να παραχωρήσουν το όνομα στην εταιρεία και β) είτε να προχωρήσουν στην δημοσιοποίηση προσβλητικού περιεχομένου στην υπάρχουσα διεύθυνση κάτι το οποίο θα είχε σοβαρές συνέπειες στην εταιρεία.

1.5.6 Κλοπή Προσωπικών Δεδομένων

Η κλοπή των *προσωπικών δεδομένων* και ειδικότερα η κλοπή ταυτότητας (identity theft) είναι ένα από τα πιο σοβαρά εγκλήματα του *διαδικτύου*. Στην σημερινή ψηφιακή ζωή που διανύουμε πάρα πολλά δεδομένα είναι αποθηκευμένα σε διάφορες ηλεκτρονικές βάσεις δεδομένων [7] τα οποία χρησιμοποιούνται για διάφορους σκοπούς όπως ιατρικούς, διαφημιστικούς, εμπορικούς. Επομένως είναι πάρα πολύ εύκολο για οποιονδήποτε να βρει τα στοιχεία ενός άλλου ατόμου και να τα χρησιμοποιήσει για πάσης φύσεως συναλλαγή.

Στις παρακάτω περιπτώσεις φαίνεται πώς διαπράττεται το έγκλημα της κλοπής προσωπικών δεδομένων και ειδικότερα της *κλοπής ταυτότητας*. **1)** Εισβάλλοντας σε βάσεις δεδομένων εταιρειών όπου υπάρχουν αποθηκευμένα προσωπικά δεδομένα πολλών ατόμων, **2)** Με ειδικό λογισμικό το οποίο παρακολουθεί την κίνηση των πακέτων στο *διαδίκτυο* και έχει τον τρόπο να αποσπά προσωπικά δεδομένα, **3)** Μέσα από τα δωμάτια συζητήσεων όπου μπορεί κάποιο άτομο να δώσει το e - mail του και το όνομά του σε κάποιο άλλο άτομο αλλά να γίνει αντιληπτό από τρίτους που βρίσκονται την δεδομένη χρονική στιγμή στο δωμάτιο. **4)** Υποκλέπτοντας τα στοιχεία ατόμων μέσα από διάφορα κοινωνικά δίκτυα όπως π.χ. το (Facebook, Twitter).

Έπειτα από την κλοπή των δεδομένων ακολουθεί η χρησιμοποίηση αυτών των στοιχείων

[7] Με τον όρο βάση δεδομένων εννοούμε μία συλλογή από δεδομένα τα οποία δημιουργούν σχέσεις μεταξύ τους και μπορεί να γίνει ανάκτηση δεδομένων μέσω κάποιας αναζήτησης.

η οποία μπορεί να πραγματοποιηθεί με τους εξής τρόπους: **α)** Ανοίγοντας λογαριασμούς σε τράπεζες τους οποίους χρεώνει με πάρα πολλές ακάλυπτες επιταγές. **β)** Δημιουργώντας πλαστά διαβατήρια, πιστωτικές κάρτες, ταυτότητες με τα κλεμμένα στοιχεία πολλών ατόμων, **γ)** Δίνοντας ψευδή στοιχεία σε διάφορα κοινωνικά δίκτυα με στόχο την εξαπάτηση άλλων ατόμων.

1.5.7 Ηλεκτρονικό Ψάρεμα

Με τον όρο *ηλεκτρονικό ψάρεμα* (phishing) στο χώρο του διαδικτύου εννοούμε την ενέργεια εξαπάτησης πολλών χρηστών σύμφωνα με την οποία ο θύτης προσπαθεί μέσω διαφόρων μηνυμάτων να αποσπάσει από τα θύματα του ευαίσθητα προσωπικά δεδομένα όπως π.χ. κωδικούς πρόσβασης για διάφορες ηλεκτρονικές υπηρεσίες, στοιχεία πιστωτικών καρτών και τραπεζικών λογαριασμών κ.λπ. Βασικό στοιχείο του *ηλεκτρονικού ψαρέματος* είναι οι πολλοί σύνδεσμοι οι οποίοι έχουν κύριο σκοπό την αποπλάνηση των χρηστών. Δείχνουν αρχικά αξιόπιστοι αλλά παραπέμπουν τον χρήστη σε διαφορετικές ιστοσελίδες από αυτές που προβλεπόντουσαν.

Η επιτυχία κάποιας επίθεσης (phishing) στηρίζεται σε τρεις κύριους παράγοντες: **1)** Στην έλλειψη προσοχής του θύματος, **2)** στη έλλειψη γνώσεων του θύματος και στην οπτική εξαπάτηση. Πολλοί από τους χρήστες του διαδικτύου χειρίζονται μόνο τις βασικές λειτουργίες ενός Η/Υ. Για τον λόγο αυτό δεν μπορούν να αναγνωρίσουν τα ίχνη του *ηλεκτρονικού ψαρέματος* όπως κάποια αλλαγμένη διεύθυνση e - mail. Οι hackers συνήθως έχουν ως στόχο οικονομικούς σκοπούς για αυτό και στις περισσότερες περιπτώσεις στοχεύουν τραπεζικούς λογαριασμούς, ή λογαριασμούς που περιέχουν προσωπικά δεδομένα των χρηστών.

Οι λύσεις που υπάρχουν ενάντια σε αυτή την μορφή ηλεκτρονικού εγκλήματος είναι οι εξής: **α)** Η ενημέρωση του κοινού και η εκπαίδευσή του η οποία είναι χρήσιμη διότι η καλύτερη αντιμετώπιση ενός προβλήματος είναι η πρόληψη. Πολλές ιστοσελίδες παρέχουν πληροφορίες στους χρήστες του διαδικτύου για τα ποσοστά των επιθέσεων, τις εντοπισμένες ιστοσελίδες όπου έγινε κάποια επίθεση και τρόπους αντιμετώπισής του, **β)** Τεχνική αντιμετώπιση του προβλήματος όπως λήψη προγραμμάτων προστασίας από ιούς και προγράμματα κατασκοπείας, λήψη προγραμμάτων που αναγνωρίζουν διάφορα παραπλανητικά μηνύματα μέσω διαφορετικής διεύθυνσης URL [8].

1.5.8 Απάτη με Νιγηριανή Επιστολή

Σε αυτό το είδος ηλεκτρονικού εγκλήματος στέλνονται ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία περιέχουν πλασματικές ιστορίες και μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν χρήματα, προσφέροντας στους παραλήπτες των μηνυμάτων τεράστια κέρδη. Αρχικά ο αποστολέας - δράστης του μηνύματος συστήνεται ως κάποιο σημαντικό πρόσωπο το οποίο ζητάει την βοήθεια του παραλήπτη της επιστολής, έτσι ώστε να διοχετεύσει εκτός της χώρας της Νιγηρίας κάποιο χρηματικό ποσό. Ζητάει δηλαδή από το υποψήφιο θύμα να γίνει ο αποδέκτης του ποσού και στην συνέχεια να στείλει τα χρήματα

[8] Ονομάζεται Ενιαίος Εντοπιστής Πόρων (Uniform Resource Locator) και δηλώνει κάποια διεύθυνση μια ιστοσελίδας του διαδικτύου. Εμπεριέχει μία πληροφορία σχετικά με το όνομα του εξυπηρετητή και το πρωτόκολλο που χρησιμοποιεί.

αυτά εκτός Νιγηρίας. Για όλη τη βοήθεια που θα προσφέρει θα ανταμειφθεί με κάποιο σημαντικό χρηματικό ποσό. Έπειτα ζητείται η ανταλλαγή ορισμένων πληροφοριών με τους τραπεζικούς λογαριασμούς του θύματος αλλά και άλλων στοιχείων που θα ήταν χρήσιμα για την πραγματοποίηση της συναλλαγής. Αφού κάποιος απαντήσει στο e - mail και αποδεχθεί την πρόταση αυτή, υπογράφεται κάποιο συμφωνητικό για την επιβεβαίωση της συναλλαγής αυτής. Προτού όμως εισπράξει το θύμα τα χρήματα του ζητείτε να καταβάλλει ορισμένα χρηματικά ποσά για τα έξοδα της μεταφοράς των χρημάτων. Έπειτα από την αποστολή του ποσού θα σταματήσει κάθε είδους επικοινωνία και είναι πολύ πιθανόν ο δράστης να χρεώνει τον τραπεζικό λογαριασμό του θύματος. Μπορεί ακόμη και να χάσει όλα τα χρήματα που βρίσκονται στον λογαριασμό του αφού έχει δώσει προσωπικά του στοιχεία όπως π.χ. στοιχεία της ταυτότητάς του, αριθμό λογαριασμού της τράπεζας κ.α

1.5.9 Παιδική Πορνογραφία

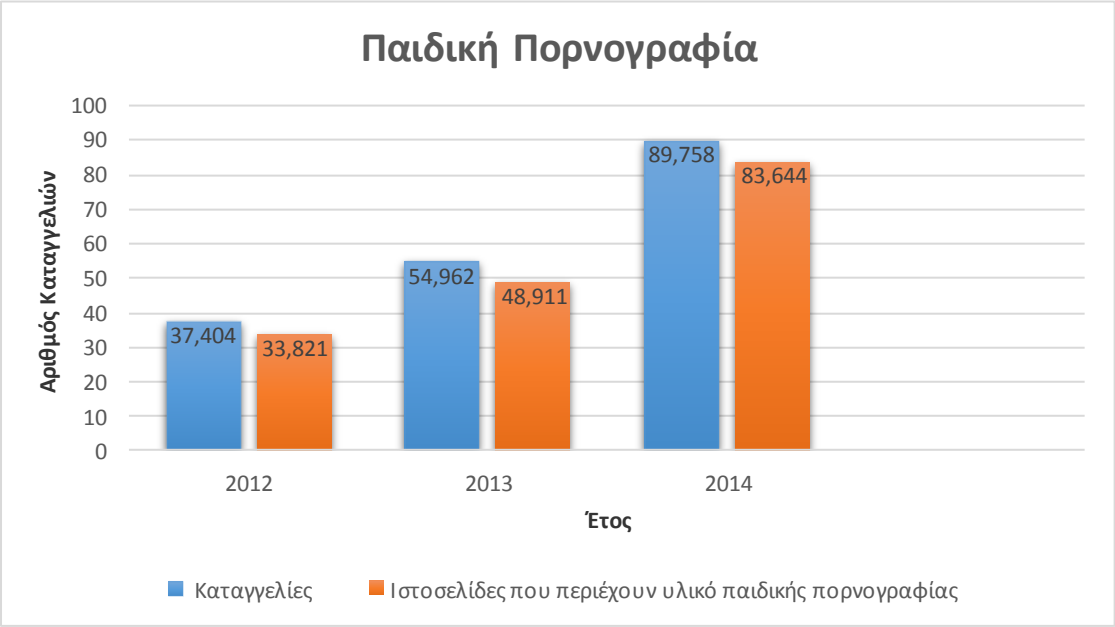
Η διακίνηση παιδικού πορνογραφικού υλικού μέσω του διαδικτύου εξελίσσεται ραγδαία στην σημερινή εποχή. Καθημερινά στην χώρα μας πάρα πολλά είναι τα θύματα αυτού του είδους ηλεκτρονικού εγκλήματος, ενώ στο εξωτερικό υπάρχουν πάρα πολλά οργανωμένα κυκλώματα παιδοφιλίας τα οποία λειτουργούν ανεξέλεγκτα. Αποτελούνται από ομάδες ανθρώπων οι οποίοι συνεργάζονται μέσω του *διαδικτύου* από διαφορετικές χώρες και έχουν ως σκοπό τη συλλογή και διανομή παιδικού πορνογραφικού υλικού. Χρειάζεται ιδιαίτερη προσοχή στα δωμάτια συνομιλιών γνωστά και ως chat rooms διότι οι παιδόφιλοι προσποιούνται ότι είναι έφηβοι με σκοπό να προσελκύσουν τα υποψήφια θύματά τους. Ξεκινούν συζητήσεις μαζί τους για να αναπτύξουν αρχικά μία φιλική σχέση με το υποψήφιο θύμα και έπειτα να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τα ενδιαφέροντά τους, τον τόπο κατοικίας τους, τα χόμπι τους κ.α. Αφού έχουν μία γενική εικόνα για αυτούς αρχίζουν συζητήσεις σεξουαλικής φύσεως και πολλοί από αυτούς στέλνουν φωτογραφίες παιδικής πορνογραφίας στα θύματά τους.

Έγκλημα διαπράττει όποιος από μόνος του παράγει, διαθέτει, διακινεί παιδικό πορνογραφικό υλικό μέσω του ηλεκτρονικού του υπολογιστή. Η αντιμετώπιση αυτού του εγκλήματος μπορεί να γίνει με τους παρακάτω τρόπους: α) Εάν γνωρίζουμε κάποιον που ασχολείται με την παιδική πορνογραφία μπορούμε να τον καταγγείλουμε στη ελληνική αστυνομία και ειδικότερα στο σώμα δίωξης ηλεκτρονικού εγκλήματος. β) Αποφεύγουμε τις συζητήσεις με αγνώστους στο διαδίκτυο και είμαστε πολλοί προσεκτικοί με κάποιον φίλο που πιθανόν να γνωρίσαμε διαδικτυακά. γ) Δεν στέλνουμε φωτογραφίες μέσω του ηλεκτρονικού ταχυδρομείου. δ) Δεν ανεβάζουμε σε ιστοσελίδες κοινωνικής δικτύωσης φωτογραφίες που είναι προκλητικές. ε) Μπορούμε να καταγγείλουμε ύποπτες ιστοσελίδες με παράνομο υλικό στον διεθνή σύνδεσμο ανοικτών γραμμών SafeLine μέσω της ηλεκτρονικής διεύθυνσης **www.safeline.gr** ο οποίος υποστηρίζεται από την Ε.Ε με σκοπό την ασφαλέστερη χρήση του διαδικτύου.

Στο σχήμα 1.1 που ακολουθεί παρατηρούμε την αύξηση του αριθμού των καταγγελιών σε που έλαβε ο INHOPE [9] τα έτη 2012, 2013 και 2014. Παρατηρούμε αύξηση του αριθμού

[9]Είναι ένας διεθνής σύνδεσμος ανοικτών γραμμών για το παράνομο περιεχόμενο του διαδικτύου. Αποτελείται από 48 οργανισμούς σε 43 χώρες παγκοσμίως. Μέλος του INHOPE είναι και η Ελλάδα με τον οργανισμό Safeline με έδρα το Ηράκλειο Κρήτης από τον Οκτώβριο του 2005. Από το 2010 διαθέτει ένα υπερσύγχρονο σύστημα

των καταγγελιών το έτος 2014 με 89.758 καταγγελίες και 83.644 ιστοσελίδες με περιεχόμενο παιδικής πορνογραφίας σε σχέση με τα έτη 2013 και 2014.



Σχήμα 1.1: *Διάγραμμα Παιδικής Πορνογραφίας*

1.5.10 Απάτη με Πιστωτικές Κάρτες

Με τις πιστωτικές κάρτες συμβαίνουν πάρα πολλά ηλεκτρονικά εγκλήματα στο διαδίκτυο και ιδιαίτερα στην χώρα μας. Υπάρχουν πάρα πολλά συστήματα τα οποία μπορούν μέσα σε ελάχιστο χρονικό διάστημα να σπάσουν τους κώδικες και να χρεώσουν την πιστωτική κάρτα χωρίς εμείς να μπορούμε να αντιδράσουμε. Οι ελληνικές τράπεζες έχουν χάσει πάνω από 15 εκατομμύρια ευρώ από ανθρώπους που υποκλέπτουν αριθμούς καρτών και κάνουν αγορές μέσω του διαδικτύου.

Μεγάλος αριθμός καταγγελιών αφορά εμπορεύματα τα οποία αγοράστηκαν μέσω κάποιας ιστοσελίδας, πληρώθηκαν με πιστωτική κάρτα αλλά δεν έφτασαν ποτέ στον προορισμό τους. Πάρα πολλές καταγγελίες επιπλέον αφορούν πολίτες που βλέπουν στην πιστωτική τους κάρτα να έχουν χρεωθεί από ηλεκτρονικό τζόγο ενώ οι ίδιοι ισχυρίζονται ότι δεν έπαιξαν ποτέ.

Προκειμένου να προστατευθούν οι πολίτες πρέπει να γνωρίζουν τα εξής: 1) Είμαστε πολλοί προσεκτικοί με τις συναλλαγές μέσω πιστωτικής κάρτας στο διαδίκτυο. 2) Εάν αντιληφθούμε κάτι ασυνήθιστο επικοινωνούμε ταχύτατα με τις αρμόδιες αρχές έτσι ώστε πιθανόν να μειώσουμε τη ζημιά που έκανε ο απατεώνας στον τραπεζικό μας λογαριασμό. 3) Επικοινωνούμε με το τμήμα ασφαλείας της τράπεζας που συνεργαζόμαστε και με τις εταιρείες πιστωτικών καρτών για κάθε ύποπτη πρόσβαση στον λογαριασμό μας. 4) Εάν έχουμε ανοίξει πρόσφατα λογαριασμό σε κάποια τράπεζα χρησιμοποιούμε στην πιστωτική μας κάρτα ισχυρούς κωδικούς πρόσβασης. 5) Ζητάμε αντίγραφο αναλυτικής κατάστασης του λογαριασμού μας και ζητάμε να μην γίνεται καμία χρέωση του λογαριασμού μας χωρίς την έγκρισή μας.

διαχείρισης καταγγελιών μέσω του οποίου επεξεργάζονται όλα τα δεδομένα ανά τον κόσμο. Χρηματοδοτείται από την Ε.Ε και συνεργάζεται με διεθνείς οργανισμούς καταστολής εγκλημάτων.

1.5.11 Επιθέσεις Παρενόχλησης

Στο διαδίκτυο την σημερινή εποχή εμφανίζεται ένα φαινόμενο το οποίο είναι γνωστό με το όνομα *επίθεση παρενόχλησης* (cyber bullying). Το φαινόμενο αυτό προκαλεί φόβο, αμηχανία, ντροπή σε πάρα πολλά παιδιά και εφήβους χρήστες του διαδικτύου. Οι βασικές αιτίες που οδηγούν συχνά τους νέους στο διαδικτυακό εκφοβισμό είναι ορισμένα συναισθήματα θυμού, απόγνωσης που υπάρχουν στο οικογενειακό τους περιβάλλον και αναγκάζουν τους νέους να ξεσπούν σε άλλα άτομα μέσω του διαδικτύου.

Κύριες μορφές ηλεκτρονικού εκφοβισμού είναι οι εξής: **1)** Παρενόχληση (harassment): Η αποστολή προσβλητικών μηνυμάτων σε πολλούς χρήστες του διαδικτύου δημιουργεί ένα κλίμα εκφοβισμού και αρκετά προβλήματα σε πολλά παιδιά στο διαδίκτυο. **2)** Ανάφλεξη (flaming): Ορισμένοι νέοι χρησιμοποιούν αγενή γλώσσα και με αυτόν τον τρόπο δημιουργούνται διαδικτυακοί διαπληκτισμοί με απρόβλεπτες εξελίξεις. **3)** Δυσφήμιση (denigration): Η δημοσίευση κουτσομπολιών ή φημών σχετικά με ένα άτομο με στόχο την δυσφήμιση του ονόματός του στο περιβάλλον του. **4)** Αποκλεισμός (exclusion): Η αποξένωση κάποιου χρήστη από μία ομάδα στο διαδίκτυο μπορεί να δημιουργήσει μέχρι και ψυχολογικά προβλήματα στο άτομο αυτό.

Τα πιο συνηθισμένα προβλήματα που δημιουργούνται έπειτα από την εμφάνιση αυτού του είδους επίθεσης στους νέους είναι τα παρακάτω: **α)** Ψυχολογικά προβλήματα εμφανίζονται σε αρκετούς εφήβους τα οποία εάν δεν αντιμετωπιστούν εγκαίρως θα δημιουργήσουν πρόβλημα στην ανάπτυξη του εφήβου. **β)** Πολλοί νέοι γίνονται απόμακροι και δεν εμπιστεύονται ούτε τα οικογενειακά τους πρόσωπα. **γ)** Αρκετοί μπορεί ακόμα και να χειροδικήσουν απέναντι στα άτομα που τους πρόσβαλαν.

2.1 Ελληνική Νομοθεσία

Στην χώρα μας οι νομοθετικές ρυθμίσεις για την αντιμετώπιση του ηλεκτρονικού εγκλήματος παρουσιάζουν αρκετές αδυναμίες. Ο νομοθέτης πρέπει να ενημερώνεται συνεχώς διότι η εξέλιξη στην τεχνολογία των υπολογιστών αυξάνεται συνεχώς και οι μορφές ηλεκτρονικών εγκλημάτων εξελίσσονται ραγδαία. Για τον λόγο αυτό παρουσιάζονται αρκετά προβλήματα στα αδικήματα τα οποία θα πρέπει να διώκονται ποινικά. Πολλές επιχειρήσεις αποφεύγουν να καταγγείλουν παραβάσεις διότι φοβούνται ότι οι δράστες θα επαναλάβουν ξανά το ίδιο αδίκημα και αυτό πιθανόν να δημιουργήσει πλήγμα στην φήμη τους.

Στην Ελλάδα αλλά και σε άλλες χώρες παγκοσμίως, τα τελευταία χρόνια έχουν γίνει συνέδρια που έχουν ως σκοπό την συζήτηση και λήψη αποφάσεων για αυτό το ζήτημα. Στην χώρα μας δεν υπάρχει αποκλειστικός νόμος ο οποίος θα αναφέρεται σε ζητήματα του διαδικτύου και στην συμπεριφορά των χρηστών του. Υπάρχει ένας νόμος ο οποίος αφορά γενικά εγκλήματα που διαπράττονται με τους ηλεκτρονικούς υπολογιστές. Υπάρχουν ορισμένες εποπτικές αρχές [14] οι οποίες εποπτεύουν ορισμένα ζητήματα ασφαλείας του διαδικτύου και ειδικότερα των επικοινωνιών στην Ελλάδα οι οποίες είναι οι εξής:

α) Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η οποία έχει ως σκοπό την τήρηση του προσωπικού απορρήτου στο διαδίκτυο. **β)** Η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών σκοπός της οποίας είναι η προστασία του απορρήτου των επιστολών με οποιοδήποτε άλλο τρόπο. **γ)** Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων που ελέγχει τον τομέα των τηλεπικοινωνιών.

2.1.1 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ)

Λειτουργεί από το 1977 και η αποστολή της είναι η τήρηση του προσωπικού απορρήτου στο διαδίκτυο. Διάφορες ιστοσελίδες συγκεντρώνουν ορισμένα προσωπικά στοιχεία των επισκεπτών τους όπως π.χ. το όνομά τους, το τηλέφωνό τους, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που διαθέτουν και έχουν υποχρέωση να τους ενημερώνουν για τον λόγο που συλλέγονται αυτά τα στοιχεία καθώς και εάν γίνονται ορατά σε τρίτα άτομα, σύμφωνα με τον νόμο περί προστασίας δεδομένων προσωπικού χαρακτήρα.

2.1.2 Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε)

Λειτουργεί από το 2003 ως ανεξάρτητη αρχή και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης επικοινωνίας με οποιοδήποτε άλλο τρόπο. Ο όρος προστασία του απορρήτου των επικοινωνιών εμπεριέχει τον έλεγχο τήρησης των κανόνων αλλά και την διαδικασία άρσης του απορρήτου. Στις αρμοδιότητές της περιλαμβάνεται η διενέργεια ελέγχου και εξέτασης των καταγγελιών. Οι πιο σημαντικές αρμοδιότητες που έχει είναι οι εξής:

α) Μπορεί να κάνει ελέγχους από μόνη της ή έπειτα από καταγγελία σε τραπεζικά δεδομένα, σε εγκαταστάσεις, σε τεχνικό εξοπλισμό αλλά και σε διάφορες δημόσιες υπηρεσίες που ασχολούνται με ταχυδρομικές και τηλεπικοινωνιακές υπηρεσίες και έχουν σχέση με την

επικοινωνία και το απόρρητο των επιστολών. **β)** Μπορεί να καλεί σε ακρόαση τους εκπροσώπους αλλά και τους υπαλλήλους των παραπάνω υπηρεσιών και οργανισμών. **γ)** Έχει το δικαίωμα να συνεργάζεται με άλλες αρχές της χώρας ή και με αντίστοιχες άλλων κρατών προκειμένου να γίνει καλύτερος συντονισμός και επίλυση κάποιας υπόθεσης σε διεθνές επίπεδο. **δ)** Απευθύνει συστάσεις για λήψη μέτρων απορρήτου των επικοινωνιών αλλά και άρσης αυτού.

2.1.3 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ)

Αποστολή της είναι ο έλεγχος του τομέα των τηλεπικοινωνιών. Αποτελεί μία ανεξάρτητη διοικητική αρχή, τα στελέχη της επιλέγονται από τη διάσκεψη των προέδρων της βουλής και με απόφαση του Υπουργού Μεταφορών και Επικοινωνιών. Υποχρεούνται να τηρούν απόλυτη εμπιστευτικότητα των πληροφοριών για τέσσερα χρόνια έπειτα από την αποχώρησή τους από την (Ε.Ε.Τ.Τ). Αρμοδιότητές της είναι ο έλεγχος του τομέα των τηλεπικοινωνιών ενώ παράλληλα εποπτεύει και την τηλεπικοινωνιακή αγορά.

2.2 Νομοθεσία στο Εξωτερικό

Το έτος 1990 τέθηκε σε ισχύ από το Κοινοβούλιο του Ηνωμένου Βασιλείου ένας νόμος που στοχεύει στην εξασφάλιση του υλικού του υπολογιστή από τη μη εξουσιοδοτημένη πρόσβαση. Ο νόμος αυτός ήταν γνωστός με το όνομα Computer Misuse Act. Σύμφωνα με αυτόν τον νόμο **1)** Η μη εξουσιοδοτημένη πρόσβαση στο υλικό σε κάποιον υπολογιστή τιμωρείται με κάθειρξη τουλάχιστον 6 μήνες ή με χρηματική ποινή. **2)**Εάν κάποιος που δεν έχει εξουσιοδότηση, με πρόθεση διαπράξει ή διευκολύνει στην διάπραξη νέων αδικημάτων τιμωρείται με κάθειρξη 6 μήνες και δεν έχει το δικαίωμα σε δίκη με ενόρκους.

Ο νόμος αυτός έχει εφαρμοστεί από αρκετές χώρες και βοηθά στην αντιμετώπιση των ηλεκτρονικών εγκλημάτων στον κυβερνοχώρο. Στις ΗΠΑ οποιαδήποτε πρόσβαση σε Η/Υ χωρίς την απαιτούμενη εξουσιοδότηση, ανάλογα και με το μέγεθος της ζημιάς που έχει προκαλέσει τιμωρείται με φυλάκιση μέχρι και ισόβια χωρίς να υπάρχει δυνατότητα να μειωθεί η ποινή.

2.3 Η Δικαιοδοσία στο Διαδίκτυο

Με τον όρο δικαιοδοσία εννοούμε την αρμοδιότητα του δικαστηρίου να δικάσει μια υπόθεση αλλά ταυτόχρονα και την αρμοδιότητα των αρχών να ερευνήσουν κάποιο ηλεκτρονικό έγκλημα. Το πρόβλημα της δικαιοδοσίας για τα εγκλήματα που γίνονται στο διαδίκτυο δεν είναι απλό διότι μπορεί ο καθένας από οποιοδήποτε σημείο του πλανήτη να εισάγει και να μάθει οποιαδήποτε πληροφορία θελήσει.

Ανάλογα με τον τόπο όπου διαπράττεται κάποιο αδίκημα έχει και την ανάλογη αρμοδιότητα το δικαστήριο που υπάρχει στην περιοχή. Για να καθοριστεί ο τόπος τέλεσης του αδικήματος [15] υπάρχουν τέσσερις θεωρίες.

1) Η θεωρία που έχει να κάνει με τον τόπο του αποτελέσματος. Η περιοχή που εκδηλώθηκε το αποτέλεσμα κάποιο αδικήματος θεωρείται τόπος τέλεσής του.

2) Η θεωρία του τόπου ενέργειας. Στην θεωρία αυτή τόπος τέλεσης του αδικήματος θεωρείται ο τόπος όπου έγινε κάποια συγκεκριμένη ενέργεια και με αυτόν τον τρόπο φτάσαμε στο άδικο αποτέλεσμα. Εάν κάποια ενέργεια έγινε σε περισσότερα από ένα κράτη τότε ο τόπος ενέργειας είναι εκείνος που ολοκληρώθηκε η ενέργεια.

3) Υπάρχει η μικτή θεωρία η οποία περιλαμβάνει τις δύο παραπάνω θεωρίες και υπάρχει η δυνατότητα της επιλογής του αδικηθέντος.

4) Στην θεωρία του βαρύνοντος τόπου εντοπίζεται στο κράτος όπου εκδηλώθηκε το έγκλημα ο τόπος του αδικήματος. Υπάρχουν όμως πολλές δυσκολίες για την εφαρμογή αυτής της θεωρίας καθώς είναι δύσκολο να καθοριστεί ο τόπος τέλεσης ενός αδικήματος.

2.4 Νομικά Ζητήματα Διαδικτύου

Η νομική ρύθμιση του διαδικτύου αποτελεί κυρίαρχο νομικό ζήτημα έτσι ώστε να μπορέσει να αντιμετωπιστεί αποτελεσματικά το ηλεκτρονικό έγκλημα. Δεν υπάρχουν συγκεκριμένες διατάξεις οι οποίες να αφορούν συγκεκριμένα αδικήματα που γίνονται στο διαδίκτυο ανάλογα με τις υπηρεσίες του. Γίνεται προσπάθεια να ρυθμιστεί αυτό το ζήτημα αλλά συναντά εμπόδια. Υπάρχουν δύο ειδών απόψεις για αυτό το θέμα.

1) Επιχειρήματα ανθρώπων που συμφωνούν στην ρύθμιση ζητημάτων που αφορούν το διαδίκτυο είναι τα εξής:

α) Πολλοί θεωρούν ότι απαιτείται ρύθμιση νομικών ζητημάτων έτσι ώστε να μπορεί να ελεγχθεί το παράνομο περιεχόμενό του. **β)** Πρέπει να γίνουν νομοθετικές ρυθμίσεις διότι αποτελεί και αυτό μέσο επικοινωνίας όπως το ραδιόφωνο και η τηλεόραση στα οποία έχουν γίνει νομικές ρυθμίσεις. **γ)** Είναι υποχρέωση της πολιτείας να ελέγχει και να αντιμετωπίζει την αυξανόμενη εγκληματική δραστηριότητα που τελείται στο χώρο του διαδικτύου. **δ)** Πολλοί χρήστες χρειάζονται νομικές ρυθμίσεις έτσι ώστε να μπορούν να προστατευθούν από την κλοπή των προσωπικών τους δεδομένων από διάφορα είδη επιθέσεων.

2) Επιχειρήματα ανθρώπων που διαφωνούν στην ρύθμιση ζητημάτων που αφορούν το διαδίκτυο είναι τα εξής:

α) Ορισμένοι πιστεύουν ότι το διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας. Κύρια χαρακτηριστικά του είναι η ειλικρίνεια και η ελευθερία. **β)** Η παγκοσμιότητα του διαδικτύου αποτελεί πρόβλημα σε οποιαδήποτε προσπάθεια ρύθμισης νομικών ζητημάτων να αντικρούει στο λόγο των πολιτών. **γ)** Πολλοί πιστεύουν ότι οι γονείς έχουν την ευθύνη για την προστασία των παιδιών τους στο διαδίκτυο και όχι τα κράτη με τις διάφορες ρυθμίσεις τους.

2.5 Η Σύμβαση με τον Κυβερνοχώρο

Η συνεχής αυξανόμενη εγκληματικότητα στον κυβερνοχώρο εξέφρασε την ανησυχία του Συμβουλίου της Ευρώπης στην έγκαιρη και αποτελεσματική αντιμετώπιση της εγκληματικότητας σε διεθνές επίπεδο. Για να επιτευχθεί αυτό ήταν απαραίτητη η διακρατική συνεννόηση μεταξύ των χωρών που βρίσκονται στην Ε.Ε.

Αυτό επετεύχθη στο συνέδριο που πραγματοποιήθηκε για το ηλεκτρονικό έγκλημα στην Βουδαπέστη και στην Συνθήκη που υπογράφτηκε από 26 υπουργούς χωρών της Ε.Ε μεταξύ

και της Ελλάδας στις 23 Νοεμβρίου του 2001. Η σύμβαση έγινε γνωστή ως Συνθήκη της Βουδαπέστης [16] λόγω του τόπου υπογραφής της. Μέσω αυτής έγινε η χάραξη μιας κοινής αντεγκληματικής πολιτικής στην Ευρώπη.

Κύριος σκοπός της σύμβασης είναι η προστασία των χωρών της Ε.Ε σε εγκλήματα που εκδηλώνονται μέσω του διαδικτύου και θέσπιση της κατάλληλης νομοθεσίας από όλα τα κράτη μέλη και την δικαστική συνεργασία για την επίλυση ενός εγκλήματος. Περιέχεται νομοθετικό πλαίσιο για την δίωξη των εγκλημάτων του κυβερνοχώρου και θέτονται οι βάσεις για την αποτελεσματική αντιμετώπιση του ηλεκτρονικού εγκλήματος.

2.5.1 Το Περιεχόμενο της Σύμβασης

Αρχικά αναφέρονται τα μέτρα τα οποία πρέπει να ληφθούν υπόψιν σε εθνικό επίπεδο. Αναφέρονται διατάξεις σχετικές με το ποινικό δίκαιο στο οποίο όλα τα κράτη μέλη της σύμβασης πρέπει να θεσπίσουν νόμους για τα εγκλήματα κατά της εμπιστευτικότητας [1] ακεραιότητας [2] και της διαθεσιμότητας [3] των δεδομένων αλλά και των συστημάτων στο διαδίκτυο. Η σημασία θέσπισης των παραπάνω νόμων είναι αρκετά σημαντική εάν αναλογιστούμε ότι μέσω του διαδικτύου διακινούνται πάρα πολλές πληροφορίες και αρκετά δεδομένα τα οποία σχετίζονται με την προσωπική αλλά και την ιδιωτική ζωή των χρηστών του. Είναι δικαίωμα του καθενός να απαιτήσει την ασφαλή διακίνηση των δεδομένων στο διαδίκτυο.

Σύμφωνα με το άρθρο 2 της Σύμβασης κάθε μέλος πρέπει να θεσπίσει νομοθετικά μέτρα για την αντιμετώπιση του εγκλήματος της παράνομης πρόσβασης (illegal access) σε συστήματα ηλεκτρονικών υπολογιστών είτε εάν αυτό γίνεται εκ προθέσεως είτε χωρίς πρόθεση. Σκοπός αυτής της διάταξης είναι η αντιμετώπιση της παράνομης εισβολής σε δίκτυα υπολογιστών, το λεγόμενο (hacking).

Το άρθρο 3 της Σύμβασης αφορά την υποκλοπή δεδομένων ηλεκτρονικών υπολογιστών. Πιο συγκεκριμένα η διάταξη αυτή αφορά κάθε μορφή υποκλοπής δεδομένων που διακινούνται στο διαδίκτυο όπως το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol) [4], το ηλεκτρονικό ταχυδρομείο και άλλες υπηρεσίες του διαδικτύου.

Σύμφωνα με το άρθρο 4 κάθε κράτος μέλος πρέπει να λάβει τα ανάλογα νομικά μέτρα και να καθιερώσει ως ποινικό αδίκημα την οποιαδήποτε επέμβαση σε ηλεκτρονικά δεδομένα χωρίς το απαιτούμενο δικαίωμα. Περιλαμβάνεται η διαγραφή (deletion), καταστροφή (damaging), φθορά (deterioration) και απόκρυψη (suppression) των δεδομένων.

Επιπλέον στο περιεχόμενο της σύμβασης υπάρχουν διατάξεις ποινικού δικονομικού δικαίου που αφορούν την έρευνα και την κατάσχεση όλων των αποθηκευμένων στοιχείων που

[1] Ο όρος εμπιστευτικότητα των δεδομένων αφορά την προστασία των δεδομένων από την μη εξουσιοδοτημένη πρόσβαση αλλά και την μη εξουσιοδοτημένη ανάγνωση. Η έννοια της εμπιστευτικότητας συνδέεται και με την ιδιωτικότητα των δεδομένων αλλά και την μυστικότητα των δεδομένων που ανήκουν σε μία επιχείρηση ή έναν οργανισμό.

[2] Η ακεραιότητα των δεδομένων δείχνει ότι τα δεδομένα που έχουν παραλειφθεί είναι πλήρη και δεν έχουν αλλοιωθεί. Στο τομέα της πληροφορικής σημαίνει πρόληψη από την μη εξουσιοδοτημένη μεταβολή των πληροφοριών.

[3] Με τον όρο διαθεσιμότητα των δεδομένων εννοούμε ότι τα δεδομένα και οι υπηρεσίες ενός δικτύου είναι προσβάσιμα και λειτουργούν παρά τις όποιες διαταραχές που ενδεχομένως να προκύψουν. Όπως διακοπή τροφοδοσίας, ατυχήματα ή επιθέσεις.

[4] Είναι η εφαρμογή που επιτρέπει την μεταφορά αρχείων από έναν διακομιστή στον τοπικό μας υπολογιστή ή και το αντίστροφο. Πρέπει να διαθέτουμε α) την διεύθυνση του διακομιστή, β) ένα όνομα χρήστη και έναν κωδικό και γ) ένα μικρό λογισμικό που διευκολύνει όλη την παραπάνω διαδικασία.

υπάρχουν στον ηλεκτρονικό υπολογιστή σε περίπτωση κάποιου είδους ηλεκτρονικού εγκλήματος. Υπάρχουν διατάξεις που σχετίζονται με τα αδικήματα που διαπράττονται με την βοήθεια του Η/Υ όπως η πλαστογραφία, αδικήματα σχετικά με την προβολή, διάθεση, διανομή υλικού παιδικής πορνογραφίας και αδικήματα σχετικά με την καταπάτηση των πνευματικών δικαιωμάτων.

Επιπροσθέτως έχουμε διατάξεις διεθνούς δικαστικής συνεργασίας μεταξύ των κρατών μελών όπως η παροχή πληροφοριών σε κάποια υπόθεση και η συνεργασία μεταξύ των χωρών για την εξακρίβωση του πραγματικού ενόχου. Υπάρχουν ρυθμίσεις για την συνέργεια και την υποκίνηση των ατόμων ώστε να διαπράξουν κάποια μορφή ηλεκτρονικού εγκλήματος.

3.1 Εισαγωγή στη Ασφάλεια του Ηλεκτρονικού Υπολογιστή

Η ασφάλεια είναι ένα θέμα που πρέπει να απασχολήσει όλους τους χρήστες των Η/Υ και του ίντερνετ. Αρκετοί αποφεύγουν να ασχοληθούν με αυτό το ζήτημα πιστεύοντας ότι δεν είναι σημαντικό, ενώ άλλοι θεωρούν ότι χρειάζονται ειδικές γνώσεις του τομέα της πληροφορικής. Τα προβλήματα που δημιουργούνται είναι πάρα πολύ σπουδαία και υπάρχει μεγάλη ανάγκη για προστασία του προσωπικού μας υπολογιστή. Συνήθως καταλαβαίνουμε την σπουδαιότητα του ζητήματος όταν κλαπούν δεδομένα από τον υπολογιστή μας ή όταν υπάρξουν εισβολείς στο σύστημά μας. Σημαντικό ρόλο παίζει η γνώση έτσι ώστε να μην γίνουμε θύματα διαφόρων μορφών ηλεκτρονικών εγκλημάτων.

3.1.1 Ορισμός Ασφάλειας

Με το όρο ασφάλεια σε ένα δίκτυο υπολογιστών [1] εννοούμε την ικανότητα κάποιας επιχείρησης ή ενός οργανισμού να προστατεύει τα δεδομένα που διαθέτει ενάντια σε κακόβουλες ενέργειες μη εξουσιοδοτημένων χρηστών του διαδικτύου, οι οποίες θέτουν σε κίνδυνο την ακεραιότητα των δεδομένων, την τήρηση του απορρήτου καθώς και άλλες υπηρεσίες που παρέχονται μέσω αυτών των συστημάτων.

Πιο συγκεκριμένα η *ασφάλεια στα δίκτυα υπολογιστών* [17] σχετίζεται με τις παρακάτω ενέργειες.

1) Πρόληψη: Είναι η διαδικασία μέσω τις οποίας λαμβάνονται μέτρα ώστε να προληφθούν φθορές που ενδεχομένως να δημιουργηθούν σε ένα δίκτυο υπολογιστών.

2) Ανίχνευση: Μέσω τις διαδικασίας τις ανίχνευσης μπορούμε να λάβουμε μέτρα έτσι ώστε να γνωρίζουμε πότε και σε ποιά χρονική στιγμή δημιουργήθηκε φθορά στο σύστημά μας.

3) Αντίδραση: Περιλαμβάνει μέτρα τα οποία στοχεύουν στην αποκατάσταση και στην ανάκτηση των δεδομένων του συστήματος του Η/Υ.

Σημαντικές ιδιότητες της ασφάλειας είναι η ακεραιότητα, η εμπιστευτικότητα, η διαθεσιμότητα, η αυθεντικότητα και η μοναδικότητα των πληροφοριών.

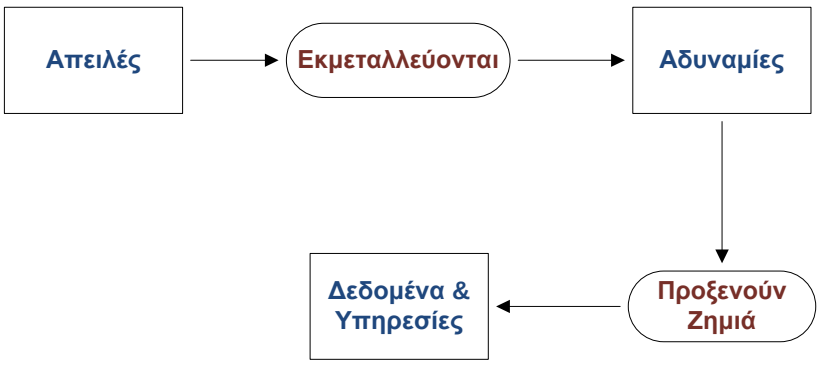
3.2 Ορισμός Απειλής

Απειλή ονομάζουμε κάποια ενέργεια ή κάποιο γεγονός το οποίο θα προκαλέσει απώλεια σε ένα ή περισσότερα χαρακτηριστικά της ασφάλειας ενός συστήματος. Οι απειλές διακρίνονται σε δύο κατηγορίες: **α)** Σκόπιμες και **β)** Τυχαίες.

Σκόπιμες ονομάζονται οι απειλές οι οποίες έχουν κακή πρόθεση και θέλουν να βλάψουν το σύστημα του Η/Υ. Εκμεταλλεύονται αδυναμίες του συστήματος με σκοπό να ζημιώσουν τις υπηρεσίες του. Ενώ Τυχαίες είναι οι απειλές αυτές που προκύπτουν από ενέργειες οι οποίες δεν έχουν ως σκοπό την κακή πρόθεση να βλάψουν το σύστημα. Με τον όρο αδυναμία

[1] Δίκτυο Υπολογιστών είναι ένα σύστημα από ανεξάρτητους ή όχι ανεξάρτητους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές είναι διασυνδεδεμένοι όταν μπορούν να ανταλλάξουν πληροφορίες ανάμεσά τους και αυτόνομοι όταν ένας Η/Υ δεν μπορεί να ελέγξει κάποιες λειτουργίες ενός άλλου υπολογιστή.

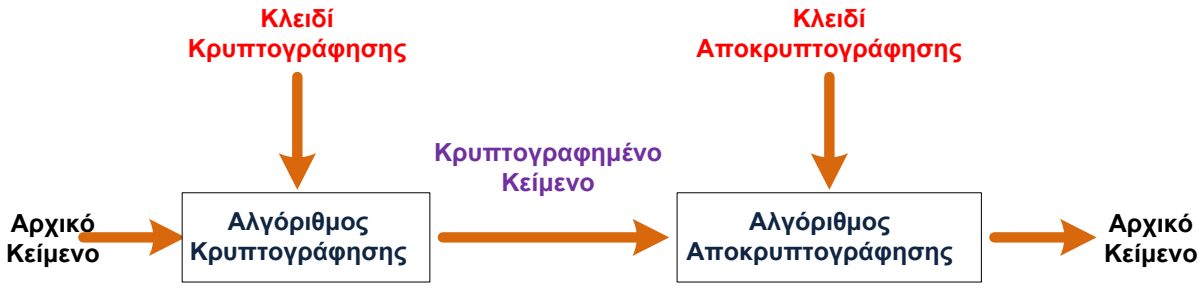
εννοούμε κάποιο σημείο ενός πληροφοριακού συστήματος το οποίο επιτρέπει να προκληθεί ζημιά στα δεδομένα και στις υπηρεσίες του. Στο παρακάτω σχήμα 3.1 παρατηρούμε τις σχέσεις μεταξύ των απειλών, αδυναμιών και υπηρεσιών ενός συστήματος. Βλέπουμε ότι οι απειλές εκμεταλλεύονται ορισμένες αδυναμίες του συστήματος και έτσι προκαλούν ζημιά στα δεδομένα και στις υπηρεσίες του.



Σχήμα 3.1: *Σχέσεις Απειλών, Αδυναμιών και Δεδομένων ενός Συστήματος*

3.3 Κρυπτογράφηση Δεδομένων

Με τον όρο *κρυπτογράφηση των δεδομένων* [18] εννοούμε την διαδικασία μέσω τις οποίας γίνεται επεξεργασία της ψηφιακής πληροφορίας έτσι ώστε να μπορεί να είναι αναγνώσιμη μόνο σε εξουσιοδοτημένα άτομα. Υπάρχουν αρκετοί αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης. Ένα σύστημα κρυπτογράφησης αποτελείται από τέσσερα σημεία. Αυτά είναι: **1)** Το αρχικό μήνυμα, **2)** Έναν αλγόριθμο κρυπτογράφησης και έναν αποκρυπτογράφησης, **3)** Το κρυπτογραφημένο μήνυμα που γίνεται μέσω ενός αλγορίθμου κρυπτογράφησης και **4)** Ένα " κλειδί " το οποίο είναι μία συμβολοσειρά από κώδικα, η οποία χρησιμοποιείται στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης μέσω κάποιων αλγορίθμων. Όλοι αυτή η διαδικασία παρουσιάζεται στο παρακάτω σχήμα 3.2 όπου φαίνεται η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος.



Σχήμα 3.2: *Σύστημα Κρυπτογράφησης - Αποκρυπτογράφησης*

Αποτελεί ένα σημαντικό εργαλείο το οποίο προστατεύει πληροφορίες εμπιστευτικού χαρακτήρα. Τα μέτρα που διασφαλίζονται με την μέθοδο της κρυπτογράφησης είναι τα παρακάτω: α) Αναβάθμιση της γνησιότητας του λογισμικού, β) Συχνή αλλαγή των κωδικών

πρόσβασης, γ) Η χρησιμοποίηση διαφόρων αριθμητικών συστημάτων ελέγχου.[2]

3.4 Μέτρα Πρόληψης

Σε ένα πληροφοριακό σύστημα ενός οργανισμού η πρόληψη αποτελεί έναν βασικό τομέα στην ασφάλεια του συστήματός μας. Μέσω διαφόρων τεχνικών που παρουσιάζονται παρακάτω θα έχουμε λιγότερα ζητήματα που θα σχετίζονται με την ασφάλεια στο σύστημά μας.

3.4.1 Διαδικασίες Αυθεντικοποίησης

Ο όρος *αυθεντικοποίηση* στον τομέα της πληροφορικής αναλύεται ως η επαλήθευση της ταυτότητας ενός χρήστη ο οποίος θέλει να συνδεθεί σε κάποιον υπολογιστή. Μέσω της αυθεντικοποίησης εμποδίζεται οποιαδήποτε μη εξουσιοδοτημένη ενέργεια για σύνδεση στο σύστημά μας. Είναι απλά μια διαδικασία " ταυτοπροσωπίας ". Για να μπορέσει κάποιος χρήστης ενός Η/Υ να επιβεβαιώσει την ταυτότητά του και να έχει πρόσβαση στον *ηλεκτρονικό του υπολογιστή* μπορεί να χρησιμοποιήσει κωδικούς πρόσβασης, ορισμένα φυσικά του χαρακτηριστικά όπως δακτυλικά αποτυπώματα, αναγνώριση φωνής κ.α. Όλα αυτά αποτελούν ορισμένα στοιχεία έτσι ώστε να μπορέσουμε να έχουμε πιστοποίηση της ταυτότητας ενός χρήστη αλλά με την εφαρμογή αυτών των στοιχείων δεν μπορούμε να πούμε ότι θα έχουμε απόλυτη ασφάλεια στο σύστημά μας.

3.4.2 Κωδικός Πρόσβασης

Οι κωδικοί πρόσβασης αποτελούν τον πιο δημοφιλή τρόπο για την προστασία των δεδομένων μας στο διαδίκτυο. Αρκεί μόνο να δημιουργήσουμε ένα όνομα χρήστη (username) και έναν κωδικό πρόσβασης (password), ξεχωριστά σε κάθε λογαριασμό που θέλουμε να χρησιμοποιήσουμε όπως π.χ. το ηλεκτρονικό ταχυδρομείο (e - mail). Μπορούμε να τα απομνημονεύσουμε εύκολα αλλά και να τα αλλάξουμε οποιαδήποτε στιγμή θελήσουμε.

Όμως όπως είπαμε προηγουμένως και αυτή η μέθοδος παρουσιάζει αρκετά κενά στο τομέα της ασφάλειας αφού υπάρχουν αρκετά εργαλεία λογισμικού τα οποία μπορούν να αποκαλύψουν τον κωδικό πρόσβασης μέσω μιας απλής διαδικασίας. Ένα σύνηθες λάθος που κάνουν αρκετοί χρήστες του διαδικτύου είναι να επιλέγουν τους ίδιους κωδικούς για πάρα πολλές εφαρμογές του διαδικτύου. Επιπλέον χρησιμοποιούν για κωδικούς πρόσβασης π.χ. τον αριθμό του τηλεφώνου τους, την ημερομηνία γέννησής τους κ.α. κάτι το οποίο είναι εξαιρετικά επικίνδυνο διότι μπορεί πάρα πολύ εύκολα ο καθένας μας να το μαντέψει και να εισβάλλει στον λογαριασμό του.

3.4.3 Βιομετρικές Τεχνικές

Βιομετρία ονομάζεται η επιστήμη που χρησιμοποιεί την ψηφιακή τεχνολογία για την ταυτοποίηση των ανθρώπων. Στόχος της είναι η επαλήθευση αλλά και η επιβεβαίωση της ταυτότητας κάποιου χρήστη σύμφωνα με ορισμένα μοναδικά χαρακτηριστικά.

[2]Με τον όρο αριθμητικό σύστημα ελέγχου εννοούμε την μετατροπή κάποιου αριθμού σε άλλο σύστημα, όχι στο δεκαδικό που χρησιμοποιούμε. Τέτοια αριθμητικά συστήματα είναι το δυαδικό το οποίο έχει σαν βάση τον αριθμό 2 και έχει δύο σύμβολα απεικόνισης ενός αριθμού, το μηδέν και το ένα.

Στις βιομετρικές τεχνικές [19] εντάσσονται:

1. Σάρωση Δακτυλικού Αποτυπώματος

   Η μέθοδος αυτή αποτελεί μία αξιόπιστη μέθοδο ταυτοποίησης ενός χρήστη αφού το δακτυλικό αποτύπωμα είναι ένα μοναδικό χαρακτηριστικό σε κάθε άτομο. Έχει διαπιστωθεί ότι η πιθανότητα για ύπαρξη ίδιου *δακτυλικού αποτυπώματος* είναι μία στο δισεκατομμύριο. Τα αποτυπώματα λαμβάνονται από οπτικούς αναγνώστες και μέσω υπέρυθρων ακτίνων.

2. Αναγνώριση Προσώπου

   Βασίζεται στα χαρακτηριστικά του προσώπου ενός χρήστη. Αποτελεί μια βιομετρική τεχνική η οποία δίνει έμφαση σε ορισμένα στοιχεία του προσώπου όπως το περίγραμμα του ματιού, οι αποστάσεις των ματιών, του στόματος κ.α. Η τεχνολογία αυτή χρησιμοποιείται και από την αστυνομία για την αναγνώριση διαφόρων υπόπτων αλλά και από πολλά προγράμματα διαχείρισης φωτογραφιών τα οποία έχουν την δυνατότητα να αναγνωρίζουν αυτόματα τα πρόσωπα διαφόρων ατόμων και να τα ταξινομούν για λογαριασμό του χρήστη. Για παράδειγμα το Facebook χρησιμοποιεί αυτό το σύστημα και κάνει αυτόματη επισήμανση (tagging) στις φωτογραφίες διάφορων προσώπων.

3. Σάρωση Φωνής

   Αυτό το είδος βιομετρικής τεχνικής γίνεται σάρωση της φωνής ενός χρήστη μέσω κάποιας λέξης ή φράσης για την ταυτοποίησή του. Η τεχνική αυτή επιτρέπει την εξ ' αποστάσεως λειτουργία και ταυτοποίηση του χρήστη. Αυτό δηλαδή σημαίνει ότι ο χρήστης μπορεί μέσω του κινητού του τηλεφώνου ή μέσω κάποιου μικροφώνου να κάνει ταυτοποίηση στο σύστημα χωρίς την φυσική του παρουσία.

4. Σάρωση Πατήματος Πλήκτρου

   Η τεχνική αυτή βασίζεται στην δύναμη, στην ταχύτητα αλλά και στον χρόνο που μεσολαβεί μέχρι ο χρήστης να δακτυλογραφήσει κάποιο συγκεκριμένο συνθηματικό. Βασίζεται ουσιαστικά στον τρόπο πληκτρολόγησης του χρήστη.

5. Σάρωση Χεριού

   Η τεχνική αυτή είναι παρόμοια με την τεχνική του προσώπου αφού και εδώ αναγνωρίζονται ορισμένα στοιχεία του χεριού όπως το μήκος των δακτύλων, στο σχήμα του χεριού κ.α. Η τεχνική αυτή δεν είναι απόλυτα ακριβής αλλά χρησιμοποιείται σε αρκετές εφαρμογές με χαμηλό επίπεδο ασφάλειας.

Μερικές από τις προηγούμενες τεχνικές είναι αρκετά αξιόπιστες και άλλες λιγότερο αξιόπιστες. Βασίζονται στα ίδια χαρακτηριστικά του χρήστη και όχι σε αριθμούς. Για το λόγο αυτό η βιομετρική τεχνολογία αναπτύσσει όλο και περισσότερες τεχνικές οι οποίες δεν μπορούν να παραβιαστούν από διάφορους εισβολείς.

3.5 Σύστημα Ανίχνευσης Εισβολής

Σε περίπτωση που ο επιτιθέμενος καταφέρει να εισβάλλει στο σύστημα θα πρέπει να υπάρχει κάποιο σύστημα το οποίο θα αποτρέπει την επίθεση όσο πιο γρήγορα γίνεται αλλά και θα αποκαταστήσει τις ζημιές που προκάλεσε μέχρι στιγμής. Αυτή την δουλειά κάνει το *σύστημα ανίχνευσης εισβολής* το οποίο αποτελεί ένα σύστημα που παρακολουθεί και αναλύει τα συμβάντα που γίνονται στους Η/Υ αλλά και σε δίκτυα υπολογιστών. Εντοπίζει ίχνη παραβίασης της εμπιστευτικότητας, της ακεραιότητας και τις διαθεσιμότητας των πόρων του συστήματος. Υπάρχουν τρία μοντέλα ανίχνευσης τέτοιων επιθέσεων:

3.5.1 Ανίχνευση Υπογραφών

Λειτουργεί παρόμοια όπως και τα συστήματα ανίχνευσης κάποιου ιού (antivirus) που υπάρχει στο σύστημά μας. Η μέθοδος ανίχνευσης υπογραφών στηρίζεται στο γεγονός ότι σε κάθε επίθεση υπάρχει μια μοναδική υπογραφή. Η *υπογραφή* αυτή αποθηκεύεται σε μία βάση δεδομένων [3] στην οποία αργότερα γίνονται συγκρίσεις μεταξύ των αποθηκευμένων υπογραφών. Κύριο θέμα αποτελεί η συνεχής ενημέρωση της βάσης μας έτσι ώστε να γίνεται πιο γρήγορος ο εντοπισμός του εισβολέα.

3.5.2 Ανίχνευση Ανωμαλιών

Ορίζεται ως η αναγνώριση προτύπων π.χ. παρεκκλίσεων, εξαιρέσεων μέσα από ένα σύνολο δεδομένων που λειτουργούν στο σύστημά μας και έχουν διαφορετική συμπεριφορά από την αναμενόμενη. Η διαδικασία λειτουργίας αυτού του συστήματος βασίζεται στην καταγραφή των ροών των δεδομένων και των διαδικασιών δημιουργώντας κάποιο είδος τυποποίησης. Όλες αυτές οι διαδικασίες στοχεύουν στον εντοπισμό των ανωμαλιών που ενδεχομένως να αποτελούν μια εισβολή στο σύστημά μας.

Τα πλεονεκτήματα αυτής της τεχνικής είναι: **α)** Η ενεργοποίηση κάποιου συναγερμού που εμφανίζεται στο σύστημά μας και μας προειδοποιεί για κάποια επίθεση που γίνεται για πρώτη φορά. **β)** Η ευκολία στον εντοπισμό του εισβολέα που παραβίασε τον Η/Υ.

Τα μειονεκτήματα αυτής της τεχνικής είναι: **α)** Δεν δίνεται κάποια εγγύηση ότι σίγουρα μια επίθεση θα ενεργοποιήσει τον συναγερμό και θα μας ενημερώσει για την εξέλιξή της. **β)** Υπάρχει κίνδυνος τα συστήματα να μην έχουν ρυθμιστεί καλά και να μπερδεύουν κάποια νόμιμη ενέργεια του χρήστη σαν μια εισβολή στο σύστημα.

3.5.3 Υβριδικό Μοντέλο

Το σύστημα αυτό είναι υπεύθυνο για τον εντοπισμό των ανωμαλιών και των δεδομένων που έχουν κακόβουλο περιεχόμενο και είναι επιβλαβή για τον Η/Υ. Εστιάζει στις απειλές που πιθανόν να προέρχονται και από το εσωτερικό περιβάλλον π.χ. σε κάποια εταιρεία εστιάζονται απειλές που πιθανόν να προέρχονται και από τους ίδιους υπαλλήλους που εργάζονται

[3] Με τον όρο βάση δεδομένων εννοούμε μία συλλογή από δεδομένα τα οποία δημιουργούν σχέσεις μεταξύ τους. Καταχωρούμε οποιοδήποτε δεδομένο χρειαζόμαστε στο σύστημά μας και έπειτα μέσω κάποιων ερωτήσεων που θέτουμε στην βάση μπορούμε να έχουμε οποιοδήποτε αποτέλεσμα θελήσουμε.

εκεί. Τοποθετείται το κατάλληλο λογισμικό σε έναν μόνο υπολογιστή και παρακολουθείται η δραστηριότητα του χρήστη.

3.6 Αντιδράσεις Συστημάτων Ανίχνευσης Εισβολής

Εφόσον εντοπιστεί κάποια επίθεση το σύστημά μας κάνει ορισμένες διαδικασίες που του έχουν ρυθμιστεί για την αντιμετώπισή της. Οι αντιδράσεις των συστημάτων αυτών διακρίνονται σε δύο κατηγορίες: **1)** Ενεργητικές και **2)** Παθητικές.

Από την στιγμή όπου το σύστημα θα εντοπίσει κάποια επίθεση οι ενεργητικές αντιδράσεις του περιλαμβάνουν μία σειρά από καθορισμένες ενέργειες για την αντιμετώπισή του. Σε περίπτωση που το ίδιο το σύστημα δεν είναι σίγουρο για την ζημιά που θα προκαλέσει μια επίθεση τότε δεν αντιδρά, αλλά συγκεντρώνει πληροφορίες και μετά αντιδρά στην επίθεση. Μόλις γίνουν τα παραπάνω ενεργοποιεί το τείχος προστασίας στον υπολογιστή και εμποδίζει την εισβολή στο δίκτυο.

Στις παθητικές αντιδράσεις το σύστημα αυτό δεν κάνει καμία ενέργεια για την παρεμπόδιση της εισβολής. Ενημερώνει μόνο τον υπεύθυνο ασφαλείας για την εισβολή. Έπειτα αξιολογείτε η ζημία και οποιεσδήποτε περαιτέρω ενέργειες γίνονται μόνο από το χρήστη.

3.6.1 Κατηγορίες Συστημάτων Ανίχνευσης Εισβολής

Στα *συστήματα ανίχνευσης εισβολής* εντάσσονται και κάποια άλλα εργαλεία που κάνουν ακριβώς την ίδια δουλειά και είναι απλά στην λειτουργία τους. Αυτά είναι: **1)** Τα συστήματα ελέγχου ακεραιότητας και **2)** τα συστήματα παρακολούθησης των αρχείων καταγραφής.

Στα *συστήματα ελέγχου ακεραιότητας* εξετάζεται η λειτουργία ορισμένων κρίσιμων αρχείων όπως τα αρχεία του συστήματός μας και εντοπίζονται οποιεσδήποτε μεταβολές έχουν γίνει σε αυτά. Μπορούν επίσης να παρακολουθούν και τους λογαριασμούς των χρηστών του Η/Υ και να εντοπίζουν εάν κάποιος χρήστης έχει αλλάξει τα δικαιώματα που διαθέτει και έχει αποκτήσει δικαιώματα διαχειριστή ενός Η/Υ. Τέτοια δικαιώματα είναι ο πλήρης έλεγχος του Η/Υ, η ανάγνωση, η εγγραφή, ποιούς φακέλους μπορεί να ανοίξει και ποιούς δεν μπορεί κ.α.

Στα *συστήματα παρακολούθησης των αρχείων καταγραφής* δημιουργείται ένας φάκελος από τα αρχεία καταγραφής των υπηρεσιών του δικτύου. Έπειτα καταγράφονται όλες οι καθημερινές λειτουργίες του συστήματος και προσπαθούν να εντοπίσουν διάφορα είδη επιθέσεων.

3.7 Έλεγχος Συστήματος

Σύμφωνα με τα παραπάνω τα αρχεία καταγραφής έχουν την δυνατότητα να εντοπίσουν κάποια επίθεση. Σε κάθε λειτουργικό σύστημα που υπάρχει σε οποιονδήποτε υπολογιστή υπάρχουν εργαλεία ελέγχου τα οποία στοχεύουν στην ενημέρωση του χρήστη για τα συμβάντα που λαμβάνουν χώρα στον προσωπικό του υπολογιστή. Στις επαγγελματικές εκδόσεις ορισμένων λειτουργικών συστημάτων της Microsoft υπάρχουν τα παρακάτω:

α) System Log το οποίο είναι κάποιο αρχείο όπου καταγράφονται προειδοποιήσεις, σφάλματα που σχετίζονται με το σύστημά μας και δημιουργήθηκαν από το λειτουργικό

σύστημα.

β) Security Log όπου καταγράφονται ορισμένα αρχεία που έχουν σχέση με τον έλεγχο που έχει καθορίσει ο διαχειριστής του συστήματος μας.

γ) Application Log το όποιο είναι ένα αρχείο που περιέχει μηνύματα και πληροφορίες και γεγονότα σχετικά με την κατάσταση ορισμένων υπηρεσιών του λειτουργικού συστήματος.

3.7.1 Διαδικασία Αντιμετώπισης Καταστροφών

Η πρόληψη και η αντιμετώπιση κάποιου είδους απειλής στο σύστημά μας εφόσον έχει εντοπιστεί αποτελούν δύο βασικούς παράγοντες σύμφωνα με τους οποίους προλαβαίνουμε τις περισσότερες ζημιές στον Η/Υ. Υπάρχουν και άλλες περιπτώσεις στις οποίες η πρόληψη και η αντιμετώπιση μιας επίθεσης δεν μπορούν να εμποδίσουν τον εισβολέα. Εφόσον ο εισβολέας έχει καταφέρει να εισχωρήσει στο σύστημά μας τότε αρχίζει και ο υπολογισμός του μεγέθους τις ζημιάς που έχει προκαλέσει. Εδώ έρχεται η διαδικασία αντιμετώπισης καταστροφών μέσω τις οποίας ορίζονται κάποιες διαδικασίες που μπορούμε να κάνουμε έτσι ώστε να εξασφαλίσουμε την ασφάλεια στο σύστημά μας.

Αρχικά είναι απαραίτητο να αποθηκεύουμε τα αρχεία και τους φακέλους που υπάρχουν στον υπολογιστή μας σε διάφορες μονάδες αποθήκευσης όπως (usb flash drive, οπτικοί δίσκοι) για να προλάβουμε μια ενδεχόμενη απειλή που πιθανόν να παρουσιαστεί στον υπολογιστή μας. Η μέθοδος αυτή είναι εξαιρετικά σημαντική σε πολλούς οργανισμούς που περιέχουν σημαντικά αρχεία που δεν πρέπει να χαθούν ή να αλλοιωθούν.

Εκτός όμως από μια ενδεχόμενη επίθεση πρέπει να λάβουμε υπ' όψιν μας και άλλα φυσικά αίτια που θα δημιουργήσουν ζημιές στο σύστημά μας. Αυτά είναι α) μια πυρκαγιά, β) ένας σεισμός, γ) μια πλημμύρα και δ) η κλοπή του υπολογιστή. Όλα αυτά αποτελούν ορισμένα σημαντικά ζητήματα στον τομέα της ασφάλειας ενός υπολογιστικού συστήματος διότι η απώλεια των δεδομένων ενός οργανισμού μπορεί να οδηγήσει μέχρι την οικονομική καταστροφή του.

Το *σύστημα ανάνηψης από καταστροφές* αποτελεί κύριο χαρακτηριστικό ενός οργανισμού ο οποίος θέλει να προστατέψει τα δεδομένα του από διάφορα είδη διαρροών και απωλειών. Το σύστημα αυτό αποτελείται από διάφορα υποσυστήματα σύμφωνα με τα οποία διασφαλίζεται η ακεραιότητα όλων των δεδομένων. Οι λειτουργίες του συστήματος αυτού εξαρτώνται από τα εξής:

1. **Το είδος των δεδομένων που είναι προς αποθήκευση**

   Ανάλογα με τις ανάγκες κάθε οργανισμού αλλά και με το χρηματικό ποσό που διαθέτει αποθηκεύει τα δεδομένα που θέλει. Για παράδειγμα, κάποια μικρή επιχείρηση θα αποθηκεύσει μόνο κάποια σημαντικά αρχεία σε αντίθεση με κάποιον μεγάλο οργανισμό που θα αποθηκεύσει περαιτέρω δεδομένα.

2. **Την συχνότητα αποθήκευσης των δεδομένων**

   Αναφέρεται στον ρυθμό σύμφωνα με τον οποίο αλλάζουν τα δεδομένα, η συνολική ποσότητα των δεδομένων που απαιτείται λήψη εφεδρικών αντιγράφων και το μέσο αποθήκευσης των αντιγράφων αυτών.

3. **Το σημείο όπου γίνεται η αποθήκευση των αρχείων**

   Η αποθήκευση των δεδομένων μπορεί να γίνει και σε τοπικούς δίσκους. Περιλαμβάνει την ασφάλεια των δεδομένων αυτών και την δυνατότητα διατήρησης των αρχείων σε καλή κατάσταση. Εφόσον υπάρχει η οικονομική δυνατότητα κάποιου οργανισμού μπορούν να υπάρχουν και εφεδρικοί υπολογιστές στους οποίους γίνεται η αποθήκευση των βασικών δεδομένων των υπολογιστών.

Μέρος του συστήματος αυτού είναι και η λήψη εφεδρικών αντιγράφων. Σε μια επιχείρηση ή και σε έναν οργανισμό δεν αρκεί μόνο ένα σύστημα ανάνηψης από καταστροφές, απαιτείται και η λήψη εφεδρικών αντιγράφων. Στα *εφεδρικά αντίγραφα* μεταφέρονται τα δεδομένα από όλα τα αρχεία που υπάρχουν στον σκληρό δίσκο του Η/Υ. Έτσι εάν ο σκληρός δίσκος πάθει κάποια βλάβη η οποία δεν διορθώνεται, μπορεί να γίνει πλήρη αποκατάσταση των δεδομένων σε κάποιον καινούργιο δίσκο.

4.1 Εισαγωγή

Η ηλεκτρονική εγκληματικότητα αποτελεί ζήτημα υψίστης ασφαλείας στην σημερινή εποχή. Η εξέλιξη της τεχνολογίας των υπολογιστών εμφανίζει καθημερινά όλο και νέες μορφές ηλεκτρονικών εγκλημάτων. Στην χώρα μας έχει δημιουργηθεί μία υπηρεσία που ερευνά υποθέσεις ηλεκτρονικών εγκλημάτων.

Αποτελεί τομέα της Ελληνικής Αστυνομίας και είναι η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ). Αποτελείται από δύο τμήματα, το ένα εδρεύει στην Αθήνα και το άλλο στην Θεσσαλονίκη. Αποστολή της είναι η πρόληψη, η έρευνα και η καταστολή των εγκλημάτων που λαμβάνουν χώρα στο διαδίκτυο.

Στο παρακάτω σχήμα 4.1 παρατηρούμε την διεύθυνση του τμήματος της *δίωξης ηλεκτρονικού εγκλήματος* έτσι ώστε να μπορεί ο κάθε πολίτης να ενημερώνεται καθημερινά για τις διάφορες επιθέσεις που γίνονται αλλά ταυτοχρόνως μπορεί και να καταγγέλλει οποιαδήποτε μορφή ηλεκτρονικού εγκλήματος διαπράχθηκε απέναντί του.

Τηλέφωνο: 11188
Fax: 210 6476462
Email: ccu@cybercrimeunit.gov.gr
Facebook: www.facebook.com/cyberkid.gov.gr
Twitter: @cyberalertGR
Ιστότοπος 1: www.cyberkid.gr
Ιστότοπος 2: www.cyberalert.gr
Ταχυδρομική Διεύθυνση: Λ.Αλεξάνδρας 173, Τ.Κ. 11522, Αθήνα

Σχήμα 4.1: *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος*

Αποτελεί μία σημαντική και πολύ καλά δομημένη υπηρεσία στην χώρα μας. Έχει καταφέρει να αποτρέψει και να εξιχνιάσει πάρα πολλά είδη ηλεκτρονικών εγκλημάτων τα οποία απειλούν της ασφάλειά μας στο διαδίκτυο. Επίσης ενημερώνει τους πολίτες αλλά και τους εφήβους μέσω διαφόρων ημερίδων για την ασφαλή πλοήγησή τους στο χώρο του *διαδικτύου*.

Το τμήμα που εδρεύει στην Αθήνα ιδρύθηκε το έτος 2004. Μέχρι τότε οι υποθέσεις αντιμετωπίζονταν από ένα άλλο τμήμα της *Ελληνικής Αστυνομίας*, το τμήμα Δίωξης Οικονομικού Εγκλήματος. Το έτος 2014 ιδρύθηκε στην Θεσσαλονίκη η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος η οποία μαζί με το τμήμα στην Αθήνα αποτελεί μία αυτοτελής κεντρική υπηρεσία η οποία υπάγεται απευθείας στον Αρχηγό της *Ελληνικής Αστυνομίας*.

4.2 Λειτουργίες και Αρμοδιότητες Δίωξης Ηλεκτρονικού Εγκλήματος

Η ΔΙΔΗΕ [20] αποτελείται από πέντε επιμέρους τμήματα σύμφωνα με τα οποία το καθένα ξεχωριστά συμβάλλει στην προστασία των χρηστών του διαδικτύου και στην ασφάλεια του κυβερνοχώρου. Τα τμήματα αυτά είναι τα εξής:

1. **Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών**

   Στο τμήμα αυτό λειτουργεί Κέντρο Επιχειρήσεων το οποίο συμβάλλει στο συντονισμό αλλά και στην επικοινωνία ολόκληρου του προσωπικού του τμήματος. Λειτουργεί σε 24ωρη βάση τηλεφωνικό κέντρο στο οποίο υπάρχει μία ειδική γραμμή καταγγελιών και μια διεύθυνση (e - mail) έτσι ώστε να μπορούν οι πολίτες οποιαδήποτε στιγμή να επικοινωνήσουν με την Υπηρεσία.

   Αρμοδιότητες αυτού του τμήματος είναι: **Α)** Διοικητική και Τεχνική υποστήριξη στις λειτουργικές ανάγκες της υπηρεσίας, **Β)** Συλλογή, Μελέτη, Ανάλυση όλων των επεξεργασμένων πληροφοριών και δεδομένων και έπειτα προώθηση των στοιχείων αυτών στα αρμόδια τμήματα για την περαιτέρω αξιοποίησή τους, **Γ)** Η συνεχής εκπαίδευση του προσωπικού της Διεύθυνσης στην καταπολέμηση του ηλεκτρονικού εγκλήματος μέσω διαφόρων εκπαιδευτικών προγραμμάτων καθώς και στην συνεργασία με άλλους φορείς της χώρας.

2. **Τμήμα Καινοτόμων Δράσεων και Στρατηγικής**

   Αρμοδιότητες του τμήματος Καινοτόμων Δράσεων και Στρατηγικής είναι οι ακόλουθες: **Α)** Η δημοσιοποίηση του έργου ολόκληρης της Υπηρεσίας σε διάφορες ιστοσελίδες κοινωνικής δικτύωσης όπως π.χ. (Twitter, Facebook κ.λπ.) με σκοπό την ενημέρωση αλλά και την ευαισθητοποίηση των πολιτών σε διάφορες μορφές ηλεκτρονικών εγκλημάτων, **Β)** Δημιουργία συνεδρίων, ημερίδων καθώς και άλλες καινοτόμες δράσεις που αφορούν την καταπολέμηση του *ηλεκτρονικού εγκλήματος*,

   Γ) Παρακολούθηση όλων των εξελίξεων που έχουν σχέση με το *ηλεκτρονικό έγκλημα* σε εσωτερικό αλλά και σε διεθνές επίπεδο, **Δ)** Υποβολή συγκεκριμένων προτάσεων για την αντιμετώπισή του, **Ε)** Καταγραφή στατιστικών στοιχείων αναφορικά με τα είδη *ηλεκτρονικών εγκλημάτων* στην χώρα μας και με την συχνότητα εμφάνισής τους.

3. **Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων**

   Το Τμήμα αυτό είναι αρμόδιο **Α)** Για το χειρισμό διαφόρων υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε διάφορα υπολογιστικά συστήματα, **Β)** Για την κλοπή και παράνομη διακίνηση λογισμικού υλικού που προστατεύεται από πνευματικά δικαιώματα, **Γ)** Την διενέργεια διαδικτυακής έρευνας με σύγχρονο τεχνολογικό εξοπλισμό για την διερεύνηση σοβαρών αδικημάτων και υποθέσεων που συμβαίνουν στην χώρα μας.

4. **Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης**

   Σκοπός του τμήματος αυτού είναι **Α)** Η εξιχνίαση και δίωξη διαφόρων εγκλημάτων που έχουν κατά κύριο στόχο ανήλικα άτομα με την βοήθεια του *διαδικτύου*, **Β)** Διερεύνηση υποθέσεων διαδικτυακής παρενόχλησης χρηστών του διαδικτύου όπως το φαινόμενο του ρατσισμού με σκοπό την αποτροπή αυτοκτονιών ή εξαφανίσεων μέσω του διαδικτύου, **Γ)** Παροχή βοήθειας σε Κρατικές Υπηρεσίες που ερευνούν υποθέσεις για διάφορα είδη εγκλημάτων που τελούνται στο χώρο του *διαδικτύου*.

5. **Τμήμα Ειδικών Υποθέσεων και Διαδικτυακών Οικονομικών Εγκλημάτων**

   Αρμοδιότητες του τμήματος αυτού είναι: **Α)** Η καταπολέμηση οικονομικών εγκλημάτων που έγιναν στο *διαδίκτυο* τόσο σε εθνικό όσο και σε διεθνές επίπεδο με την συνεργασία διαφόρων υπηρεσιών και έχουν ως σκοπό οικονομικά συμφέροντα κατά του δημοσίου και αποτελούν ένα οργανωμένο οικονομικό έγκλημα στο οποίο για την διερεύνησή του απαιτούνται εξειδικευμένες γνώσεις, **Β)** Συνεχής έρευνα στο χώρο του *διαδικτύου* για την ανακάλυψη και άλλων μορφών ηλεκτρονικών εγκλημάτων τα οποία διαπράττονται σε ολόκληρη την Χώρα.

4.2.1 Στατιστικά Στοιχεία Έτους 2014

Το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στο σχήμα 4.2 που ακολουθεί παρατηρούμε ότι το έτος 2014 το 33 τοις εκατό αφορά υποθέσεις για διάφορες απάτες μέσω του διαδικτύου όπως π.χ. ηλεκτρονικό ψάρεμα, ηλεκτρονικό ταχυδρομείο κ.α, το 11 τοις εκατό αφορά προθέσεις αυτοκτονίας ατόμων κάτι το οποίο απέτρεψε η ΔΙΔΗΕ να συμβεί, το 10 τοις εκατό αφορά υποθέσεις σχετικά με την πορνογραφία ανηλίκων, το 9 τοις εκατό αφορά παραβιάσεις προσωπικών δεδομένων, το 7 τοις εκατό αφορά απειλές σε βάρος χρηστών του διαδικτύου, το 5 τοις εκατό είναι για υποθέσεις σχετικά με την παράνομη πρόσβαση σε διάφορα υπολογιστικά συστήματα και το υπόλοιπο 25 τοις εκατό αφορά διάφορα άλλα αδικήματα που τελούνται στο χώρο του διαδικτύου.

Σχήμα 4.2: *Υποθέσεις ΔΙΔΗΕ έτους 2014*

4.3 Εντοπισμός Ηλεκτρονικού Εγκληματία

4.3.1 Εισαγωγή

Οι αρχές που κάνουν διερεύνηση διαφόρων μορφών ηλεκτρονικών εγκλημάτων έχουν βασικό στόχο την ανακάλυψη των δραστών ή του δράστη που διέπραξε το έγκλημα, καθώς και την συγκέντρωση αποδεικτικών στοιχείων και ιχνών έτσι ώστε και από την νομική σκοπιά να μπορέσει να τεκμηριωθεί το αποτέλεσμα.

Στην σημερινή εποχή οι δράστες εκμεταλλεύονται τις δυνατότητες που τους δίνει το διαδίκτυο και με διάφορους τρόπους καταφέρνουν να διατηρήσουν την ανωνυμία τους και με αυτόν τον τρόπο να αποφύγουν την σύλληψή τους για κάποια ηλεκτρονική απάτη που διέπραξαν.

Από την άλλη σκοπιά όμως η εξέλιξη της τεχνολογίας βοηθάει το έργο των αρμόδιων αρχών αφού υπάρχουν πολλοί τρόποι εξακρίβωσης του πραγματικού ενόχου. Παρακάτω αναλύονται μερικοί τρόποι εντοπισμού του ηλεκτρονικού εγκληματία από τις αρμόδιες υπηρεσίες της χώρας μας.

4.3.2 Αρχεία Καταγραφής (Log Files)

Είναι αρχεία μέσα στα οποία αποθηκεύονται πληροφορίες σχετικά με τις λειτουργίες του συστήματος. Συντάσσει σε ένα κατάλογο όλες τις ενέργειες που έγιναν στο σύστημα. Το αρχείο αυτό είναι χρήσιμο στην παρακολούθηση ενός Η/Υ καθώς και στην ανάκτηση δεδομένων σε περίπτωση κάποιας ανάγκης.

Οι ερευνητές των ηλεκτρονικών εγκλημάτων μέσα από αυτά τα αρχεία μπορούν να διαπιστώσουν εάν κάποιος χρήστης χρησιμοποίησε κάποια εφαρμογή, εάν κάποιος μη εξουσιοδοτημένος χρήστης εισέβαλε στο σύστημα και άλλες σημαντικές πληροφορίες.

Εκτός όμως από το λειτουργικό σύστημα, δημιουργούνται αρχεία καταγραφής και από διάφορες άλλες εφαρμογές. Το τείχος προστασίας [1] (firewall) αποθηκεύει πολλές πληροφορίες στα αρχεία καταγραφής του. Μέσω αυτών των πληροφοριών αποτελούν βασικό αποδεικτικό υλικό σε αρκετές περιπτώσεις στις οποίες έχουμε κάποια μη εξουσιοδοτημένη πρόσβαση σε κάποιο δίκτυο.

4.3.3 Συναγερμοί (Alarms)

Το τείχος προστασίας [21] του υπολογιστή εφόσον διαπιστώσει ότι κάποια ύποπτη δραστηριότητα συμβαίνει στο υπολογιστή αποστέλλει μηνύματα σε συγκεκριμένους παραλήπτες. Τα μηνύματα αυτά στέλνονται μέσω του ηλεκτρονικού ταχυδρομείου στον διαχειριστή του Η/Υ ενώ παράλληλα ολόκληρη η δραστηριότητα καταγράφεται στα αρχεία καταγραφής.

Μέσω αυτών οι αρμόδιες αρχές μπορούν να βγάλουν χρήσιμα συμπεράσματα αλλά και να ανακαλύψουν και τον πραγματικό δράστη που τέλεσε το συγκεκριμένο αδίκημα. Αυτή η λειτουργία του τείχους προστασίας είναι εξαιρετικά σημαντική διότι μπορεί να αποτρέψει μία ενδεχόμενη επίθεση πριν ακόμη διαπραχθεί.

[1] Ο όρος τείχος προστασίας στην επιστήμη της πληροφορικής είναι κάποια συσκευή ή κάποιο πρόγραμμα το οποίο είναι ρυθμισμένο για να επιτρέπει αλλά και να απορρίπτει για αποστολή πακέτα με δεδομένα μεταξύ δύο δικτύων υπολογιστών.

4.3.4 Εντοπισμός Ονόματος Χώρου και Διεύθυνσης IP

Ο εντοπισμός μιας διεύθυνσης IP [2] αποτελεί μία βασική ενέργεια των αρχών έτσι ώστε να φτάσουν στην εξιχνίαση υποθέσεων ηλεκτρονικού εγκλήματος. Στις επιθέσεις αυτές οι επιτήδειοι χρησιμοποιούν πλαστές διευθύνσεις για να παραπλανήσουν τις αρμόδιες αρχές. Κάθε διεύθυνση στο διαδίκτυο έχει και ένα αριθμό IP.

Σε μια επίθεση ο εισβολέας καταφέρνει να πλαστογραφήσει την διεύθυνσή του, όχι όμως τον αριθμό IP ο οποίος είναι μοναδικός για κάθε συσκευή που συνδέεται στο δίκτυο. Συσκευές όπως το τείχος προστασίας (firewall) μπορούν και ελέγχουν εάν μια διεύθυνση είναι αληθινή ή όχι και έτσι δίνουν τη δυνατότητα σε κάποιον να έχει πρόσβαση στον Η/Υ. Επιπλέον υπάρχουν διάφορα εργαλεία σύμφωνα με τα οποία ο ερευνητής μπορεί να ελέγξει εάν οι ηλεκτρονικές διευθύνσεις όσων απέκτησαν πρόσβαση στον Η/Υ αναλογούν σε γνήσιους αριθμούς IP.

4.3.5 Προειδοποιήσεις (Alerts), Αναφορές (Reports)

Σε περίπτωση εκδήλωσης κάποιας επίθεσης ειδοποιείται με ένα μήνυμα ηλεκτρονικού ταχυδρομείου (e - mail) ο διαχειριστής του συστήματός μας μέσω κάποιας προειδοποίησης [22] (Alerts). Σε αντίθετη περίπτωση μία αναφορά δίνει αρκετές πληροφορίες για την επίθεση που προκλήθηκε στο σύστημά μας. Όπως τον αριθμό των αποτυχημένων προσπαθειών για απόκτηση πρόσβασης στον Η/Υ, την συχνότητα των σφαλμάτων κ.α.

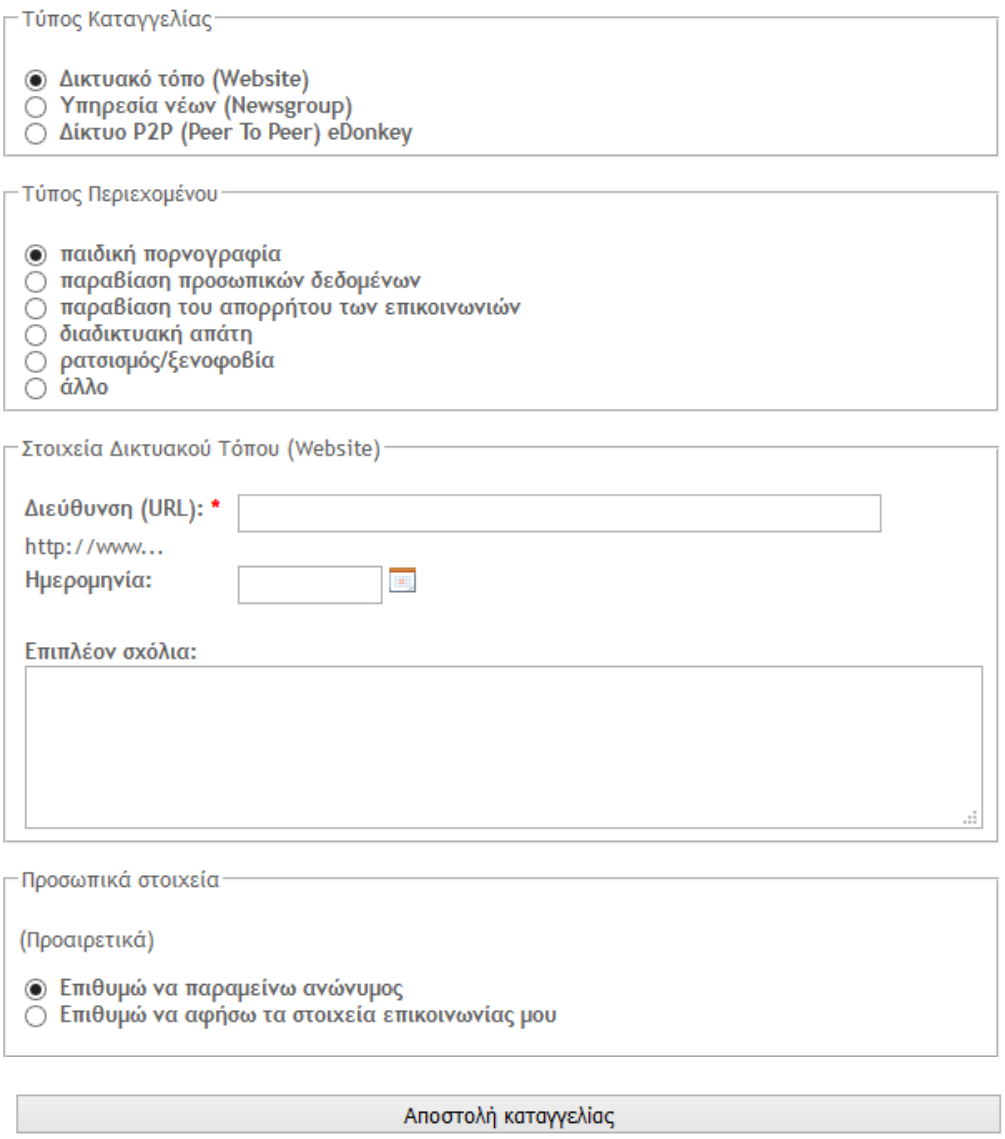
4.4 Διεθνής Γραμμή Καταγγελιών

Η ιστοσελίδα **www.safeline.gr** αποτελεί μια διεθνής γραμμή καταγγελιών [1] η οποία δέχεται καταγγελίες για παράνομο περιεχόμενο που υπάρχει στο διαδίκτυο. Ξεκίνησε να λειτουργεί στις 14 Απριλίου 2003. συνεργάζεται με την Ελληνική Αστυνομία, με Ερευνητικά Ιδρύματα, με το Σχολικό Δίκτυο κ.λπ. Κύριος στόχος της είναι εικόνες κακοποιημένων παιδιών που κυκλοφορούν στο διαδίκτυο, οποιαδήποτε μορφή εγκλήματος που διαπράττεται στον κυβερνοχώρο καθώς και η μέριμνα για την ασφάλεια των παιδιών στο διαδίκτυο.

Μέσω αυτής της ηλεκτρονικής διεύθυνσης μπορεί κάποιος να κάνει μία καταγγελία σχετικά με το περιεχόμενο που θεωρείτε παράνομο στο χώρο του διαδικτύου. Αυτό μπορεί να γίνει **1)** είτε στέλνοντας e - mail στη ηλεκτρονική διεύθυνση **report@safeline.gr**, είτε **2)** συμπληρώνοντας την φόρμα υποβολής καταγγελίας που φαίνεται στην εικόνα 4.1.

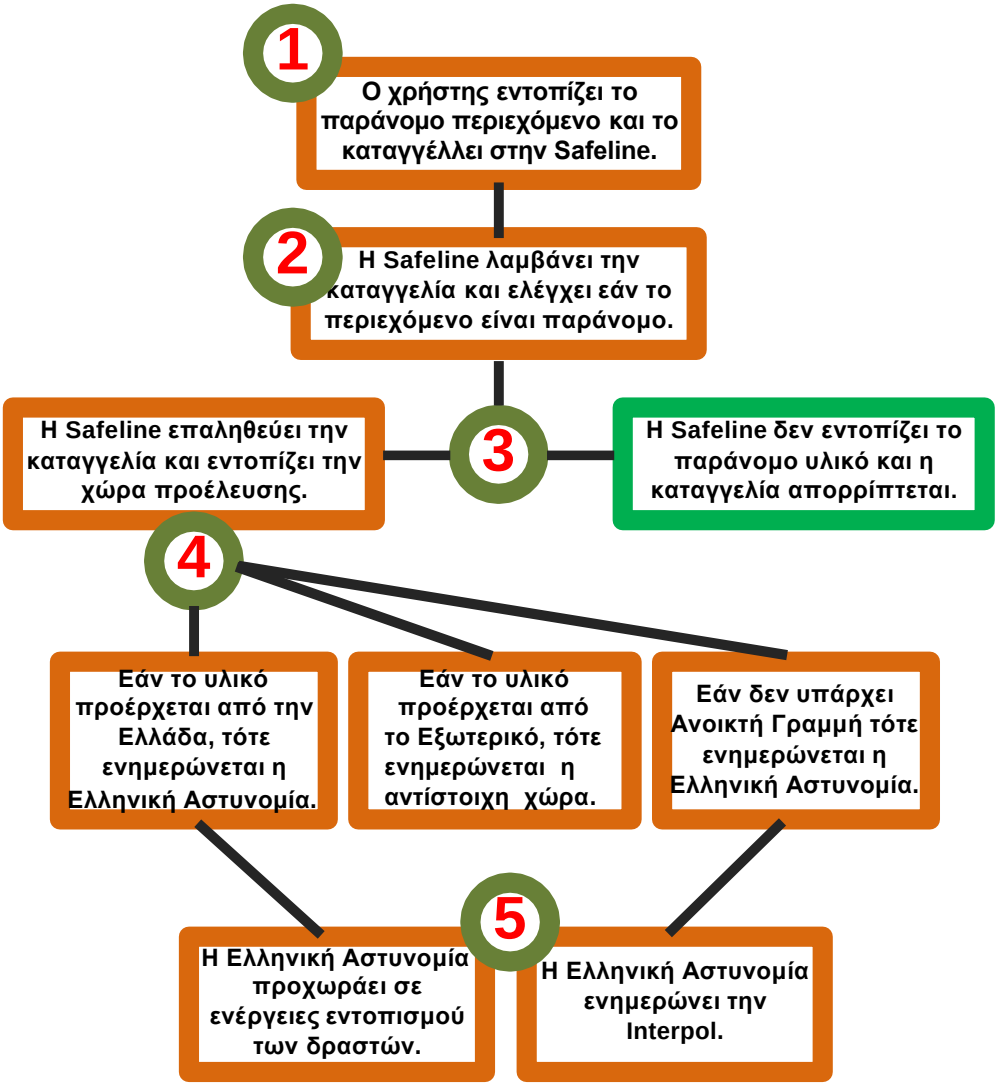
Αρχικά συμπληρώνουμε τον τύπο της καταγγελίας που θέλουμε να κάνουμε εδώ έχουμε επιλέξει για τύπο καταγγελίας έναν δικτυακό τόπο, έπειτα επιλέγουμε το περιεχόμενο της καταγγελίας μας π.χ. παιδική πορνογραφία, επιπλέον συμπληρώνουμε την ηλεκτρονική διεύθυνση του ιστότοπου καθώς και μερικά σχόλια που εμείς θεωρούμε σημαντικά και τέλος μπορούμε είτε να στείλουμε την καταγγελία ανώνυμα, είτε να συμπληρώσουμε τα προσωπικά μας στοιχεία και έπειτα επιλέγουμε το εικονίδιο αποστολή της καταγγελίας μας.

[2] Είναι ένας μοναδικός αριθμός ο οποίος χρησιμοποιείται από πολλές συσκευές και χρησιμεύει στην μεταξύ τους αναγνώριση σε ένα δίκτυο υπολογιστών.



Εικόνα 4.1: *Φόρμα Καταγγελιών Safeline [1]*

Αφού η Safeline λάβει μία καταγγελία στο παρακάτω σχήμα 4.3 περιγράφεται η διαδικασία που ακολουθείται. **1)** Όταν κάποιος χρήστης εντοπίσει το παράνομο περιεχόμενο, το καταγγέλλει στην Safeline. **2)** Στο επόμενο βήμα γίνεται κάποιος έλεγχος από την Safeline για να εξακριβώσει εάν όντως υπάρχει κάποιο παράνομο περιεχόμενο. **3)** Εάν δεν εντοπίσει κάποιο παράνομο περιεχόμενο απορρίπτει την καταγγελία. Εάν όμως εντοπίσει τότε βρίσκει την χώρα προέλευσής του. **4)** Εάν το περιεχόμενο έρχεται από την χώρα μας τότε ενημερώνεται η Ελληνική Αστυνομία, εάν έρχεται από το Εξωτερικό ενημερώνεται η αντίστοιχη Ανοικτή Γραμμή της αρμόδιας χώρας, εάν δεν υπάρχει ανοικτή Γραμμή κάποιας χώρας ενημερώνεται η Ελληνική Αστυνομία, η οποία με την σειρά της **5)** θα ενημερώσει την Interpol. Εάν το περιεχόμενο προέρχεται από την χώρα μας η Αστυνομία κάνει έρευνες εντοπισμού των δραστών.



Σχήμα 4.3: *Διαδικασία Επεξεργασίας Καταγγελιών Safeline*

4.5 Ιστότοπος Δίωξης Ηλεκτρονικού Εγκλήματος

Το Υπουργείο Εσωτερικών μαζί με την Ελληνική Αστυνομία και τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος δημιούργησαν έναν ιστότοπο με το όνομα **www.cyberalert.gr** στον οποίο καταγράφονται οι διάφοροι κίνδυνοι που αντιμετωπίζουν καθημερινά οι χρήστες του διαδικτύου.

Στόχος της ιστοσελίδας αυτής είναι η συνεχής ενημέρωση των πολιτών για τις νέες μορφές ηλεκτρονικού εγκλήματος που εμφανίζονται καθημερινά στο διαδίκτυο καθώς και η προστασία των χρηστών από όλους αυτούς τους κινδύνους εφόσον ενημερώσουν τις διωκτικές αρχές ταχύτατα και ουσιαστικά.

4.5.1 Ημερίδες Ασφαλούς Πλοήγησης

Η *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος* και το Αρχηγείο της Ελληνικής Αστυνομίας έχουν διοργανώσει διάφορες ενημερωτικές ημερίδες [23] σε αρκετές πόλεις της χώρας

μας. Στόχος αυτών των ημερίδων είναι η ενημέρωση των μαθητών, των γονέων και των εκπαιδευτικών για τα διάφορα φαινόμενα διαδικτυακής βίας που υπάρχουν σε αρκετές σελίδες κοινωνικής δικτύωσης όπως π.χ. το Facebook, το Twitter κ.α.

Επιπλέον μας ενημερώνει για τους διάφορους κινδύνους που εμφανίζονται με την συνεχής εξέλιξη των υπολογιστών. Από το έτος 2011 έως σήμερα έχουν πραγματοποιηθεί 135 ενημερωτικές ημερίδες σε διάφορες πόλεις στην χώρα μας.

4.5.2 Συνέδρια σε Πανευρωπαϊκό Επίπεδο

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο διαδίκτυο [24], σύμφωνα με την (ΔΙΔΗΕ) έχουν πραγματοποιηθεί τέσσερα συνέδρια στα οποία παρουσιάζονται από εξειδικευμένους επιστήμονες της Ελλάδας αλλά και του Εξωτερικού θέματα σχετικά με την ασφάλεια κατά την πλοήγησή μας στο *διαδικτύο*. Επιπλέον αναπτύχθηκαν θεματολογίες σχετικά με τις εξελίξεις στο τομέα της πληροφορικής καθώς και στην νομοθεσία που υπάρχει για τα αδικήματα που διαπράττονται στον κυβερνοχώρο. Τα συνέδρια αυτά μεταδίδονταν και από την ιστοσελίδα της Ελληνικής Αστυνομίας.

Τα συνέδρια αυτά είναι διαθέσιμα σε ηλεκτρονική μορφή στην ιστοσελίδα της Ελληνικής Αστυνομίας και δίνεται η δυνατότητα στους πολίτες να τα κατεβάσουν στον Η/Υ και να ενημερωθούν για τις εξελίξεις αυτές.

4.5.3 Τηλεδιάσκεψη με Σχολικές Μονάδες

Μέσω της τεχνολογίας των τηλεδιασκέψεων [3] πραγματοποιούνται ενημερώσεις σε αρκετά σχολεία σε όλη την επικράτεια στα οποία γίνεται μία παρουσίαση θεμάτων που αφορούν την ασφάλεια και την προστασία των παιδιών στο διαδίκτυο. Τα σχολεία συμμετέχουν στην τηλεδιάσκεψη μέσω της πλατφόρμας του Πανελλήνιου Σχολικού Δικτύου. Γίνεται δηλαδή μια συνομιλία μεταξύ ομιλητών και ακροατών οι οποίοι βρίσκονται σε απόσταση.

[3] Ο όρος τηλεδιάσκεψη στο τομέα της πληροφορικής ονομάζεται η ταυτόχρονη συνάντηση από απόσταση μέσω του διαδικτύου. Υπάρχουν διάφορες πλατφόρμες ανοικτού λογισμικού για τηλεδιάσκεψη π.χ. Skype, meeting.sch.gr κ.α.

5.1 Εισαγωγή

Ο ηλεκτρονικός υπολογιστής και το διαδίκτυο αποτελούν ένα ισχυρό μαθησιακό εργαλείο στην σημερινή εποχή. Καθημερινά πολλά ανήλικα άτομα χρησιμοποιούν το *διαδίκτυο*. Μερικοί από τους λόγους που το χρησιμοποιούν είναι: **1)** Για να ψάξουν για εκπαιδευτικό υλικό, **2)** Για ενημέρωση, **3)** Για να συνδεθούν σε διάφορα κοινωνικά δίκτυα όπως (Facebook, Twitter) κ.α, **4)** Για να ακούσουν μουσική, **5)** Για να παίξουν παιχνίδια.

Όλοι όμως αυτοί οι λόγοι ενέχουν αρκετούς κινδύνους για την ασφάλεια των παιδιών. Στο *διαδίκτυο* έχει καταργηθεί κάθε εμπόδιο ανταλλαγής πληροφοριών μέσω των διαφόρων χρηστών του και με αυτόν τον τρόπο μπορούν να έχουν πρόσβαση σε οποιαδήποτε πληροφορία θελήσουν ανήλικα άτομα. Έχουν καταγραφεί αρκετά περιστατικά εξαπάτησης παιδιών από διάφορους επιτήδειους οι οποίοι δρουν ανενόχλητοι και επιτυγχάνουν τους στόχους τους.

Ο εθισμός των νέων στο *διαδίκτυο* αποτελεί ένα σημαντικό πρόβλημα σε κάθε οικογένεια. Η πολύωρη χρήση του Η/Υ και του *διαδικτύου* μπορούν να προκαλέσουν αρκετά προβλήματα στις κοινωνικές σχέσεις των ατόμων. Για τον λόγο αυτό πρέπει να υπάρχει έλεγχος των εφήβων και ιδιαίτερα των ανηλίκων που χρησιμοποιούν τον Η/Υ από τους γονείς για την εξάλειψη σημαντικών προβλημάτων που αργότερα θα επηρεάσουν την προσωπικότητα κάθε ατόμου.

5.1.1 Θετικά Στοιχεία του Διαδικτύου

Τα κυριότερα πλεονεκτήματα από την χρήση του *διαδικτύου* [25] μπορούμε να τα κατηγοριοποιήσουμε ως εξής:

1. **Επικοινωνία**

   Αποτελεί τον βασικότερο στόχο του *διαδικτύου* και έχει ξεπεράσει τις προσδοκίες μας. Μέσω διαφόρων προγραμμάτων και εφαρμογών μπορούμε να επικοινωνήσουμε με κάποιο πρόσωπο που βρίσκεται σε κάποιο άλλο μέρος του πλανήτη.

2. **Πληροφορίες**

   Αποτελεί ένα σημαντικό επίτευγμα του *διαδικτύου* και θεωρείται ως ένας εικονικός θησαυρός γνώσεων. Είναι ένα σημαντικό εργαλείο που βοηθάει καθημερινά εκατοντάδες άτομα στον χώρο της εκπαίδευσης. Αποτελεί πηγή γνώσης και ενημέρωσης αφού και ιατρικές μελέτες δημοσιεύονται στο *διαδικτύου* και μπορεί ο καθένας μας να ενημερωθεί για τις όποιες εξελίξεις.

3. **Ψυχαγωγία**

   Αρκετοί νέοι χρησιμοποιούν τον προσωπικό τους υπολογιστή για ψυχαγωγία στο *διαδίκτυο*. Το 'κατέβασμα' (downloading) παιχνιδιών αποτελεί μια καθημερινή συνήθεια για αρκετούς νεαρούς χρήστες του *διαδικτύου*. Επιπλέον τα δωμάτια συνομιλίας γνωστά ως (chat rooms) είναι τα πιο δημοφιλή καθώς εκεί μπορούν να συνομιλήσουν με καινούργια άτομα από όλη την Ελλάδα. Επιπροσθέτως η μουσική και οι ειδήσεις αποτελούν μια κύρια μορφή ενημέρωσης και ψυχαγωγίας στον χώρο του διαδικτύου.

4. **Υπηρεσίες**

   Ο χώρος του *διαδικτύου* εμπεριέχει πάρα πολλές υπηρεσίες οι οποίες βοηθούν τους χρήστες σε αρκετά ζητήματα που τους απασχολούν. Για παράδειγμα υπάρχουν υπηρεσίες για αναζήτηση εργασίας, κάτι το οποίο είναι ιδιαίτερα σημαντικό στις μέρες μας αφού αρκετοί νέοι δεν έχουν δουλειά. Υπάρχουν υπηρεσίες οι οποίες καθοδηγούν πολλά άτομα για κάθε πτυχή της ζωής τους. Επιπλέον μέσω του *διαδικτύου* μπορούμε να κάνουμε διάφορες αγορές π.χ. εισιτηρίων, ρούχων, κρατήσεις σε ξενοδοχεία κ.α.

5.1.2 Αρνητικά Στοιχεία του Διαδικτύου

Μερικά από τα μειονεκτήματα του *διαδικτύου* είναι τα παρακάτω:

1. **Μορφές Ηλεκτρονικών Εγκλημάτων**

   Οι χρήστες του Η/Υ έχουν να αντιμετωπίσουν διάφορα είδη ηλεκτρονικών εγκλημάτων τα οποία ποικίλουν στην εποχή μας. Μερικά από αυτά είναι α) Απειλές από ιούς, β) Πορνογραφία ανηλίκων, γ) Κλοπή Προσωπικών Δεδομένων, δ) Παρενόχληση μέσω του διαδικτύου κ.α. Όλα τα παραπάνω είδη ηλεκτρονικών εγκλημάτων έχουν ραγδαία αύξηση και καθημερινά όλο και περισσότερα άτομα γίνονται θύματα τέτοιων επιθέσεων.

2. **Παραπληροφόρηση**

   Όπως είπαμε και προηγουμένως στα θετικά του διαδικτύου εντάσσεται ότι μπορούμε να αναζητήσουμε οποιαδήποτε πληροφορία σε πραγματικό χρόνο. Πάρα πολλά είδη πληροφοριών προέρχονται από αναξιόπιστες πηγές και δεν είναι αληθινές οι πληροφορίες που μας δίνουν. Έτσι διάφοροι χρήστες πέφτουν θύματα και διαβάζουν πληροφορίες που δεν είναι αληθινές. Για τον λόγο αυτό πρέπει να είμαστε ιδιαίτερα προσεκτικοί στις πληροφορίες που διαβάζουμε, να είναι από αξιόπιστες πηγές.

5.2 Εθισμός στο Διαδίκτυο

Με τον όρο εθισμό στο διαδίκτυο εννοούμε την υπερβολική χρήση του *διαδικτύου* και τον εκνευρισμό που παρουσιάζεται σε πολλά ανήλικα άτομα [26] σε περίπτωση στέρησής του. Ο *εθισμός* προκαλεί σημαντικά προβλήματα στην ανάπτυξη της προσωπικότητα κάποιου ατόμου. Για πολλούς γονείς προκαλεί ένα κλίμα εκνευρισμού να βλέπουν τα παιδιά τους να ασχολούνται ώρες με το διαδίκτυο.

Πολλοί από αυτούς πίστευαν ότι το *διαδίκτυο* θα ανοίξει νέους ορίζοντες στην σταδιοδρομία των παιδιών τους. Σύντομα όμως συνειδητοποίησαν ότι τα παιδιά τους, αντί να διαβάζουν τα μαθήματά τους και σε οποιαδήποτε απορία έχουν να ανατρέξουν στο *διαδίκτυο* περνούσαν αρκετές ώρες παίζοντας παιχνίδια ή μιλώντας με αγνώστους σε διάφορα είδη κοινωνικής δικτύωσης.

5.2.1 Είδη Εθισμού

Αρκετοί χρήστες εθίζονται μέσω διαφόρων δραστηριοτήτων στον χώρο του *διαδικτύου*. Ορισμένοι βασικοί τύποι συμπεριφορών στους οποίους παρατηρείται εξάρτηση και υπερβολική χρήση νέων ατόμων και ειδικότερα ανηλίκων στο *διαδίκτυο* είναι οι εξής:

Α) Το πρώτο είδος τέτοιας συμπεριφοράς αφορά αρκετά είδη ιστοσελίδων που απευθύνονται σε ενήλικα άτομα και έχουν διαδικτυακό πορνογραφικό υλικό.

Β) Υπερβολική χρήση διαφόρων ιστοσελίδων κοινωνικής δικτύωσης με σκοπό την δημιουργία διαδικτυακών σχέσεων και ανταλλαγής μηνυμάτων, η οποία αποτελεί μια καθημερινή ενέργεια αρκετών εφήβων.

Γ) Ενασχόληση με τον ηλεκτρονικό τζόγο και με διάφορες ηλεκτρονικές αγορές αποτελεί τον τρίτο τύπο συμπεριφοράς όπου παρατηρείται εξάρτηση ατόμων διαφόρων ηλικιών.

Δ) Η πολύωρη περιήγηση δηλαδή το διαρκές 'σερφάρισμα' καταναλώνει αρκετό από τον προσωπικό χρόνο των ατόμων και αποτελεί βασικό παράγοντα εξάρτησης στο *διαδίκτυο*.

Ε) Τα ηλεκτρονικά παιχνίδια και η υπερβολική ενασχόληση με τους Η/Υ στην χώρα μας αποτελούν κύρια πηγή εξάρτησης και εθισμού πολλών ανηλίκων ατόμων όπου παραμελούν τα μαθήματά τους και ασχολούνται ώρες χωρίς την σύμφωνη γνώμη των γονέων τους.

5.2.2 Σημάδια και Συμπτώματα Εθισμού των Εφήβων

Τα άτομα στα οποία παρατηρούνται σημάδια εθισμού είναι μοναχικά άτομα, διαζευγμένων οικογενειών τα οποία αφού έρχονται από το σχολείο τους δεν έχουν κάποιο άτομο ώστε να μιλήσουν για τα προβλήματά τους και καταφεύγουν στον κόσμο του *διαδικτύου*. Η κοινωνική απόρριψη, ο ρατσισμός και διάφορα άλλα προβλήματα ωθούν τους νέους σε κάποιο είδος εξάρτησης μέσω του *διαδικτύου*.

Για τον λόγο αυτό μπορούμε να πούμε ότι τα βασικά σημάδια εξάρτησης που εμφανίζονται σε διάφορες ηλικιακές ομάδες στο *διαδίκτυο* και πρέπει οι γονείς να είναι αρκετά προσεκτικοί είναι τα παρακάτω:

- Οι συνεχόμενες ώρες στον Η/Υ και στο διαδίκτυο.
- Η αδιαφορία για φαγητό και η έλλειψη ξεκούρασης.
- Η αδιαφορία για μελέτη των μαθημάτων του σχολείου του.
- Η επιθυμία του να περνά όλο και περισσότερες ώρες στο διαδίκτυο.
- Απομόνωση από την οικογένειά του και οι χαμηλές σχολικές επιδόσεις του.

Επιπλέον μπορούν να παρατηρηθούν και διάφορα σωματικά και ψυχολογικά συμπτώματα [27] όπως:

- Συχνοί πονοκέφαλοι και ημικρανίες από την πολύωρη χρήση του Η/Υ.
- Παραμέληση της προσωπικής υγιεινής του ατόμου.
- Εμφάνιση υπνηλίας της πρωινές ώρες εξαιτίας της νυχτερινής χρήσης του διαδικτύου.
- Μυωπία.
- Πόνοι στην μέση και μυοσκελετικές παθήσεις όπως π.χ. σκολίωση.

5.3 Ηλεκτρονικά Παιχνίδια

Ο όρος *ηλεκτρονικό παιχνίδι* ορίζεται οποιοδήποτε παιχνίδι το οποίο χρειάζεται τη ύπαρξη και την υποστήριξη μιας ηλεκτρονικής συσκευής για να λειτουργήσει. Αυτό μπορεί να είναι ένας ηλεκτρονικός υπολογιστής. Τα διαδικτυακά παιχνίδια [28] είναι σε μεγάλο βαθμό υπεύθυνα για την εξάρτηση που δημιουργούν σε αρκετά παιδιά κατά την πλοήγησή τους στο *διαδίκτυο*.

Επιπλέον η μοναξιά, η εσωστρέφεια και η απομόνωση των ατόμων στην σημερινή εποχή οδηγούν άτομα νεαρής ηλικίας στον εικονικό χώρο των παιχνιδιών. Η βία που πολλές φορές παρουσιάζεται σε διάφορα *ηλεκτρονικά παιχνίδια* εντυπωσιάζει τα παιδιά και αποτελεί βασική αιτία εθισμού. Επίσης όταν κάποιος έφηβος δεν έχει κάποιο συγκεκριμένο στόχο προς επίτευξη, όταν όλα φαίνονται ανούσια σε αυτόν οδηγείτε στον εικονικό χώρο των *ηλεκτρονικών παιχνιδιών*.

Εξοικειώνονται τα παιδιά με την βία και προσπαθούν να την επιβάλλουν σε συνομήλικούς τους στο σχολείο. Στα παιδιά η άσκηση βίας μπορεί να φαίνεται σαν μια συνηθισμένη πράξη για την οποία δεν συνειδητοποιούν τις επιπτώσεις που μπορεί να έχει και στον ίδιο τους τον εαυτό.

5.3.1 Πρόληψη και Αντιμετώπιση

Για να αντιμετωπίσουμε το φαινόμενο του εθισμού των παιδιών στα *ηλεκτρονικά παιχνίδια* πρέπει να λειτουργήσουμε προληπτικά. Σημαντικό ρόλο έχουν οι γονείς οι οποίοι πρέπει να θέσουν ορισμένους κανόνες στα παιδιά τους ώστε να αντιμετωπιστεί αυτό το φαινόμενο.

Αρχικά πρέπει **1)** να τεθούν χρονικά όρια σχετικά με την ενασχόληση των παιδιών στα *ηλεκτρονικά παιχνίδια*. **2)** Πρέπει οι γονείς να συμβουλεύουν τα παιδιά τους να ασχοληθούν και με άλλες δραστηριότητες όπως π.χ. ενασχόληση με κάποιο άθλημα, έτσι ώστε να τους δημιουργηθούν νέα ενδιαφέροντα και να σταματήσουν να περνούν ώρες μπροστά στην οθόνη του Η/Υ.

3) Πρέπει να συμβουλεύουν τα παιδιά τους να κάνουν κάποιο διάλειμμα για 20 περίπου λεπτά έτσι ώστε να γίνεται ξεκούραση των οφθαλμών τους και να μην γίνεται συνεχή χρήση του Η/Υ κάτι που θα δημιουργήσει εξάρτηση και εθισμό στα παιδιά τους.

5.4 Κοινωνικά Δίκτυα και Ανήλικοι

Στην σημερινή εποχή αρκετοί ανήλικοι χρήστες του διαδικτύου χρησιμοποιούν από πάρα πολύ μικρή ηλικία αρκετά κοινωνικά δίκτυα όπως π.χ. (Facebook, Twitter, Youtube) και έχουν την δυνατότητα να γνωρίσουν νέους ανθρώπους και να δημιουργήσουν ένα καινούργιο εικονικό δίκτυο επαφών όπου μπορούν να επικοινωνούν μέσω της αρμόδιας ιστοσελίδας. Ορισμένα πλεονεκτήματα που προσφέρουν τα *κοινωνικά δίκτυα* είναι τα εξής:

- Προσφέρουν δυνατότητα επικοινωνίας με πάρα πολλά άτομα από διάφορα μέρη του πλανήτη.
- Δημιουργία νέων φίλων και αναζήτηση φωτογραφιών, βίντεο που απεικονίζονται οι ίδιοι και δεν θα μπορούμε να έχουμε πρόσβαση με διαφορετικό τρόπο όπως π.χ. (με έντυπα

μέσα).

- Γρήγορη ενημέρωση για οτιδήποτε συμβαίνει στο κόσμο μέσα σε ελάχιστο χρονικό διάστημα, αφού οι πληροφορίες μεταδίδονται πολύ γρήγορα μέσω των πολλών χρηστών του.

- Δυνατότητα ενασχόλησης με διάφορα ηλεκτρονικά παιχνίδια που συναρπάζουν ανήλικα αλλά και ενήλικα άτομα.

- Δημιουργία διαφόρων εκδηλώσεων και αποστολή προσκλήσεων ηλεκτρονικά χωρίς να χρειάζεται τηλεφωνική ειδοποίηση για κάθε ένα από τα άτομα που θέλουμε να καλέσουμε.

Εκτός όμως από τα πλεονεκτήματα των κοινωνικών δικτύων υπάρχουν και αρκετοί κίνδυνοι για τα παιδιά που επισκέπτονται αυτές τις ιστοσελίδες. Πολλοί κίνδυνοι εμφανίζονται όταν τα παιδιά στέλνουν τα προσωπικά τους στοιχεία σε άγνωστα άτομα.

Ο κόσμος στο *διαδίκτυο* είναι διαφορετικός από τον πραγματικό κόσμο. Για τον λόγο αυτό τα παιδιά θα πρέπει να είναι ιδιαίτερα προσεκτικά στα πράγματα που λένε αλλά και κάνουν στα *κοινωνικά δίκτυα*. Ορισμένοι κίνδυνοι που παρουσιάζονται στα παιδιά κατά την πλοήγησή τους στο χώρο των *κοινωνικών δικτύων* είναι τα παρακάτω:

- Υπάρχει κίνδυνος τα προσωπικά τους στοιχεία να τα χρησιμοποιήσει κάποιος άλλος άνθρωπος, να δημιουργήσει ένα ψεύτικο προφίλ και να στέλνει προσβλητικά μηνύματα σε άλλα άτομα.

- Πολλά είναι τα θύματα των παιδόφιλων που στόχο έχουν την εξαπάτηση ανήλικων ατόμων.

- Χρειάζεται μεγάλη προσοχή στα μηνύματα που λαμβάνουμε από άγνωστα άτομα και περιέχουν διάφορους συνδέσμους στους οποίους προτρέπεται ο χρήστης να συμπληρώσει τα προσωπικά του στοιχεία σε κάποια ιστοσελίδα υποκλοπής δεδομένων.

- Παρενόχληση από άγνωστα άτομα χωρίς την δυνατότητα αντιμετώπισης τέτοιων φαινομένων.

5.4.1 Συμβουλές για Ασφαλή Πλοήγηση στα Κοινωνικά Δίκτυα

Παρακάτω ορίζονται μερικές χρήσιμες συμβουλές τις οποίες πρέπει να λάβουν τα παιδιά σοβαρά υπ' όψιν τους ώστε να πλοηγούνται με ασφάλεια σε διάφορα κοινωνικά δίκτυα.

1. Κάνουμε φίλους μόνο άτομα τα οποία γνωρίζουμε.

2. Δεν δημοσιεύουμε τον αριθμό τηλεφώνου μας και την διεύθυνση κατοικίας μας.

3. Δεν δημοσιεύουμε που βρισκόμαστε κάποια δεδομένη χρονική στιγμή.

4. Ορίζουμε στις ρυθμίσεις απορρήτου τις πληροφορίες και τα στοιχεία μας να είναι ορατά μόνο στους φίλους μας.

5. Οποιοδήποτε πρόβλημα αν αντιμετωπίσουμε ενημερώνουμε τους γονείς μας
6. Δεν περνάμε πολλές ώρες στα κοινωνικά δίκτυα.
7. Προσέχουμε με ποιον μιλάμε στα δωμάτια συζητήσεων που υπάρχουν σε πολλά παιχνίδια.
8. Ζητάμε την άδεια των φίλων μας προτού δημοσιεύσουμε κάποια φωτογραφία που τους απεικονίζει.
9. Δεν δημοσιεύουμε οικογενειακές φωτογραφίες εάν δεν έχουμε πάρει έγκριση από τους γονείς μας.
10. Χρησιμοποιούμε ασφαλείς κωδικούς και εφόσον ο λογαριασμός μας έχει παραβιαστεί κάνουμε μία αναφορά στο *κοινωνικό δίκτυο*.

5.5 Διαδικτυακός Τζόγος και Ανήλικοι

5.5.1 Εισαγωγή

Αρκετοί ανήλικοι χρησιμοποιούν καθημερινά διάφορες υπηρεσίες του *διαδικτύου*. Παρατηρούμε ότι ο χώρος του *διαδικτύου* έχει συμβάλλει σημαντικά σε πάρα πολλούς τομείς της εκπαίδευσης, της ενημέρωσης αλλά παράλληλα έχει δημιουργήσει και αρκετές συνέπειες για πολλούς ανήλικους χρήστες.

Στην σημερινή εποχή παρατηρείται έντονα το φαινόμενο του διαδικτυακού τζόγου από ανήλικα άτομα. Σημαντικό ρόλο έχουν δημιουργήσει τα μέσα κοινωνικής δικτύωσης τα οποία συμβάλλουν στον εθισμό πολλών ανηλίκων στον τζόγο, καθώς υπάρχουν πολλά διαδικτυακά παιχνίδια τα οποία δεν απαιτούν υψηλό κόστος συμμετοχής.

Ο διαδικτυακός τζόγος των ανηλίκων υπάρχει σε παγκόσμιο επίπεδο. Ορισμένες έρευνες που που έχουν πραγματοποιηθεί πρόσφατα σε διάφορες χώρες του εξωτερικού έδειξαν ότι: **1)** ο τζόγος των ανηλίκων στην Αυστραλία φτάνει στο 6,7 τοις εκατό, **2)** στις ΗΠΑ ανέρχεται στο ποσό 4,9 τοις εκατό.

Η Ελλάδα μαζί με την Ρουμανία παρουσιάζουν τα υψηλότερα ποσοστά ηλεκτρονικού τζόγου από ανήλικους χρήστες. Αποτελεί ένα κρίσιμο ζήτημα για αρκετούς γονείς καθώς όσοι έφηβοι ασχολούνται με τον *διαδικτυακό τζόγο* εμφανίζουν σημάδια εξάρτησης από αυτό, ενώ αρκετοί από αυτούς παίζουν τυχερά παιχνίδια και στον πραγματικό κόσμο.

5.5.2 Λόγοι Εξάρτησης Ανηλίκων και Επιπτώσεις

Καθοριστικό ρόλο εξάρτησης ανηλίκων ατόμων από τον *διαδικτυακό τζόγο* έχει δημιουργήσει η οικονομική κρίση. Αρκετοί ανήλικοι νιώθουν άγχος, κατάθλιψη κ.λπ και μέσω του *διαδικτυακού τζόγου* αναζητούν το εύκολο κέρδος και καταφέρνουν να ξεπεράσουν αυτά τα προβλήματα. Επίσης η φτώχεια καθώς και η ανεργία έχουν περιορίσει τις κοινωνικές δραστηριότητες πολλών παιδιών και βρίσκουν καταφύγιο στο *διαδίκτυο* όπου μπορούν να περάσουν ευχάριστα την ώρα τους.

Η οικογενειακή τους ζωή παίζει σημαντικό ρόλο και σε αρκετές περιπτώσεις παρατηρούμε ότι τα παιδιά έμαθαν να παίζουν *διαδικτυακό τζόγο* από τους γονείς τους. Χρειάζεται ιδιαίτερη

προσοχή από τους γονείς στα πράγματα που επιτρέπουν να κάνουν τα παιδιά τους στο *διαδίκτυο*. Σε άλλες περιπτώσεις παρατηρούμε το φαινόμενο τα παιδιά να έχουν κλέψει τις πιστωτικές κάρτες των γονιών τους και να τις χρησιμοποιούν σε διαδικτυακά τυχερά παιχνίδια.

5.5.3 Γραμμή Βοήθειας για τον Διαδικτυακό Τζόγο

Άρχισε να λειτουργεί από το έτος 2011 σε συνεργασία με τον όμιλο ΟΠΑΠ και αντιμετωπίζει διάφορα προβλήματα σχετικά με τα τυχερά παιχνίδια και τον διαδικτυακό τζόγο. Έχει στόχο να ενημερώνει **α)** τους παίκτες που έχουν ενασχόληση με τον τζόγο και **β)** τα άτομα της οικογένειάς τους για διάφορα προβλήματα καθώς και για τον εθισμό στον τζόγο ατόμων διαφόρων ηλικιών.

Η γραμμή αυτή λειτουργεί από Δευτέρα έως Παρασκευή και ώρες 09:00 - 21:00 καλώντας στον τετραψήφιο αριθμό **1114** και μπορείτε να στείλετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) στην διεύθυνση **1114a@kethea-alfa.gr**

Στόχοι αυτής της γραμμής συμβουλευτικής και ψυχολογικής καθοδήγησης είναι οι παρακάτω:

- Η πληροφόρηση των ατόμων για διάφορα προγράμματα απεξάρτησης από τυχερά παιχνίδια.
- Η ενημέρωση καθώς και η παροχή προτάσεων για την αντιμετώπιση κάποιας προβληματικής κατάστασης με τον τζόγο, καθώς και η αναφορά των συνεπειών που μπορεί να προκαλέσει όχι μόνο στο άτομο που ασχολούνται με τον τζόγο αλλά και στο περιβάλλον τους.
- Υποστήριξη από συμβούλους στους οποίους μπορείτε να αναφέρετε τέτοιες συμπεριφορές, καθώς και η συμβουλευτική καθοδήγηση για το πώς να χειριστείτε μια τέτοια κατάσταση.

5.6 Παραπληροφόρηση στο Διαδίκτυο

5.6.1 Εισαγωγή

Το *διαδίκτυο* σήμερα παρέχει στους χρήστες του πάρα πολλούς πόρους και δίνει αρκετές ευκαιρίες μάθησης σε πολλά νεαρά άτομα. Πολλές όμως πληροφορίες που υπάρχουν μπορεί να μην είναι χρήσιμες και άλλες να μην είναι αξιόπιστες. Για τον λόγο αυτό πρέπει να βοηθήσουμε τα παιδιά μας να αναπτύξουν μία κριτική σκέψης και να μπορέσουν από μικρή ηλικία να βγάλουν χρήσιμα συμπεράσματα για την ακρίβεια των πληροφοριών που διαβάζουν.

Πρέπει οι γονείς να μάθουν στα παιδιά τους ότι οτιδήποτε βλέπουν και διαβάζουν στο *διαδίκτυο* δεν είναι πάντοτε αληθινό. Μπορεί ο καθένας μας να δημιουργήσει μία ιστοσελίδα και να δημοσιεύει γεγονότα και πληροφορίες που δεν είναι πάντοτε αληθινές.

5.6.2 Συμβουλές προς τους Γονείς

Κάθε γονέας έχει υποχρέωση να ενημερώνει, να συμβουλεύει και να βοηθάει τα παιδιά του να εντοπίζουν οποιοδήποτε είδος *παραπληροφόρησης* στον χώρο του διαδικτύου. Παρακάτω δίνονται μερικές χρήσιμες συμβουλές για κάθε γονέα, ο οποίος πρέπει να ενημερώσει τα παιδιά γι' αυτό το ζήτημα.

- Πολλά παιδιά ακόμη και από την προσχολική ηλικία μπαίνουν στο *διαδίκτυο* την σημερινή εποχή. Πρέπει να ξεκινήσουμε να ενημερώνουμε τα παιδιά μας από μικρή ηλικία σχετικά με την αναζήτηση πληροφοριών, έτσι ώστε να μπορέσουν να διακρίνουν και να ξεχωρίζουν κάποιο γεγονός από κάποια άποψη κάποιου ανθρώπου στο *διαδίκτυο* και να μπορούν να ξεχωρίζουν τις διάφορες τοποθεσίες που χρησιμοποιούν διάφορα στερεότυπα και άλλες που έχουν ως στόχο την προπαγάνδα.

- Πρέπει να ρωτήσετε τα παιδιά σας για τις διάφορες πληροφορίες που συλλέγουν από το *διαδίκτυο* εάν έπειτα κάνουν μια επαλήθευση με άλλες πηγές για να δουν εάν οι πληροφορίες που βρήκαν είναι αληθινές. Μπορούν να ανατρέξουν σε διάφορες εφημερίδες, σε περιοδικά και σε βιβλία για την διασταύρωση των πληροφοριών που κατέγραψαν.

- Ενθαρρύνετε τα παιδιά σας να σας συμβουλεύονται και διδάξτε τους μερικές τεχνικές για τις πληροφορίες που εντοπίζουν στον παγκόσμιο ιστό. Μπορείτε να ενημερώσετε τα παιδιά σας να χρησιμοποιούν διάφορες μηχανές αναζήτησης όχι μόνο μία. Με αυτόν τον τρόπο θα έχετε βελτιώσει σε αρκετά μεγάλο βαθμό την ικανότητά τους να εντοπίζουν ποιοτικές πληροφορίες.

6.1 Εισαγωγή

Η ασφάλεια των παιδιών [29] κατά την πλοήγησή τους στο *διαδίκτυο* είναι ένα εξαιρετικά σημαντικό ζήτημα που κάθε γονέας πρέπει να λάβει υπ' όψιν του, ώστε να μην δημιουργηθούν προβλήματα στην συμπεριφορά και εξέλιξη του κάθε ατόμου.

Προτού όμως τα παιδιά μάθουν να εξερευνούν το *διαδίκτυο* πρέπει ο κάθε γονέας να βεβαιωθεί ότι το παιδί του καταλαβαίνει στο τι πρέπει να κάνει και σε τι όχι σε αυτόν τον χώρο. Ένας τρόπος να τα πετύχουμε αυτό το θέμα είναι να καθίσουμε και να μιλήσουμε με κάθε παιδί στην οικογένεια και να ορίσουμε μερικούς οικογενειακούς κανόνες οι οποίοι θα είναι κατάλληλοι για την ηλικία του κάθε παιδιού στο χρόνο που θα περνάει στο *διαδίκτυο*. Παρακάτω περιγράφονται μερικοί κανόνες χρήσης του *διαδικτύου* τους οποίους μπορεί ο κάθε γονιός να ορίσει στα παιδιά του ώστε αυτά να πλοηγούνται με ασφάλεια στον *διαδίκτυο*.

- Ορίζουμε την ώρα που θα μένουμε συνδεδεμένοι στο *διαδίκτυο* και συζητάμε τις τοποθεσίες που επιτρέπεται να επισκέπτονται τα παιδιά.
- Δεν αποκαλύπτουμε ποτέ την διεύθυνση κατοικίας μας, αριθμό τηλεφώνου, το όνομα του σχολείου που πηγαίνουμε χωρίς την σύμφωνη άδεια των γονέων μας.
- Ενημερώνουμε αμέσως του γονείς για οτιδήποτε ασυνήθιστο συμβαίνει κατά την πλοήγησή μας στο *διαδίκτυο*.
- Δεν αποκαλύπτουμε τους κωδικούς πρόσβασης για διάφορες υπηρεσίες του *διαδικτύου* σε κάποιον φίλο μας, μόνο στους γονείς μας.
- Δεν στέλνουμε φωτογραφίες δικές μας ή άλλων μελών της οικογένειάς μας σε αγνώστους χωρίς την άδεια των γονιών μας.
- Δεν μιλάμε σε άγνωστα άτομα που μόλις γνωρίσαμε στο *διαδίκτυο* και δεν τα συναντάμε χωρίς την απαιτούμενη άδεια από τους γονείς μας.

6.1.1 Διαδικτυακοί Διαφθορείς

Κατά την πλοήγηση των παιδιών στο *διαδίκτυο* διατρέχουν άμεσο κίνδυνο επικοινωνίας με διάφορους *διαδικτυακούς διαφθορείς* οι οποίοι εκμεταλλευόμενοι την ανωνυμία του *διαδικτύου* προσπαθούν να δημιουργήσουν σχέσεις με νεαρά ανήλικα άτομα που δεν γνωρίζουν καλά το χώρο αυτό.

Τα άτομα αυτά έρχονται σε επαφή με τα παιδιά μέσω των δωματίων συζητήσεων (chat rooms), μέσω των κοινωνικών δικτύων (facebook, twitter), μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) και προσπαθούν να παρασύρουν τα παιδιά σε γεγονότα και καταστάσεις που θέλουν οι ίδιοι. Αφιερώνουν αρκετό χρόνο μιλώντας με ευγένεια και ακούγοντας με προσοχή κάθε υποψήφιο θύμα ώστε να γνωρίσουν όσο περισσότερα πράγματα για εκείνο.

Τα άτομα που κινδυνεύουν από *διαδικτυακούς διαφθορείς* είναι: **1)** Άτομα νέα στο χώρο του διαδικτύου, χωρίς πείρα, **2)** Νεαρά άτομα που αναζητούν την προσοχή άλλων ατόμων,

3) Μοναχικά άτομα, **4)** Άτομα που βρίσκονται σε σύγχυση και παρασύρονται από ενήλικα άτομα.

Κάθε γονιός μπορεί να καταλάβει εάν το παιδί του έχει πέσει θύμα κάποιου *διαδικτυακού διαφθορέα* εάν:

- Καταναλώνει αρκετό χρόνο στον Η/Υ και στο διαδίκτυο, κλείνει την πόρτα του δωματίου του και δεν φανερώνει την δραστηριότητά στον Η/Υ.
- Παίρνει τηλεφωνήματα από άγνωστους αριθμούς και βρίσκεται στο τηλέφωνο για αρκετή ώρα. Πολλοί *διαδικτυακοί διαφθορείς* προτρέπουν σε μια συνάντηση με το υποψήφιο θύμα τους. Άλλοι διαθέτουν αριθμούς χωρίς χρέωση ώστε να καλούν τα παιδιά και να μην γνωρίζουν τίποτα οι γονείς.
- Βρίσκεται πορνογραφικό υλικό στο Η/Υ. Αρκετά άτομα χρησιμοποιούν αυτή την τεχνική για να προσελκύσουν τα παιδιά.

6.2 Γονικός Έλεγχος και Ασφάλεια στο Διαδίκτυο

Ο *γονικός έλεγχος* είναι ένα σημαντικό πρόγραμμα σε κάθε Η/Υ μέσω του οποίου δίνεται η δυνατότητα σε κάθε γονέα να περιορίζει την πλοήγηση κάθε παιδιού στο διαδίκτυο και να το προστατεύει από διάφορες ιστοσελίδες με κακόβουλο περιεχόμενο. Τα προγράμματα *γονικού ελέγχου* που κυκλοφορούν στην αγορά δίνουν στους γονείς αρκετές δυνατότητες περιορισμού τοποθεσιών στα παιδιά τους όπως:

1. Περιορισμό στον χρόνο όπου μπορεί να χρησιμοποιήσει τον Η/Υ ένα ανήλικο άτομο.
2. Μπορούν να ορίσουν οι γονείς τις διάφορες ιστοσελίδες που θέλουν να έχει πρόσβαση το παιδί τους.
3. Ορίζουν μερικά ηλεκτρονικά παιχνίδια που είναι κατάλληλα και μπορεί να παίξει το παιδί τους στο χρόνο που καταναλώνει στο *διαδίκτυο*.
4. Υπάρχει επίσης η δυνατότητα περιορισμού των προγραμμάτων που είναι εγκατεστημένα στον Η/Υ και μπορεί να χρησιμοποιήσει κάποιο ανήλικο άτομο.

Δίνεται επίσης η δυνατότητα ελέγχου από τους γονείς για την δραστηριότητα του παιδιού τους στο *διαδίκτυο*. Μερικές από τις δυνατότητες ελέγχου που υπάρχουν στα προγράμματα *γονικού ελέγχου* παρουσιάζονται παρακάτω:

1. Ειδοποιείται ο γονιός στον λογαριασμό του εάν το παιδί του προσπαθήσει να συνδεθεί σε κάποια απαγορευμένη σελίδα.
2. Γίνεται έλεγχος των ιστοσελίδων όπου επισκέπτεται το παιδί τους στο *διαδίκτυο*.
3. Ελέγχονται οι επαφές με τις οποίες συνομιλεί κάποιο ανήλικο άτομο σε διάφορα κοινωνικά δίκτυα.

6.2.1 Χρήσιμες Συμβουλές

Υπάρχουν διάφορα προγράμματα *γονικού ελέγχου* που κυκλοφορούν στο *διαδίκτυο*, άλλα με πληρωμή και άλλα διανέμονται δωρεάν αλλά με περιορισμένες δυνατότητες. Ορισμένες δωρεάν πλατφόρμες *γονικού ελέγχου* είναι: 1) Norton Family, 2) K9 Web Protection κ.α. Με πληρωμή μερικές πλατφόρμες *γονικού ελέγχου* είναι: 1) Web Watcher, 2) McAfee Safe Eyes κ.α.

Προτού όμως αγοράσετε κάποιο πρόγραμμα *γονικού ελέγχου* πρέπει να ασφαλίσετε τον λογαριασμό σας με κάποιο ισχυρό κωδικό πρόσβασης έτσι ώστε να μην μπορούν να το μαντέψουν τα παιδιά σας. Καλό είναι να δημιουργήσετε έναν ξεχωριστό λογαριασμό στο κάθε παιδί σας όπου θα έχουν περιορισμένες δυνατότητες στον Η/Υ και δεν θα μπορούν να εγκαταστήσουν προγράμματα ή και να αλλάξουν τις ρυθμίσεις που έχετε ορίσει.

Πρέπει να παροτρύνετε τα παιδιά σας να μοιράζονται μαζί σας οποιαδήποτε δυσκολία συναντήσουν προτού κάνουν κάποια άλλη ενέργεια. Χρειάζεται να είστε πολύ προσεκτικοί με όλες αυτές τις τεχνικές *γονικού ελέγχου* διότι το παιδί σας μπορεί να καταλάβει ότι παρακολουθείτε και να μην έχουμε τα κατάλληλα αποτελέσματα.

6.3 Γενικές Συμβουλές προς τους Γονείς

Το *διαδίκτυο* είναι ένα σημαντικό μέσο επικοινωνίας στην σημερινή εποχή. Κίνδυνοι υπάρχουν όπως και σε άλλα μέσα επικοινωνίας, γι' αυτό αντί να απαγορεύουν να το χρησιμοποιούν τα παιδιά τους καλό είναι να έχουν ενημερωθεί για τους κινδύνους που υπάρχουν και να έχουν μια εξοικείωση με τις υπηρεσίες που προσφέρονται, ώστε να μπορούν να προσφέρουν στα παιδιά τους καθοδήγηση σε οποιαδήποτε δυσκολία συναντήσουν. Παρακάτω ορίζονται μερικές χρήσιμες συμβουλές προς τους γονείς ώστε να ελέγχουν τα παιδιά τους κατά την πλοήγησή τους στο *διαδίκτυο*.

- Δεν πρέπει να απαγορεύεται στα παιδιά σας να χρησιμοποιούν το *διαδίκτυο*. Μπορούν να έχουν πρόσβαση στις διάφορες υπηρεσίες του και από το σχολείο αλλά και από υπολογιστές συμμαθητών τους.
- Τοποθετείστε τον Η/Υ σε κοινόχρηστους χώρους όπως στο σαλόνι ώστε να επιβλέπεται τα παιδιά σας χωρίς όμως να τους δίνεται η αίσθηση ότι ελέγχονται από εσάς.
- Ενημερωθείτε για τις δυνατότητες που προσφέρονται στον χώρο του *διαδικτύου* και δώστε κίνητρα στα παιδιά σας να επισκέπτονται ιστοσελίδες με ενημερωτικό και εκπαιδευτικό περιεχόμενο.
- Συζητήστε με τα παιδιά σας για τους κινδύνους που υπάρχουν σε διάφορα δωμάτια συζητήσεων γνωστά ως (chat rooms) και πείτε τους να μην συνομιλούν με αγνώστους χωρίς την παρουσία κάποιου γονέα.
- Ενημερώστε τα παιδιά σας για το πόσο σημαντικό ζήτημα είναι η ασφάλειά τους τις ώρες που καταναλώνουν στο *διαδίκτυο*.
- Χρησιμοποιήστε ορισμένα ειδικά εργαλεία λογισμικού ώστε να παρεμποδίζετε την πρόσβαση σε ακατάλληλες τοποθεσίες.

- Ενημερωθείτε ηλεκτρονικά από τις διάφορες ημερίδες ασφαλούς πλοήγησης του *διαδικτύου* που υπάρχουν στην ιστοσελίδα της *δίωξης ηλεκτρονικού εγκλήματος*.

- Μην αντιδράτε χωρίς ψυχραιμία εάν το παιδί παραμένει πολλές ώρες στον Η/Υ αλλά μπορείτε να ορίσετε μερικούς οικογενειακούς κανόνες χρήσης του μαζί με το παιδί σας.

6.3.1 Συμβουλές για Ενήλικες

- Εάν δεν γνωρίζετε τον αποστολέα κάποιου μηνύματος ηλεκτρονικού ταχυδρομείου (e-mail) μην απαντάτε στο μήνυμα που σας έστειλε. Επιπλέον μην ανοίγετε αρχεία που σας έχει στείλει κάποιος άγνωστος στον Η/Υ. Μπορεί τα αρχεία να είναι μολυσμένα.

- Μην χρησιμοποιείται τον αριθμό της πιστωτικής σας κάρτας σε αναξιόπιστους δικτυακούς τόπους και μην στέλνετε με (e-mail) τον αριθμό της κάρτας σας. Στην σημερινή εποχή το οικονομικό έγκλημα έχει ραγδαία ανάπτυξη.

- Χρησιμοποιείτε λογισμικό (antivirus) για προστασία του Η/Υ από διάφορους ιούς και προσέξτε τα αρχεία που κατεβάζετε από το *διαδίκτυο*.

- Βεβαιωθείτε ότι ο Η/Υ προστατεύεται από ένα τείχος προστασίας (firewall).

- Μην δίνετε τα προσωπικά σας στοιχεία σε άγνωστα άτομα ή σε άτομα που μόλις γνωρίσατε στο *διαδίκτυο*.

6.4 Συμβουλές ανά Ηλικία

Χρειάζεται πολύ προσοχή το χρονικό διάστημα που περνάνε τα παιδιά σας στο *διαδίκτυο*. Πρέπει να μάθουν να μιλάνε στους γονείς για οποιαδήποτε δυσκολία συναντήσουν και δεν μπορούν να την αντιμετωπίσουν.

Επιπλέον είναι πολύ σημαντικό να είστε διαρκώς ενήμεροι για τις εξελίξεις που συμβαίνουν στο *διαδίκτυο* π.χ. απάτες μέσω του *διαδικτύου*, διάφορα είδη ηλεκτρονικών εγκλημάτων κ.α και να ενημερώνεστε και από την δίωξη ηλεκτρονικού εγκλήματος μέσω διαφόρων ημερίδων αλλά και ανακοινώσεων που δημοσιεύει, ώστε να γνωρίζετε που πρέπει να απευθυνθείτε σε κάποια δύσκολη στιγμή.

Παρακάτω παρουσιάζονται ορισμένες χρήσιμες συμβουλές για τους γονείς που έχουν παιδιά στις παρακάτω ηλικιακές κατηγορίες.

6.4.1 Παιδιά 5 έως 6 ετών

Όταν τα παιδιά σας φτάσουν σε ηλικία 5 ετών θα θελήσουν να εξερευνήσουν τον χώρο του διαδικτύου μόνα τους. Διατηρούν μια θετική στάση και σε αρκετές περιπτώσεις μιμούνται τους γονείς τους. Για τον λόγο αυτό εάν χρησιμοποιούν οι γονείς έναν Η/Υ, θα θελήσουν να το χρησιμοποιήσουν και οι ίδιοι.

Οι γονείς πρέπει να τα καθοδηγήσουν ώστε να πλοηγούνται με ασφάλεια. Σε καμία περίπτωση δεν πρέπει να τα αφήσουμε μόνα τους στον Η/Υ. Τα παιδιά σε αυτήν την ηλικία

μαθαίνουν να χρησιμοποιούν διάφορες λειτουργίες του Η/Υ όπως π.χ. το ποντίκι, το πληκτρολόγιο και μαθαίνουν να παίζουν διάφορα παιχνίδια που υπάρχουν σε κάθε υπολογιστή.

Χρειάζονται τους γονείς τους για την ανεύρεση τοποθεσιών στο *διαδίκτυο* ώστε να μπορέσουν να δουν την αγαπημένη τους παιδική σειρά. Παρακάτω παρουσιάζονται ορισμένες συμβουλές ασφαλείας για τους γονείς ώστε να μπορέσουν να βοηθήσουν τα παιδιά τους και να έχουν μια σωστή ανάπτυξη στην ζωή τους.

- Μπορείτε να χρησιμοποιήσετε μηχανές αναζήτησης που να είναι κατάλληλες για τα παιδιά αυτής της ηλικίας.
- Πρέπει να ενημερώσετε τα παιδιά σας για το απόρρητο των πληροφοριών και να μην δίνουν βασικές πληροφορίες του εαυτού τους σε άγνωστα άτομα.
- Μην επιτρέπετε να μπαίνουν σε δωμάτια συνομιλιών ή να στέλνουν μηνύματα στην ηλικία αυτή.

6.4.2 Παιδιά 7 έως 8 ετών

Τα παιδιά σε αυτή την ηλικιακή κατηγορία έχουν ως στόχο να μπορέσουν να δουν μέχρι σε πιο σημείο μπορούν να φτάσουν στο *διαδίκτυο* χωρίς να τιμωρηθούν από τους γονείς τους. Αρχίζουν σιγά σιγά να αναπτύσσουν την δική τους ταυτότητα και έχουν ανεπτυγμένο το αίσθημα ευθύνης για κάποιο κακό που πιθανόν έχουν κάνει και θέλουν να το διορθώσουν.

Τα παιδιά αυτής της ηλικίας πλοηγούνται στο *διαδίκτυο* κατά κύριο λόγο για διασκέδαση και για να παίξουν διαδικτυακά παιχνίδια. Σε αρκετές περιπτώσεις βλέπουμε να είναι εξοικειωμένα με τον Η/Υ και να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο αλλά και διάφορα δωμάτια συνομιλιών.

Μερικά παιδιά μαζί με τα αδέρφια τους μαθαίνουν να μπαίνουν και σε διάφορες ιστοσελίδες κοινωνικής δικτύωσης. Οι γονείς δεν πρέπει να αφήσουν το παιδί τους να παραμείνει για αρκετή ώρα στο *διαδίκτυο*. Ορισμένες συμβουλές για τους γονείς ώστε να αντιμετωπίσουν τα παιδιά αυτής της ηλικιακής ομάδας δίνονται παρακάτω.

- Δημιουργήστε μερικούς οικογενειακούς κανόνες χρήσης του *διαδικτύου* μαζί με τα παιδιά σας.
- Μπορείτε να δημιουργήσετε ένα κοινό λογαριασμό ηλεκτρονικού ταχυδρομείου μαζί με τα παιδιά σας, αντί να τους επιτρέψετε να έχουν κάποιο λογαριασμό δικό τους.
- Μάθετε στα παιδιά σας να σας συμβουλεύονται και να σας λένε εάν αντιμετωπίζουν κάποιο πρόβλημα στο *διαδίκτυο*.
- Μπορείτε να μιλήσετε στα παιδιά σας για την σεξουαλικότητα γιατί μπορεί να συναντήσουν κάποιο ακατάλληλο περιεχόμενο στον χώρο αυτό.
- Συζητήστε μαζί τους για τους διαδικτυακούς φίλους που γνώρισαν και ενημερώστε τους να μην στέλνουν φωτογραφίες και άλλα προσωπικά δεδομένα σε αγνώστους.

6.4.3 Παιδιά 9 έως 12 ετών

Τα παιδιά σε αυτή την ηλικία είναι προέφηβοι και θα θελήσουν να γνωρίζουν όλο και περισσότερα πράγματα για τον Παγκόσμιο Ιστό. Οι γονείς πρέπει να χρησιμοποιήσουν μερικά προγράμματα γονικού ελέγχου που υπάρχουν στο *διαδίκτυο*, ώστε να μπορέσουν να δουν την διαδικτυακή δραστηριότητα που κάνουν τα παιδιά τους, αλλά και να αποκλείσουν ορισμένες ακατάλληλες τοποθεσίες όπου απαγορεύεται να έχουν πρόσβαση ανήλικα άτομα.

Μέσω του *διαδικτύου* τα παιδιά μαθαίνουν να αναζητούν πληροφορίες για διάφορες σχολικές εργασίες. Ακούν μουσική, παίζουν διαδικτυακά παιχνίδια, δημιουργούν λογαριασμούς ηλεκτρονικού ταχυδρομείου και μπαίνουν σε διάφορα κοινωνικά δίκτυα. Παρακάτω δίνονται μερικές συμβουλές για τους γονείς με παιδιά σε αυτές τις ηλικίες.

- Ενημερώστε τα παιδιά σας για τα πνευματικά δικαιώματα στο *διαδίκτυο* και πείτε τους να μην αντιγράφουν πληροφορίες που προστατεύονται από τον αντίστοιχο νόμο και έπειτα να τις προσαρμόζουν σε δικές τους σχολικές εργασίες.
- Μιλήστε στα παιδιά σας για την παιδική πορνογραφία και πείτε τους να μην συνομιλούν με άτομα που δεν γνωρίζουν.
- Μιλήστε τους για τους τρόπους καλής συμπεριφοράς στο *διαδίκτυο* αλλά και στην κοινωνική τους ζωή.
- Πείτε τους να είναι πολύ προσεκτικοί στους φίλους που δημιουργούν σε διάφορα κοινωνικά δίκτυα.
- Δημιουργείστε μερικούς κανόνες χρήσης του *διαδικτύου* για να μην δημιουργούνται προβλήματα στην καθημερινή ενασχόλησή τους.

6.4.4 Παιδιά 13 έως 17 ετών

Τα παιδιά σε αυτή την ηλικία είναι έφηβοι και χρειάζεται πολύ προσοχή από τους γονείς η αντιμετώπισή τους. Παρατηρούμε πολλές περιπτώσεις τα παιδιά αυτών των ηλικιών να γνωρίζουν περισσότερα πράγματα για το *διαδίκτυο* από τους γονείς τους. Πρέπει να έχουν οριστεί μερικοί οικογενειακοί κανόνες τους οποίους θα τηρούν και τα παιδιά αλλά και οι γονείς.

Τα παιδιά είναι τεχνικά καταρτισμένα στο χώρο αυτό και έχουν λογαριασμό σε διάφορα κοινωνικά δίκτυα, επισκέπτονται δωμάτια συνομιλιών, παίζουν ηλεκτρονικά παιχνίδια, στέλνουν μηνύματα και γενικά επισκέπτονται πολλές δικτυακές τοποθεσίες. Μερικές συμβουλές για τους γονείς που έχουν παιδιά σε αυτές τις κατηγορίες παρουσιάζονται παρακάτω.

- Μάθετε με ποια άτομα συνομιλούν τα παιδιά σας στο *διαδίκτυο* και ενθαρρύνετέ τα να σας μιλούν χωρίς φόβο για την προσωπική τους ζωή.
- Πείτε τους να μην δημοσιεύουν προσωπικά τους δεδομένα στα κοινωνικά δίκτυα και όχι μόνο, διότι αργότερα μπορεί να μετανιώσουν αλλά η κατάσταση που θα έχει δημιουργηθεί δεν θα μπορεί να αλλάξει.
- Πείτε τους να σας συμβουλευτούν προτού εκτελέσουν κάποια οικονομική συναλλαγή.

- Συζητήστε μαζί τους για τον ηλεκτρονικό τζόγο και για τους κινδύνους που εμφανίζει σε ανήλικα άτομα.
- Καθοδηγείστε τα παιδιά σας να σας συμβουλεύονται σε οποιαδήποτε δυσκολία συναντήσουν, χωρίς να φοβηθούν να σας μιλήσουν.
- Μιλήστε τους για την πορνογραφία στο *διαδίκτυο* και για τους κινδύνους που εμφανίζει.
- Ενημερώστε τα παιδιά σας για τα διάφορα είδη ηλεκτρονικών εγκλημάτων που εμφανίζονται στον χώρο αυτό και δώστε οδηγίες προφύλαξης αλλά και αντιμετώπισής τους.

6.5 Προστασία από Ηλεκτρονική Εξαπάτηση

Αρκετά άτομα και πιο συγκεκριμένα πολλά παιδιά πέφτουν θύματα ηλεκτρονικής εξαπάτησης μέσω του Η/Υ κατά την διάρκεια πλοήγησης στο *διαδίκτυο*. Χρειάζεται πολύ προσοχή σε οποιαδήποτε ενέργεια που πραγματοποιούμε στον χώρο αυτό. Παρακάτω παρουσιάζονται μερικές χρήσιμες συμβουλές ώστε να μην γίνουμε θύματα κάποιου είδος ηλεκτρονικής εξαπάτησης.

- Πρέπει να δημιουργήσετε δυναμικούς κωδικούς πρόσβασης σε όλους τους λογαριασμούς που έχετε στο *διαδίκτυο*. Ένας κωδικός είναι ισχυρός όταν περιέχει σε συνδυασμό οκτώ και άνω αριθμούς, γράμματα, σύμβολα έτσι ώστε να είναι αρκετά δύσκολος να τον υποκλέψουν. Μην έχετε τον ίδιο κωδικό σε πολλούς λογαριασμούς, αλλά δημιουργείστε διαφορετικό σε κάθε έναν.
- Μην απαντάτε σε διάφορα μηνύματα ηλεκτρονικού ταχυδρομείου όπου σας στέλνουν άγνωστα άτομα και μην δίνετε ποτέ προσωπικά στοιχεία, χωρίς να γνωρίζετε τον παραλήπτη.
- Προστατεύστε τον υπολογιστή με κάποιο λογισμικό αντιμετώπισης ιών και ενεργοποιείστε το τείχος προστασίας του Η/Υ.
- Για αγορές μέσω πιστωτικών καρτών μέσω του *διαδικτύου* καλό θα είναι να έχετε κάρτες με χαμηλό πιστωτικό όριο ώστε σε περίπτωση παραβίασης της κάρτας να γίνετε περιορισμός στο ποσό που μπορεί να κλέψει κάποιος ηλεκτρονικός εγκληματίας.

7.1 Λογισμικό Αντιμετώπισης Ιών

Το λογισμικό αντιμετώπισης ιών (antivirus) έχει σαν στόχο την πρόληψη, τον εντοπισμό και την άρση όλων εκείνων τον κακόβουλων προγραμμάτων που στοχεύουν στην μόλυνση του Η/Υ. Στην αγορά, υπάρχουν πακέτα λογισμικού προστασίας ενάντια σε ιούς από διάφορες εταιρείες όπως π.χ. (mcafee, eset, kaspersky) κ.α. με πληρωμή έτσι ώστε να διασφαλίζεται η μέγιστη προστασία κατά την πλοήγησή μας στο *διαδίκτυο* αλλά και με δωρεάν δοκιμή για τριάντα ημέρες.

Κάθε χρήστης του Η/Υ πρέπει να έχει εγκαταστήσει ένα τέτοιο λογισμικό έτσι ώστε να μπορεί **1)** να ενημερώνεται σε περίπτωση κάποιας επίθεσης που διαπράττεται στον Η/Υ του, **2)** να μπορεί να κάνει σάρωση ολόκληρου του συστήματός του για εντοπισμό κακόβουλων προγραμμάτων που έχουν εγκατασταθεί χωρίς ο ίδιος να το γνωρίζει και περιέχουν μολυσμένα αρχεία που επιβραδύνουν τη λειτουργία του συστήματος, **3)** Να ελέγχει τον Η/Υ και τα διάφορα αφαιρούμενα μέσα που χρησιμοποιεί όπως π.χ. ένα (usb, cd), έναν εξωτερικό σκληρό δίσκο για μολυσμένα αρχεία προτού κάνει οποιαδήποτε ενέργεια μεταφοράς διάφορων αρχείων στον υπολογιστή του, **4)** να απομονώνει τα μολυσμένα αρχεία σε καραντίνα και έπειτα να μπορέσει να τα διαγράψει εξολοκλήρου από τον Η/Υ.

Με τα λογισμικά αντιμετώπισης ιών [30] πρέπει να γνωρίζουν οι χρήστες του Η/Υ ότι δεν διασφαλίζεται πάντοτε η μέγιστη προστασία τους στο *διαδίκτυο*. Σε σύντομα χρονικά διαστήματα εμφανίζονται όλο και περισσότερα είδη απειλών όπου αυτά τα λογισμικά δεν έχουν κατάλληλα ενημερωθεί ώστε να αποτρέψουν την ενδεχόμενη παραβίαση του συστήματός μας. Πρέπει επίσης να γνωρίζεται ότι εκτός από τα παραπάνω πλεονεκτήματα που είπαμε για τα λογισμικά αυτά, υπάρχουν και μειονεκτήματα κατά την διάρκεια χρήσης τους. Ορισμένα από αυτά είναι: **1)** Επηρεάζεται η απόδοση του Η/Υ καθώς το λογισμικό προστασίας από ιούς καταναλώνει πολλούς πόρους του υπολογιστικού μας συστήματος και έτσι μπορεί να επιβραδυνθεί η λειτουργία του Η/Υ,

2) Πολλοί χρήστες εγκαθιστούν πολλά τέτοια προγράμματα νομίζοντας ότι θα έχει μεγαλύτερη προστασία ο υπολογιστής τους αλλά γίνεται ακριβώς το αντίθετο και επιβραδύνεται σημαντικά το σύστημά τους, **3)** Άλλοι χρήστες δεν είναι ιδιαίτερα εξοικειωμένοι με την λειτουργία αυτών των λογισμικών και δεν μπορούν να κατανοήσουν τις αποφάσεις που λαμβάνει για προστασία το λογισμικό αυτό, **4)** Αρκετοί χρήστες δεν ενημερώνουν καθημερινά το λογισμικό τους και δεν έχουν πλήρη προστασία του Η/Υ, διότι η καθημερινή ενημέρωση είναι υποχρεωτική και αντιμετωπίζει πολλά είδη απειλών.

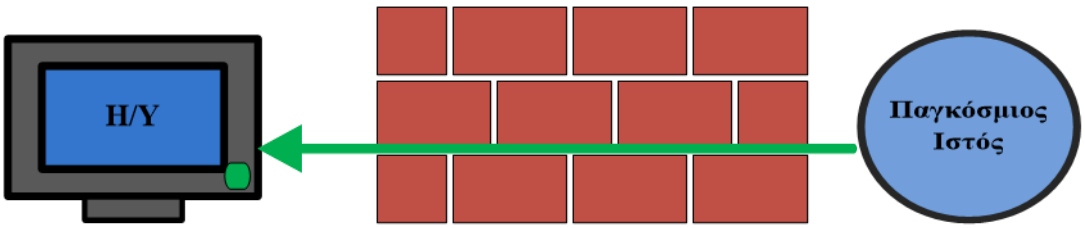
Επιπροσθέτως πρέπει να γνωρίζεται ότι με την αγορά και την εγκατάσταση ενός τέτοιου λογισμικού δεν μπορούμε να πούμε ότι θα έχουμε πλήρη προστασία. Η πιο χρήσιμη πρόληψη και προστασία μπορεί να την εφαρμόσει ο χρήστης κάθε Η/Υ, προσέχοντας την συμπεριφορά του κατά την διάρκεια που είναι στο *διαδίκτυο* και ακολουθώντας τις διάφορες συμβουλές ασφαλείας που είπαμε προηγουμένως.

7.2 Τείχος Προστασίας

Το *τείχος προστασίας* [21] (firewall) είναι το λογισμικό εκείνο όπου ελέγχει τις πληροφορίες που προέρχονται από το *διαδίκτυο* και έπειτα άλλες αφήνει να περάσουν στον Η/Υ και άλλες πληροφορίες τις αποκλείει, ανάλογα με τις διάφορες ρυθμίσεις που έχουμε κάνει στον Η/Υ. Συνιστώνται οι παρακάτω ρυθμίσεις να έχουμε κάνει στο *τείχος προστασίας*. **1)** Πρέπει να είναι πάντοτε ενεργοποιημένο, **2)** Να είναι ενεργοποιημένο για όλες τις συνδέσεις δικτύου μας, **3)** Πρέπει να έχουμε ορίσει ποιες συνδέσεις θα αποκλείει και ποιες θα επιτρέπει να στείλουν δεδομένα και πληροφορίες στον Η/Υ.

Τοποθετούμε ένα *τείχος προστασίας* [31] στον Η/Υ για να έχουμε πρόληψη και αποφυγή διάφορων ειδών επιθέσεων στο τοπικό μας δίκτυο. Απαιτείται σωστή ρύθμισή του και πολύ καλές γνώσεις στα δίκτυα υπολογιστών. Για άτομα που δεν γνωρίζουν πολλά πράγματα πάνω σε αυτό τον τομέα μπορούν να επιλέγουν τις προτεινόμενες ρυθμίσεις του Η/Υ τους για την ενεργοποίηση του *τείχους προστασίας*.

Στο παρακάτω σχήμα 7.1 που ακολουθεί παρατηρούμε τον τρόπο με τον οποίο λειτουργεί ένα *τείχος προστασίας*. Έχουμε: α) έναν Η/Υ, β) το τείχος προστασίας και γ) τον παγκόσμιο ιστό. Με πράσινο χρώμα είναι οι συνδέσεις που επιτρέπονται να περάσουν από τον διαδίκτυο μέσω του τείχους προστασίας στον προσωπικό μας υπολογιστή. Οι υπόλοιπες συνδέσεις είναι αυτές που δεν έχουμε ρυθμίσει να γίνονται αποδεκτές και βρίσκουν πάνω στο *τείχος προστασίας* και δεν εισέρχονται στον Η/Υ.



Σχήμα 7.1: *Τείχος Προστασίας*

7.3 Λογισμικά Φίλτρα

Με τον όρο λογισμικό φίλτρο εννοούμε ένα πακέτο λογισμικού το οποίο έχει την δυνατότητα να αποκλείσει την πρόσβαση σε διάφορες ιστοσελίδες με επιβλαβές περιεχόμενο για τον Η/Υ. Επιπλέον μέσω αυτού του λογισμικού εξασφαλίζουμε την προστασία των παιδιών μας ενάντια σε διάφορους κινδύνους του διαδικτύου.

Τα φίλτρα αυτά δίνουν την δυνατότητα στους γονείς να επιλέγουν και να απορρίπτουν διάφορες ιστοσελίδες με ακατάλληλο περιεχόμενο για τα παιδιά τους αλλά και να βλέπουν σε ποιες ιστοσελίδες προσπάθησαν να συνδεθούν.

7.4 Προστασία από Διάφορες Μορφές Ηλεκτρονικών Εγκλημάτων

Όπως είχαμε αναλύσει και σε προηγούμενα κεφάλαια οι διάφορες μορφές *ηλεκτρονικών εγκλημάτων* ποικίλουν την σημερινή εποχή. Για το λόγο αυτό κάθε χρήστης του Η/Υ πρέπει να είναι ενήμερος για τις διάφορες επιθέσεις που γίνονται καθημερινά σε ανυποψίαστους πολίτες κατά την πλοήγησή τους στο *διαδίκτυο*. Επίσης πρέπει να γνωρίζουμε μερικούς τρόπους ασφαλείας για την αποφυγή αλλά και την αντιμετώπιση τέτοιων εγκλημάτων.

7.4.1 Προστασία από Ανεπιθύμητη Αλληλογραφία

1. Δεν πρέπει ποτέ να απαντάμε σε κάποιο (spam) μήνυμα ηλεκτρονικού ταχυδρομείου, διότι με αυτό τον τρόπο δείχνουμε ότι η ηλεκτρονική μας διεύθυνση είναι ενεργή.
2. Δεν δημοσιεύουμε το e-mail και άλλα προσωπικά μας στοιχεία σε διάφορες ιστοσελίδες και σε διάφορους οργανισμούς τους οποίους δεν εμπιστευόμαστε.
3. Δεν προωθούμε ποτέ ένα τέτοιο μήνυμα στους φίλους μας.
4. Εγκαθιστούμε μερικά ειδικά φίλτρα τα οποία μπλοκάρουν αυτά τα e-mail.
5. Χρησιμοποιούμε πάντοτε κάποιο λογισμικό προστασίας από ιούς και κάνουμε καθημερινή ενημέρωσή του.

7.4.2 Προστασία από Κακόβουλο Λογισμικό

1. Επιλέγουμε ένα καλό λογισμικό προστασίας από ιούς.
2. Κάνουμε τακτική ενημέρωσή του.
3. Κάνουμε συχνή σάρωση του συστήματός μας.
4. Ελέγχουμε με το antivirus κάθε αφαιρούμενο δίσκο που εισάγουμε στον Η/Υ για τυχόν ιούς.
5. Κρατάμε ένα αντίγραφο ασφαλείας όλων των αρχείων του Η/Υ.
6. Δεν απενεργοποιούμε το τείχος προστασίας του υπολογιστή μας.
7. Είμαστε ιδιαίτερα προσεκτικοί κατά την λήψη αρχείων από το διαδίκτυο και την εγκατάσταση στον προσωπικό μας υπολογιστή.

7.4.3 Προστασία Προσωπικών Δεδομένων

1. Δεν αποκαλύπτουμε προσωπικά μας στοιχεία σε άγνωστα άτομα.
2. Δημιουργούμε έναν ξεχωριστό λογαριασμό ηλεκτρονικού ταχυδρομείου για τις ηλεκτρονικές μας συναλλαγές στο διαδίκτυο.
3. Έχουμε πάντα ενεργό το τείχος προστασίας του Η/Υ.

4. Χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης.

5. Έχουμε πάντοτε εγκατεστημένο και ενημερωμένο λογισμικό προστασίας από ιούς.

7.4.4 Προστασία Οικονομικών Συναλλαγών

1. Δεν πραγματοποιούμε οικονομικές συναλλαγές μέσω του διαδικτύου από Η/Υ στους οποίους έχουν πρόσβαση πολλοί πολίτες. Για παράδειγμα Η/Υ σε διάφορες βιβλιοθήκες, σε διάφορα internet cafe κ.λπ. Προτιμάμε τον προσωπικό μας υπολογιστή για τέτοιες ενέργειες.

2. Χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης και τους αλλάζουμε σε τακτά χρονικά διαστήματα.

3. Κάνουμε αγορές από γνωστές εταιρείες οι οποίες παρέχουν εγγυήσεις ασφαλείας.

4. Χρησιμοποιούμε διαφορετική κάρτα για αγορές μέσω του διαδικτύου. Σε περίπτωση κάποιας απάτης δεν χρειάζεται να ακυρώσετε όλες σας τις κάρτες.

5. Προστατεύουμε τον Η/Υ με λογισμικό antivirus.

6. Ελέγχουμε τακτικά τους λογαριασμούς μας και σε περίπτωση κάποιας ασυνήθιστης συναλλαγής ενημερώνουμε το ταχύτερο δυνατό την τράπεζά μας.

8.1 Επισκόπηση Εφαρμογής

Το Υπουργείο Εσωτερικών, η Ελληνική Αστυνομία και η Δίωξη Ηλεκτρονικού Εγκλήματος δημιούργησαν μια ιστοσελίδα η οποία έχει ως βασικό στόχο την ενημέρωση και την ευαισθητοποίηση παιδιών διαφόρων ηλικιών αλλά και τους γονείς τους, σχετικά με την ασφάλεια κατά την πλοήγησή τους στον χώρο του διαδικτύου.

Ο ιστότοπος αυτός δίνει χρήσιμες συμβουλές σχετικά με ψυχαγωγία και την προβολή διαφόρων θετικών στοιχείων που υπάρχουν στο *διαδίκτυο*. Επιπλέον γονείς και παιδιά έχουν την δυνατότητα να ενημερώνονται σε πραγματικό χρόνο για τους κινδύνους που υπάρχουν στον χώρο αυτό.

Η εφαρμογή αυτή διατίθεται και στα κινητά τηλέφωνα και πήρε χρυσό βραβείο στις 2 Απριλίου 2015 ως η καλύτερη εφαρμογή ως προς την κοινωνική ανάπτυξη. Η ηλεκτρονική διεύθυνση αυτής της ιστοσελίδας είναι η **www.cyberkid.gov.gr**

Στην παρακάτω εικόνα 8.1 παρατηρούμε το μενού αυτής της ιστοσελίδας. Πατώντας στο εικονίδιο Cyber Alert μεταφερόμαστε στην σελίδα της δίωξης ηλεκτρονικού εγκλήματος και μπορούμε οποιαδήποτε στιγμή θελήσουμε να μιλήσουμε με εξειδικευμένο προσωπικό της Ελληνικής Αστυνομίας και να κάνουμε κάποια καταγγελία.

Επίσης πατώντας στο εικονίδιο Ψηφιακή Αλάνα μέσω της παραπάνω ιστοσελίδας υπάρχουν πολλά ηλεκτρονικά παιχνίδια για παιδιά διαφορετικών ηλικιακών κατηγοριών. Επιπλέον μέσω αυτής της ιστοσελίδας μπορούν οι γονείς να έχουν μια συνεχή ενημέρωση για θέματα που σχετίζονται με την ασφάλεια των παιδιών τους στο διαδίκτυο, δίνονται χρήσιμες συμβουλές για διάφορα ζητήματα στο χώρο αυτό και πώς μπορούν οι γονείς να προτρέψουν τα παιδιά τους ώστε να παραμένουν λίγες ώρες στον Η/Υ.

Εικόνα 8.1: *Ιστότοπος Cyberkid [2]*

Η εφαρμογή αυτή αποτελεί ένα ενδιαφέρον ηλεκτρονικό μέσο ψυχαγωγίας αλλά και ενημέρωσης πολλών θεμάτων για αρκετά παιδιά. Στην παρακάτω εικόνα 8.2 παρατηρούμε ορισμένα παιχνίδια που διαθέτει η ιστοσελίδα αυτή και μπορούν οι γονείς να ενθαρρύνουν τα παιδιά τους να την επισκέπτονται και να πλοηγούνται με ασφάλεια.

Εικόνα 8.2: *Ηλεκτρονικά Παιχνίδια Ιστοσελίδας Cyberkid [2]*

Η ιστοσελίδα αυτή αποτελεί και ένα βασικό εργαλείο μάθησης για παιδιά ηλικίας μέχρι 8 ετών, αλλά και για παιδιά μεταξύ 12 - 18 ετών. Εκτός από τα παιχνίδια που υπάρχουν στην συγκεκριμένη ιστοσελίδα και αποτελούν και αυτά πηγή μάθησης μέσω του Η/Υ δίνονται επίσης συμβουλές για διάφορες μορφές ηλεκτρονικών εγκλημάτων όπως π.χ. παραβίαση προσωπικών δεδομένων, ηλεκτρονικό ψάρεμα κ.α, έτσι ώστε τα παιδιά να μαθαίνουν από μικρή ηλικία όχι μόνο για τα οφέλη και τις δυνατότητες του παγκόσμιου ιστού αλλά και για τα διάφορα προβλήματα που μπορεί να προκύψουν κατά την πλοήγησή του στο διαδίκτυο.

Στην παρακάτω εικόνα 8.3 παρατηρούμε διάφορες εφαρμογές της ιστοσελίδας αυτής όπως μπορούν τα παιδιά μας να επισκεφτούν στον συγκεκριμένο ιστότοπο ώστε να ενημερωθούν για τα βασικές πληροφορίες σχετικά με το διαδίκτυο π.χ. α) για τα κοινωνικά δίκτυα, β) για το λογισμικό αντιμετώπισης ιών κ.α. Επιπλέον δίνονται σημαντικές πληροφορίες που αφορούν την ασφάλειά του στον χώρο αυτό.

Εικόνα 8.3: *Ενημερωτικά Στοιχεία Ιστοσελίδας Cyberkid [2]*

Παραρτήματα

Τύπος βιβλιογραφικής πηγής	Αριθμός αναφοράς
Βιβλίο ξενόγλωσσο	[5, 3]
Βιβλίο ελληνικό	[7, 17]
Άρθρο σε επιστημονικό περιοδικό	[4]
Παρουσίαση σε επιστημονικό συνέδριο	[23, 24]
Ιστοσελίδα	[6, 9, 11, 10, 12, 13, 21, 2, 1, 20, 29]
Διπλωματική εργασία	[18, 22, 15]
Πτυχιακή εργασία	[8, 28, 25, 19, 16, 14]
Μεταπτυχιακή διπλωματική εργασία	[31, 30]
Διδακτορική διατριβή	[26, 27]

Βιβλιογραφία

[1] *Διεθνής Γραμμή Καταγγελιών*. https://www.safeline.gr/. Ημερομηνία πρόσβασης: 15-10-2015.

[2] *Ιστότοπος Cyberkid*. https://www.cyberkid.gov.gr/main.html. Ημερομηνία πρόσβασης: 10-10-2015.

[3] Robert Moore. *Cyber Crime*. Routledge, 2015.

[4] H. Berghel. 2012.

[5] John Townsend. *Cyber Crime*. Raintree, 2004.

[6] *Donn B. Parker*. http://en.wikipedia.org/wiki/Donn_B._Parker. Ημερομηνία πρόσβασης: 12-05-2015.

[7] Κωνσταντίνος Βλαχόπουλος. *Ηλεκτρονικό Έγκλημα*. Νομική Βιβλιοθήκη, 2007.

[8] Ελένη Σολδάτου. *Ηλεκτρονικό Έγκλημα*. Πτυχιακή εργασία, Τμήμα Πληροφορικής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2013.

[9] *Brain Virus*. http://en.wikipedia.org/wiki/Brain_computer_virus. Ημερομηνία πρόσβασης: 14-05-2015.

[10] *Λειτουργικό Σύστημα Unix*. http://en.wikipedia.org/wiki/Unix. Ημερομηνία πρόσβασης: 16-05-2015.

[11] *Μεταγλωττιστής σε Γλώσσα C*. http://en.wikipedia.org/wiki/Compiler. Ημερομηνία πρόσβασης: 16-05-2015.

[12] *Λογισμικό Packet Sniffer*. https://el.wikipedia.org/wiki/Packet_sniffer. Ημερομηνία πρόσβασης: 20-05-2015.

[13] *Πρωτόκολλο Διαδικτύου Internet Protocol, (IP)*. https://el.wikipedia.org/wiki/Internet_Protocol. Ημερομηνία πρόσβασης: 23-05-2015.

[14] Ελένη Καβουρτσίκη. *Μελέτη Τεχνικών και Μεθοδολογιών Έρευνας Κυβερνοεγκλήματος και Συλλογή Ψηφιακών Ιχνών*. Πτυχιακή εργασία, Τμήμα Διαχείρισης Πληροφοριών, ΤΕΙ Καβάλας, 2009.

[15] Ευαγγελία Ελπεκόγλου. *Διαδικτυακή Εγκληματικότητα, Σύγχρονες Μορφές Παραβατικότητας με Χρήση Η/Υ*. Διπλωματική εργασία, Πανεπιστήμιο Μακεδονίας, 2011.

[16] Δημήτριος Σιδερίδης, Γεωργία Σκαφιδά. *Ο Ρόλος του Κοινοτικού Νοσηλευτή στην Προστασία της Παιδικής Ηλικίας και το Ηλεκτρονικό Έγκλημα*. Πτυχιακή εργασία, Τμήμα Νοσηλευτικής, ΑΤΕΙ Θεσσαλονίκης, 2011.

[17] Ανδρέας Σουρής, Δημήτρης Πατσός, Νίκος Γρηγοριάδης. *Ασφάλεια της Πληροφορίας*. Νέων Τεχνολογιών, 2004.

[18] Κωνσταντίνα Λιανού. *Έγκλημα και Διαδίκτυο*. Διπλωματική εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, 2013.

[19] Χριστίνα Δημητριάδου. *Ηλεκτρονικό Έγκλημα*. Πτυχιακή εργασία, Τμήμα Πληροφορικής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2009.

[20] *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, Ελληνική Αστυνομία*. https://www.astynomia.gr. Ημερομηνία πρόσβασης: 14-10-2015.

[21] *Τείχος Προστασίας Firewall*. https://el.wikipedia.org/wiki/Firewall. Ημερομηνία πρόσβασης: 06-09-2015.

[22] Βασιλική Στούρη. *Εγκλήματα στο Διαδίκτυο*. Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, 2010.

[23] Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος . *Ασφαλή Πλοήγηση στο Διαδίκτυο* . *1ο Συνέδριο για την Ασφαλή Πλοήγηση στο Διαδίκτυο*, Divani Caravel Hotel, 2012.

[24] Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος . *Η Ασφαλή Πλοήγηση στο Διαδίκτυο είναι Υπόθεση όλων μας* . *4ο Συνέδριο για την Ασφαλή Πλοήγηση στο Διαδίκτυο*, Μέγαρο Μουσικής Αθηνών, 2015.

[25] Μυρσίνη Δημητρίου, Μαρία Παλιανιώτη. *Έρευνα για την Ασφάλεια των Παιδιών στο Διαδίκτυο*. Πτυχιακή εργασία, Τμήμα Διαχείρισης Πληροφοριών, ΤΕΙ Καβάλας, 2011.

[26] Φωτεινή Φραγκουλίδου. *Μελέτη των Επιδράσεων του Διαδικτύου στους Έφηβους Χρήστες*. Διδακτορική Διατριβή, ΑΠΘ Θεσσαλονίκης, 2006.

[27] Κωνσταντίνος Σιώμος. *Εθισμός των Εφήβων στους Η/Υ και στο Διαδίκτυο*. Διδακτορική Διατριβή, Πανεπιστήμιο Θεσσαλίας, 2008.

[28] Χριστίνα Αθανασοπούλου, Ράνια Μπαλαμάτση, Ελένη Μπέλου. *Ασφαλές Διαδίκτυο, Πεδίο Χειραφέτησης ή Πεδίο Χειραγώγησης*. Πτυχιακή εργασία, Τμήμα Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης, ΑΤΕΙ Θεσσαλονίκης, 2010.

[29] *Οδηγός Παιδικής Ασφάλειας στο Διαδίκτυο*. http://www.specialeducation.gr/files4users/files/pdf/web_safety_booklet.pdf. Ημερομηνία πρόσβασης: 18-10-2015.

[30] Μιχαήλ Στεφανουδάκης. *Εγκλήματα στο Διαδίκτυο, Εναλλακτικοί Τρόποι Εκδήλωσης και Αντιμετώπισης*. Μεταπτυχιακή διπλωματική εργασία, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά, 2011.

[31] Εμμανουέλα Παναγιωτάκη. *Προστασία του Καταναλωτή στο Διαδίκτυο*. Μεταπτυχιακή διπλωματική εργασία, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιά, 2010.

βλπ	βλέπε
ΔΙΔΗΕ	Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
Ε.Ε	Ευρωπαική Ένωση
Η/Υ	Ηλεκτρονικός Υπολογιστής
κ.α	και άλλα
κ.λπ.	και τα λοιπά
κ.ο.κ	και ούτω καθεξής
π.χ.	παραδείγματος χάριν

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος
ανίχνευση	detection
αντίδραση	reaction
απόκρυψη	suppression
αρχεία καταγραφής	log files
βάση δεδομένων	database
γονικός έλεγχος	parental control
διαγραφή	deletion
επισήμανση	tagging
ηλεκτρονική πειρατεία	hacking
ηλεκτρονικό έγκλημα	electonic crime
θύρα	port
ιός	virus
καταστροφή	damaging
κλοπή ταυτότητας	identity theft
κοινωνικά δίκτυα	social networks
κωδικός	password
όνομα χρήστη	username
παράνομη πρόσβαση	illegal access
πρόληψη	prevention
πρωτόκολλο μεταφοράς αρχείων	file transfer protocol
συναγερμοί	alarms
τείχος προστασίας	firewall
τηλεδιάσκεψη	videoconference
φθορά	deterioration

Ευρετήριο ελληνικών όρων

Ευρετήριο ξενόγλωσσων όρων

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ - ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ - ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Βασίλειος Π. Μαυριάς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΑΡΤΗ,
ΝΟΕΜΒΡΙΟΣ
2015

Θέση barcode

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ - ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ - ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Βασίλειος Π. Μαυριάς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΑΡΤΗ,
ΝΟΕΜΒΡΙΟΣ
2015

Θέση barcode

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Βασίλειος Π. Μαυριάς

ΣΠΑΡΤΗ

ΝΟΕΜΒΡΙΟΣ 2015

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ηλεκτρονικό Έγκλημα και Ασφάλεια των Παιδιών στο Διαδίκτυο

Βασίλειος Π. Μαυριάς

ΣΠΑΡΤΗ

ΝΟΕΜΒΡΙΟΣ 2015