Τ.Ε.Ι ΠΑΤΡΩΝ

ΣΧΟΛΗ ΕΠΑΓΓΕΛΜΑΤΩΝ ΥΓΕΙΑΣ ΚΑΙ ΠΡΟΝΟΙΑΣ ΤΜΗΜΑ ΚΟΙΝΩΝΙΚΗΣ ΕΡΓΑΣΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μορφές Ηλεκτρονικού Εγκλήματος και προτάσεις για την μείωση του φαινομένου: Οι απόψεις των ειδικών που ασχολούνται με το Ηλεκτρονικό Έγκλημα.

ΣΠΟΥΔΑΣΤΕΣ :

ΠΑΝΑΓΟΥ Β. ΑΙΚΑΤΕΡΙΝΗ

ΣΠΙΝΟΥ Σ. ΘΕΟΔΩΡΑ

ΕΙΣΗΓΗΤΗΣ : ΚΟΛΟΚΥΘΑΣ ΓΙΩΡΓΟΣ

ΠΑΤΡΑ,2010

Τ.Ε.Ι. ΠΑΤΡΑΣ

ΣΧΟΛΗ: Σ.Ε.Υ.Π.

ΤΜΗΜΑ: ΚΟΙΝΩΝΙΚΗ ΕΡΓΑΣΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

«Μορφές Ηλεκτρονικού Εγκλήματος και προτάσεις για την μείωση του φαινομένου: Οι απόψεις των ειδικών που ασχολούνται με το Ηλεκτρονικό Έγκλημα.»

ΕΡΕΥΝΗΤΙΚΗ ΟΜΑΔΑ:

ΠΑΝΑΓΟΥ Β. ΑΙΚΑΤΕΡΙΝΗ

ΣΠΙΝΟΥ Σ. ΘΕΟΔΩΡΑ

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:

ΚΟΛΟΚΥΘΑΣ ΓΕΩΡΓΙΟΣ

Πτυχιακή εργασία για τη λήψη πτυχίου στην Κοινωνική Εργασία από το τμήμα Κοινωνικής Εργασίας της Σχολής Επαγγελμάτων Υγείας και Πρόνοιας του Τεχνολογικού Εκπαιδευτικού Ιδρύματος (Τ.Ε.Ι) Πάτρας.

Πάτρα, Μάιος 2010

Η διπλωματική εργασία της Πανάγου Β. Αικατερίνης και της Σπίνου Σ. Θεοδώρας εγκρίνεται:

Υπογραφές

1. **Κολοκυθάς Γεώργιος , Καθηγητής (επιβλέπων καθηγητής)**

Μέλη εξεταστικής επιτροπής:

2. **……**

3. **……**

Στις οικογένειές μας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ **ΣΕΛΙΔΕΣ**

ΥΠΟΚΕΦΑΛΑΙΟ 5: Ασφάλεια στο Διαδίκτυο

ΕΥΧΑΡΙΣΤΙΕΣ

Μετά την ολοκλήρωση της μελέτης θεωρούμε χρέος μας να εκφράσουμε τις θερμότερες ευχαριστίες μας στους ανθρώπους που βοήθησαν για την επιτυχή έκβαση της.

Ευχαριστούμε τον υπεύθυνο καθηγητή μας κο Κολοκυθά Γεώργιο για τις κατευθύνσεις και τις επισταμένες συμβουλές του . Ιδιαίτερα σημαντική υπήρξε και η καθοδήγηση που λάβαμε από τον οδηγό συγγραφής πτυχιακής εργασίας ο οποίος συντάχθηκε από την κα. Ζαφειροπούλου Γ., την κα. Πανταζάκα Α., την κα. Πενταράκη Μ. και τον κο. Δρίτσα Ι., με την βοήθεια του οποίου βοηθηθήκαμε για την πληρέστερη αντιμετώπιση του γνωστικού αντικειμένου της διπλωματικής εργασίας.

Θα θέλαμε να ευχαριστήσουμε ιδιαίτερα τον κο Σφακιανάκη προϊστάμενο του τμήματος Δίωξης ηλεκτρονικού εγκλήματος του νομού Αττικής ο οποίος συνεργάστηκε με μεγάλη προθυμία και προσέφερε αμέριστα κατευθύνσεις για την επιτυχή έκβαση της έρευνας μας καθώς και τον κο Παπαντωνίου του τμήματος Δίωξης ηλεκτρονικού εγκλήματος του νομού Θεσσαλονίκης .

Ιδιαίτερα, ευχαριστούμε για την συνεργασία, τους ψυχολόγους από το νομό Θεσσαλονίκης και Αττικής, τους προγραμματιστές από το νομό Ημαθίας και Αττικής, την νομικό από το νομό Αττικής και την διδάσκουσα του ΑΠΘ για την παροχή των απαραίτητων δεδομένων και συνεντεύξεων , χωρίς τις οποίες θα ήταν αδύνατη η πραγματοποίηση της έρευνας.

Επιπλέον ευχαριστούμε προσωπικά η μία την άλλη για την άψογη συνεργασία μας κατά την διάρκεια της μελέτης μας δίνοντας στήριξη και βοήθεια για την ολοκλήρωση της .

Τέλος, θεωρούμε υποχρέωσή μας να ευχαριστήσουμε τις οικογένειές μας που συνέβαλαν με το δικό τους τρόπο στην πραγματοποίηση αυτής της εργασίας.

ΠΕΡΙΛΗΨΗ

Η διπλωματική εργασία έχει θέμα : «Μορφές Ηλεκτρονικού Εγκλήματος και προτάσεις για την μείωση του φαινομένου: Οι απόψεις των ειδικών που ασχολούνται με το Ηλεκτρονικό Έγκλημα.» Αποτελείται από δυο μέρη, το θεωρητικό και το ερευνητικό, και συνολικά από δώδεκα κεφάλαια.

Το πρώτο μέρος είναι το θεωρητικό και περιέχει οχτώ κεφάλαια.

Το πρώτο κεφάλαιο έχει τίτλο «Ηλεκτρονικό έγκλημα». Στο κεφάλαιο αυτό καταγράφονται κάποιοι ορισμοί εννοιών ,παρουσιάζεται όλη η ιστορική αναδρομή του διαδικτύου και του εγκλήματος και επιχειρείται η εξέταση των διάφορων μορφών εγκλήματος ,τα οποία διακρίνονται σε γνήσια ηλεκτρονικά εγκλήματα που τελούνται μόνο στον κυβερνοχώρο και σε εγκλήματα που τελούνται με την χρήση ηλεκτρονικών υπολογιστών .

Στο κεφάλαιο δύο με τίτλο «Άλλες μορφές ηλεκτρονικού εγκλήματος» περιγράφονται και άλλες μορφές εγκλημάτων στις οποίες συμμετέχουν και άλλες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων ,όπως τα κινητά τηλέφωνα ,οι παιχνιδομηχανές και τα μηχανήματα ανάληψης μετρητών .

Στο κεφάλαιο τρία με τίτλο «Προφίλ θύματος» περιγράφεται το προφίλ του θύματος και τα χαρακτηριστικά του καθώς και τρόποι για την πρόληψη της θυματοποίησης .

Στο κεφάλαιο τέσσερα με τίτλο «Το προφίλ των δραστών» καταγράφεται το προφίλ των δραστών καθώς και οι κατηγορίες δραστών ηλεκτρονικών εγκλημάτων.

Στο κεφάλαιο πέντε με τίτλο «Ασφάλεια στο Διαδίκτυο» καταγράφονται χρήσιμες συμβουλές και προληπτικά μέτρα για την προστασία των χρηστών.

Στο κεφάλαιο έξι με τίτλο «Χαρακτηριστικά Γνωρίσματα του Εγκλήματος στον Κυβερνοχώρο» αναφέρονται τα ποιοτικά χαρακτηριστικά του εγκλήματος στον κυβερνοχώρο .

Στο κεφάλαιο εφτά με τίτλο «Η Παρέκκλιση στον Κυβερνοχώρο σε Παγκόσμιο Επίπεδο» καταγράφεται μία Παγκόσμια Προσέγγιση της Παρέκκλισης στον Κυβερνοχώρο .

Στο κεφάλαιο οχτώ με τίτλο «Νομοθεσία» προσεγγίζονται τα νομικά ζητήματα που προκύπτουν από την εφαρμογή του ισχύοντος δικαίου. Επίσης παρατίθεται η ισχύουσα στην Ελλάδα νομοθεσία για το ηλεκτρονικό έγκλημα .

Το δεύτερο μέρος της διπλωματικής εργασίας είναι το ερευνητικό μέρος και περιλαμβάνει δυο κεφάλαια.

Το δεύτερο κεφάλαιο με τίτλο «Μεθοδολογία έρευνας» περιλαμβάνει το είδος της έρευνας, τον σκοπό και τους στόχους της, τις ερευνητικές υποθέσεις, τον πληθυσμό και το δείγμα, το εργαλείο της έρευνας, τον τόπο και χρόνο πραγματοποίησης της έρευνας. Καθώς και ζητήματα δεοντολογίας, προσβασιμότητα, κατηγοριοποίηση και ανάλυση δεδομένων και αποτελέσματα της έρευνας.

Το τρίτο κεφάλαιο με τίτλο «Μεθοδολογία ανάλυσης» περιλαμβάνει την κωδικοποίηση και την ανάλυση δεδομένων .

Το τέταρτο κεφάλαιο με τίτλο «Παρουσίαση αποτελεσμάτων έρευνας» παρουσιάζονται τα αποτελέσματα της έρευνας.

Το πέμπτο κεφάλαιο με τίτλο «Συμπεράσματα και προτάσεις για μελλοντικές έρευνες » αναφέρει τα συμπεράσματα και τις προτάσεις των ερευνητριών για αντιμετώπιση του φαινομένου και για μελλοντικές έρευνες.

Ακολουθεί το παράρτημα όπου συμπεριλαμβάνει τις αυτούσιες συνεντεύξεις των ειδικών και τον οδηγό συνέντευξης.

Summary Final

The diplomatic work has subject "Forms of Cyber Crime and suggestions for reducing this phenomenon: The views of experts who deal with cyber crime." It consists of two parts: theory and research, and it has a total of twelve chapters.

The first part is theoretical and contains eight chapters:

The first chapter is titled «Cybercrime» in this chapter, definitions are recorded, concepts are presented throughout the history of the internet and crime and an attempt is made to examine the various forms of crime which is divided into original electronic crimes committed only in cyberspace and in crimes committed using computers.

In Chapter two, entitled «Other forms of cyber crime »other forms of crimes are also described, involving other data processing devices such as mobile phones, game consoles and ATM.

In chapter three entitled «Profile victim» the profile of the victim and the characteristics of and ways to prevent victimization are described.

In chapter four, entitled «The profile of offenders» the profile of the perpetrators and the perpetrators of computer crimes categories are described.

In chapter five titled «Internet Safety Useful Tips and Preventive Measures for the Protection of Users »are recorded.

In chapter six, entitled «Features of cybercrime» qualities of cybercrime are mentioned.

In chapter seven «The transgression in cyberspace» a Global Approach to the transgression in Cyberspace is reported.

In chapter eight entitled «Legislation» the legal issues arising from the application of the applying laws are approached. Furthermore, the Greek legislation on cyber crime is presented.

The second part of this thesis is the research part and consists of four chapters.

The second chapter, entitled «Survey Methodology» includes the type of research, the purpose and objectives, the research hypotheses, population and sample research, place and time of the research. Also, ethical issues, accessibility, categorization and analysis of data and research results.

The third chapter entitled "Methodology analysis "consists of the coding and data analysis.

The fourth chapter, entitled "Presentation of research results" presents the results of the investigation.

The fifth chapter entitled "Conclusions and suggestions for future research," said the conclusions and recommendations of researchers to address the problem and for future research.

The twelfth chapter entitled «Conclusions» contains the conclusions of the research by researchers, and also proposals.

Then follows the Annex which includes interviews from specialists and the interview guide.

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία έχει σκοπό να παρουσιάσει τις μορφές του ηλεκτρονικού εγκλήματος στην Ελλάδα αλλά και να αναδείξει το ήδη υπάρχον πρόβλημα προτείνοντας τρόπους και μέτρα πρόληψης για την εξασφάλιση ενός ασφαλέστερου δικτύου τόσο για τους εξειδικευμένους του είδους, όσο κυρίως και για τους απλούς χρήστες του διαδικτύου.

Παρόλο όμως τη ραγδαία εξέλιξη της τεχνολογίας, την ανάπτυξη της πληροφορικής και την ευρύτατη χρήση του Διαδικτύου, που αναμφίβολα έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές της καθημερινότητας μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

(Μάτσα,2009)

Η διπλωματική μας εργασία έχει θέμα: «Μορφές Ηλεκτρονικού Εγκλήματος και προτάσεις για την μείωση του φαινομένου: Οι απόψεις των ειδικών που ασχολούνται με το Ηλεκτρονικό Έγκλημα.» Μέσω αυτής της πρωτότυπης έρευνας αισιοδοξούμε να δοθούν νέα ερεθίσματα για παραπάνω σκέψη, για ευρύτερη και αναλυτικότερη εμβάθυνση και ενασχόληση με το πρόβλημα της παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο.

Σκοπός της παρούσας έρευνας είναι η διερεύνηση, η καταγραφή, η ανάλυση και η αποσαφήνιση του προβλήματος της παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο .

Επιπλέον, η διεξαγωγή της έρευνας μέσω συνεντεύξεων από ειδικούς με εμπειρία και γνώσεις απέναντι στο θέμα του ηλεκτρονικού εγκλήματος θα επιτρέψει την εις βάθος κατανόηση του φαινομένου αλλά και θα μας προσφέρει λύσεις και τρόπους για την ασφαλέστερη πλοήγηση μας στο ιντερνέτ. Το θέμα αφορά την ηλεκτρονική εγκληματικότητα. Γίνεται

εκτενής αναφορά αρχικά στην ιστορική αναδρομή του διαδικτύου και του εγκλήματος και επιχειρείται εξέταση των διάφορων μορφών εγκλήματος. Επίσης καταγράφονται χρήσιμες συμβουλές και προληπτικά μέτρα για την προστασία των χρηστών .Τέλος προσεγγίζονται τα νομικά ζητήματα που προκύπτουν από την εφαρμογή του ισχύοντος δικαίου και παρατίθεται η ισχύουσα στην Ελλάδα νομοθεσία για το ηλεκτρονικό έγκλημα

Προβλήματα που αντιμετωπίστηκαν κατά την διεξαγωγή της διπλωματικής εργασίας ήταν η ελλιπής βιβλιογραφία για τον κοινωνικό λειτουργό σε σχέση με το ρόλο του στην αντιμετώπιση της παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο . Επίσης τα πιο πρακτικά βιβλία δεν ήταν διαθέσιμα στις δημόσιες βιβλιοθήκες και έπρεπε να αγοραστούν. Το μεθοδολογικό πλαίσιο περιλάμβανε την ποιοτική έρευνα, με εργαλείο την ημι-δομημένη συνέντευξη. Πληθυσμός της έρευνας αποτέλεσαν ειδικοί με εμπειρία και γνώσεις στο διαδίκτυο και το δείγμα ήταν 8 άτομα από το νομό Αττικής, Θεσσαλονίκης και το νομό Ημαθίας.

ΜΕΡΟΣ Α

ΚΕΦΑΛΑΙΟ 1
ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ/ΑΝΑΣΚΟΠΗΣΗ ΣΥΝΑΦΩΝ ΜΕΛΕΤΩΝ ΚΑΙ ΕΡΕΥΝΩΝ

ΥΠΟΚΕΦΑΛΑΙΟ 1: Το ηλεκτρονικό έγκλημα

1.1 Ορισμοί Εννοιών

1.1.1 Ηλεκτρονικά Εγκλήματα

Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των ατομικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον των περιουσιακών αγαθών. (Γαλανόπουλος, 2006)

1.1.2 Ηλεκτρονικό Έγκλημα

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη , η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο. (Αργυρόπουλος ,2006)

Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου. (Αργυρόπουλος ,2006)

1.1.3 Συνθήκη της Βουδαπέστης.

«Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα». (Λάζος,2001 σελ.35)

«Οι Μορφές Κυβερνοεγκλήματος. Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «CyberCrime... and Punishment» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες: Παρεμπόδιση (κυβερνο)κυκλοφορίας, Τροποποίηση και Κλοπή δεδομένων, Εισβολή και Σαμποτάζ σε δίκτυο, Μη εξουσιοδοτημένη πρόσβαση, Διασπορά ιών, Υπόθαλψη αδικημάτων, Πλαστογραφία και Απάτη». (Αργυρόπουλος ,2006 σελ.80)

Οι κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ είναι:

1. Απάτες μέσω Διαδικτύου.
2. Παιδική πορνογραφία.
3. Cracking και hacking.
4. Διακίνηση-πειρατεία λογισμικού.
5. Πιστωτικές κάρτες.
6. Διακίνηση ναρκωτικών.
7. Έγκλημα στα chat rooms(http://www.e-crime.gr/news.htm)

1.1.4 Ορισμός Internet

Ιντερνέτ ή αλλιώς διαδίκτυο είναι ένα δίκτυο υπολογιστών συνδεδεμένοι μεταξύ τους. Οι κυριότεροι λόγοι ύπαρξης ενός δικτύου είναι για:

1.να μπορούν οι χρήστες των υπολογιστών να επικοινωνούν μεταξύ τους και

2. να χρησιμοποιούν από απόσταση τις υπηρεσίες που προσφέρει κάποιος υπολογιστής του δικτύου. (Αργυρόπουλος ,2006)

1.2 Ιστορική Αναδρομή

1.2.1 Ιστορική Αναδρομή για το Έγκλημα

Το έγκλημα αποτελεί αναπόσπαστο κομμάτι κάθε οργανωμένης κοινωνίας εδώ και αιώνες .Ανέκαθεν οι άνθρωποι αντιδρούν και παραβιάζουν τους κανόνες και τους νόμους που έχει ορίσει η κοινωνία με αποτέλεσμα να δέχονται τις ανάλογες κυρώσεις ώστε να συμμορφωθούν .Το είδος της ποινής που θα επιβάλει η κάθε κοινωνία ώστε να επιβληθεί στο άτομο που παρέβη τους κανόνες της εξαρτάται από την εποχή και τον πολιτισμό .Παρόλο την ύπαρξη των νομικών συστημάτων καμιά χώρα δεν απαλλάχθηκε από το έγκλημα αντίθετα παρατηρείται μια συνεχής αύξηση του και παράλληλα η εμφάνιση νέων μορφών εγκλήματος και η αποποινικοποίηση των υφιστάμενων εγκλημάτων . (Βλαχόπουλος,2007)

Το εγκληματικό φαινόμενο συνθέτουν τρία βασικά στοιχεία :ο κανόνας (ποινικός νόμος)β)παράβαση (έγκλημα)και γ)η κύρωση (ποινή).

Α)Κανόνας (ποινικός νόμος) :Η κοινωνική ζωή έχει ανάγκη να θεσπίζονται κάποιοι κανόνες συμπεριφοράς ,σημασία παίζει πάντα το πολιτικό σύστημα ,οι κοινωνικές αλλά και οικονομικές καταστάσεις .Συγκεκριμένα όταν ο κανόνας προβλέπει τις παραβιάσεις και τις ποινές ,τότε έχουμε να κάνουμε με ποινικό νόμο . (Βλαχόπουλος,2007)

β)Η παράβαση (έγκλημα) :Το έγκλημα υπάρχει σε όλη την κοινωνία και σε όλες τις εποχές καθώς δεν είναι δυνατόν όλα τα μέλη της κοινωνίας να

συμμορφωθούν στους ίδιους κανόνες αφού δεν έχουν την ίδια προσωπικότητα και κοινωνικοοικονομική κατάσταση .Το έγκλημα θα μπορούσαμε να το χαρακτηρίσουμε και ως χρήσιμο πέρα από αρνητικό αφού η κάθε εγκληματική πράξη εξεγείρει την συλλογική συνείδηση και επιφέρει ηθικές και νομικές αλλαγές . (Βλαχόπουλος,2007)

γ)Η κύρωση: Η ποινή αποτελεί την συνέπεια της παράβασης του κανόνα .Υπάρχει μια διάκριση μεταξύ των σκοπών που εξυπηρετεί η πρόβλεψη και η επιβολή της ποινής, υπάρχουν δύο προσεγγίσεις η ανταπόδοσης και της κοινωνικής άμυνας .Σύμφωνα με την προσέγγιση της κοινωνικής άμυνας η κύρωση προβλέπεται και επιβάλλεται κατά του δράστη ,προκειμένου οι υπόλοιποι πολίτες να παραδειγματιστούν και διαπαιδαγωγηθούν ώστε να υπάρχει γενική πρόληψη και κοινωνική χρησιμότητα .Αντίθετα με την προσέγγιση της ανταπόδοσης ο νόμος υπάρχει ώστε να ανταποδώσει το κακό που έγινε με την πληρωμή του κακού που έγινε με κάτι άλλο ισάξιο . (Βλαχόπουλος,2007)

1.2.2 Ιστορική Αναδρομή Διαδικτύου

Δεκαετία '60: Η αρχή του θαύματος: «Όλα ξεκίνησαν κατά την περίοδο του Ψυχρού Πολέμου μεταξύ της τότε ΕΣΣΔ και των ΗΠΑ. Στη σκέψη των Αμερικανών, υπήρχε η σχεδίαση ενός δικτύου, το οποίο σε περίπτωση πυρηνικού πολέμου, δεν θα κατέρρεε. Η σκέψη αυτή υλοποιήθηκε από την εταιρεία ARPA(Advance Research Projects Agency), η οποία ανέπτυξε ένα δίκτυο υπολογιστών στα τέλη της δεκαετίας του 1960. Το όνομα αυτού ARPAnet. Το δίκτυο αυτό αποτελούνταν αρχικά από τέσσερις(4) υπολογιστές, 3 εκ των οποίων βρίσκονταν στην Καλιφόρνια και ένας(1) στην πολιτεία της Γιούτα. Το πρωτόκολλο που χρησιμοποιήθηκε για την κατασκευή του συγκεκριμένου δικτύου ήταν το NCP(Network Control Protocol). Κάπως έτσι λοιπόν ξεκίνησε το διαδίκτυο. «Οκτώβριος 1969, στο πανεπιστήμιο του Stanford μια ομάδα ειδικών στους Η/Υ στέκεται γύρω από την οθόνη ενός υπολογιστή. Την ίδια στιγμή, στην άλλη άκρη της πολιτείας, στο Πανεπιστήμιο UCLA σε ένα αντίστοιχο δωμάτιο υπάρχει ένα παρόμοιο σκηνικό. Όταν οι λέξεις που εμφανίστηκαν στην οθόνη του L.A.

ήταν οι ίδιες με εκείνες στο Stanford, η πρώτη συνομιλία μεταξύ δύο υπολογιστών είχε επιτευχθεί και το ARPAnet είχε γεννηθεί.» Αργότερα με το πέρασμα των χρόνων εξελίχθηκε, εμφανίστηκαν οι όροι TCP/IP ως πλέον το πιο προσφιλή πρωτόκολλο εν χρήση, BITNET(because its time network), CSNET(Computer Science Networks), NSFNET(National Foundation Network) το μεγαλύτερο backbone δίκτυο στην εποχή του. Η ARPANET αργότερα διασπάστηκε σε ARPANET και σε MILnet (Military Network)». (Λάζος,2001)

Δεκαετία '70: Τα πρώτα βήματα: Μέσα στη δεκαετία του ‘70 το ARPAnet μεγάλωσε. Περισσότεροι κόμβοι συνδέθηκαν και ακόμη περισσότεροι χρήστες χρησιμοποιούσαν καθημερινά τις υπηρεσίες του δικτύου. Οι χρήστες δεν προέρχονταν πια μόνο από ακαδημαϊκές κοινότητες και ιδρύματα, αλλά οποιοσδήποτε μπορούσε να συνδεθεί μ’ αυτό, εφ’ όσον διέθετε έναν υπολογιστή που να μπορεί να μιλά τη γλώσσα του δικτύου, αλλά κι ένα λογαριασμό (άδεια πρόσβασης) σε κάποιον πανεπιστημιακό υπολογιστή. (Λάζος,2001)

«Το 1973 ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Internetting Project (Πρόγραμμα Διαδικτύωσης), προκειμένου να ενοποιηθούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται το Internet Protocol (IP), από το οποίο θα πάρει αργότερα το όνομά του το Internet. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Επίσης, σχεδιάζεται μια άλλη τεχνική για τον έλεγχο της μετάδοσης των δεδομένων, το Transmission Control Protocol (TCP). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (Email). Σταδιακά συνδέονται με το ARPAnet ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία)». (Λάζος,2001 σελ.55)

Δεκαετία '80: Το Δίκτυο παίρνει μορφή: «Το 1983 το πρωτόκολλο TCP/IP αναγνωρίζεται ως πρότυπο από το αμερικανικό υπουργείο Άμυνας. Η έκδοση του λειτουργικού συστήματος Berkeley UNIX, το οποίο περιλαμβάνει το TCP/IP, συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών. Εκατοντάδες πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPAnet, το οποίο επιβαρύνεται πολύ, και το 1983 χωρίζεται σε MILNET (για στρατιωτικές επικοινωνίες) και στο νέο ARPAnet (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση)». (Λέανδρος ,2005 σελ 250)

«Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το NSFnet, χρησιμοποιώντας το TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπερυπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας, όλο και περισσότερες χώρες συνδέονται στο NSFnet. Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα, τα οποία κατόπιν συνδέουν στο παγκόσμιο δίκτυο, το οποίο αρχίζει να γίνεται γνωστό ως Internet και να εξαπλώνεται ραγδαία σε ολόκληρο τον κόσμο». (Λέανδρος ,2005 σελ 250)

Δεκαετία '90: Το Δίκτυο γίνεται προσιτό: Η Ελλάδα συνδέεται με το NSFnet το 1990. Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει τον Παγκόσμιο Ιστό (World Wide Web - WWW) του Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών multimedia που βρίσκονται αποθηκευμένες σε δικτυωμένους υπολογιστές, και παρουσίασης τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον κάνει την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Διαδικτύου (Internet Service Providers - ISP) και προσφέρουν πρόσβαση σε όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFnet καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα. Το 1995, οι συνολικοί κόμβοι ήταν δεκάδες χιλιάδες, ενώ περισσότεροι από πέντε (5) εκατομμύρια περίπου χρήστες ανά τον κόσμο συνδέονται καθημερινά στο δίκτυο για τις συναλλαγές τους, για να

συνομιλήσουν, να ανταλλάξουν απόψεις, γνώσεις και προγράμματα και γενικά για να βγουν on-line. (Λέανδρος ,2005)

Το Internet στον 21ο αιώνα: Το Διαδίκτυο δεν αποτελεί πλέον ένα μέσο επικοινωνίας και ανταλλαγής δεδομένων αποκλειστικά μεταξύ φοιτητών και ερευνητών. Έχει επεκταθεί και εισβάλει στην καθημερινότητα όλων. Ήδη μιλάμε για ηλεκτρονικό εμπόριο, τηλεργασία, τηλεκπαίδευση, τηλεϊατρική. Ο πλανήτης είναι, με λίγα λόγια, δικτυωμένος. Και με το πέρασμα του χρόνου θα δικτυώνεται ολοένα και περισσότερο. (Ζαννή,2005)

Το Internet εδώ και πολλά χρόνια είναι ιδιαίτερα δημοφιλές στη παγκόσμια κοινότητα κι έχει συμβάλει πάρα πολύ στην έρευνα και στη διαπροσωπική επικοινωνία. Ο ρυθμός ανάπτυξής του είναι πολύ εντυπωσιακός αφού ο αριθμός των κόμβων του (hosts) διπλασιάζεται κάθε χρόνο. (Ζαννή,2005)

Οι ημερομηνίες που αποτέλεσαν σταθμό στην ιστορία του Ιντερνέτ.

- 1960 Εφεύρεση της μεταγωγής δεδομένων
- 1967 Σχέδια υλοποίησης της θεωρίας μεταγωγής πακέτων
- 1969

Ορίζεται η ARPAnet από το Υ.ΕΘ.Α των ΗΠΑ, να ερευνήσει την δυνατότητα διαδικτύωσης των υπολογιστών.

Σύνδεση των πρώτων 4 κέντρων

- 1970 Χρήση του Network Control Protocol (NCP) των κόμβων (=nodes) του ARPAnet.
- 1972 Ίδρυση του InterNetworking Working Group (INWG) με σκοπό τον ορισμό των standards.
- 1973 Πρώτες διεθνές συνδέσεις του ARPAnet. Σύνδεση με Νορβηγία και Βρετανία
- 1976 Αναπτύχθηκε το UUCP (Unix to Unix Copy Protocol) από την AT&T Bell Labs.
- 1979 Γέννηση του USEnet που κάνει χρήση του UUCP
- 1981 Ίδρυση των BITNET και CSNET

- 1982 Το INWG ορίζει το TCP/IP σαν το πρωτόκολλο του ARPAnet. Το Υπουργείο Άμυνας των ΗΠΑ το υιοθετεί.
- 1983

Δημιουργία του Name Server από το Πανεπιστήμιο του Wisconsin. Οι χρήστες δεν χρειάζεται να ξέρουν την διαδρομή για να βρουν τα άλλα συστήματα.

Διάσπαση του ARPAnet σε ARPAnet και MILnet

- 1984 Εγκατάσταση του DNS (Domain Name Server). 1,000 hosts
- 1986 Ίδρυση του NSFnet με κορμό στα 56Kbps
- 1989 Αναβάθμιση του κορμού του NSFnet σε T1, 1.544Mbps.

100,000 hosts

- 1990

Κατάργηση του ARPAnet.

Ίδρυση της Electronic Frontier Foundation (EFF).

Ανακοινώνεται η υπηρεσία Archie

- 1991

Ίδρυση του Commercial Internet Exchange (CIX).

Δημιουργία των υπηρεσιών WAIS και Gopher

- 1992

Ίδρυση της Internet Society.

Το CERN δημιουργεί το World-Wide-Web.

Ο κορμός του NSFnet αναβαθμίζεται σε T3 δηλ. 44.736Mbps.

Πάνω από 1,000,000 hosts στο Internet

- 1993

Ιδρύεται το InterNIC από την NSF με σκοπό την παροχή πληροφοριών στους χρήστες.

Τα MME δίνουν σημασία στο Internet.

- 1994 Αλλαγή πολιτικής του NSF. Ο έλεγχος του κορμού περνάει σε ιδιώτες ενώ άρονται οι περιορισμοί που αφορούσαν τις διεθνείς συνδέσεις

(http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm)

Έτος-	**Αριθμός υπολογιστών**
1977	111
1981	213
1983	562
1984	1.000
1986	5.000
1987	10.000
1989	100.000
1992	1.000.000
2001	175.000.000
2002	>200.000.000
2010	80% του πλανήτη θα είναι στο διαδίκτυο

(http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm)

1.2.3 Ιστορική Αναδρομή Ηλεκτρονικού Εγκλήματος

Στις αρχές τις δεκαετίας του 20ου αιώνα νέες τεχνικές για την διάπραξη εγκλημάτων δημιουργήθηκαν .Με την ανάπτυξη της τεχνολογίας και των ηλεκτρονικών υπολογιστών συντελούνται αλλαγές και στο εγκληματικό φαινόμενο .Εμφανίζονται νέες μορφές εγκλήματος που το μέσω διάπραξης τους είναι ο ηλεκτρονικός υπολογιστής και άλλες παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων . (Βλαχόπουλος,2007)

Οι ρίζες του ηλεκτρονικού εγκλήματος ανιχνεύονται ταυτόχρονα κατά την εμφάνιση των υπολογιστών .Οι επίδοξοι ηλεκτρονικοί εγκληματίες εκμεταλλεύονταν τις νέες ευκαιρίες για την διάπραξη πλήθους εγκλημάτων. Χρονικά η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα .Στις πρώτες δεκαετίες της σύγχρονης τεχνολογίας πληροφοριών τα εγκλήματα υπολογιστών διαπράττονταν συνήθως από δυσαρεστημένους και ανέντιμους εργαζόμενους . (Βλαχόπουλος,2007)

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία. (Βλαχόπουλος,2007)

1960-1980: Η εποχή της αθωότητας-σαμποτάζ: Η σωματική βλάβη σε συστήματα ηλεκτρονικών υπολογιστών ήταν μια σημαντική απειλή, τεκμηριώθηκαν οι θεωρίες για την μετάδοση ιών όπως rabbits ,δούρειοι ίπποι. Η αποστολή ιών (Trojan Horses, worms κ.ά.) μέσω του ηλεκτρονικού ταχυδρομείου έχουν την ιδιότητα να εισβάλλουν στα προγράμματα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου, να διαβάζουν όλες τις καταχωρημένες διευθύνσεις, να αυτό-αποστέλλονται και τελικά να καταστρέφουν εταιρικούς ή ακαδημαϊκούς servers προκαλώντας ζημιές δισεκατομμυρίων δολαρίων. (Ζαννή,2005)

Οι εγκληματίες συχνά είχαν στους υπολογιστές των εταιριών με σκοπό να υπονομεύσουν τα συστήματα ασφαλείας για οικονομικό κέρδος και για εκδίκηση . (Ζαννή,2005)

1980- Μέχρι τα μέσα της δεκαετίας του 1990:Το ηλεκτρονικό έγκλημα έκανε τη μαζική του εμφάνιση στις αρχές της δεκαετίας του '80. Αρχικό εργαλείο ήταν η πρόσβαση από ένα υπολογιστικό σύστημα σε άλλο, με τη χρήση του modem. (Ζαννή,2005)

Οι ανταλλαγές των πληροφοριών για τα «σπασμένα» δίκτυα και συστήματα γίνονταν μέσω των σχεδόν πρωτόγονων βάσεων δεδομένων των BBS (Bulletin Broad Systems). Ήταν τα πρώτα βήματα για τη δημιουργία μιας υπόγειας κοινωνίας χρηστών του Διαδικτύου και τα πρώτα ακούσματα των όρων όπως hacking, phreaking και άλλες απάτες με πιστωτικές κάρτες ήταν ένα ολοένα και αυξανόμενο πρόβλημα των καταναλωτών και για το δίκαιο επιβολής .Αναφορικά ο Morris worm προσέβαλλε 6.000 υπολογιστές οδηγώντας στην δημιουργία του πρώτου cert .

Αξίζει να αναφερθεί πως ο τομέας των ηλεκτρονικών αδικημάτων όπου η Ελλάδα επαξίως διεκδικεί την πρώτη θέση αυτή την δεκαετία, τουλάχιστον σε ευρωπαϊκό επίπεδο, είναι η πειρατεία λογισμικού. (Ζαννή,2005)

Τέλη δεκαετίας του 1990-2000:οι απάτες των πιστωτικών καρτών εντάχθηκαν σε μια ευρύτερη κατηγορία της κλοπής ταυτότητας η ταχύτερη μορφή απάτης σήμερα .Επίσης αναπτύχθηκαν ραγδαία και άλλες μορφές εγκλήματος όπως το ξέπλυμα χρήματος ,η διακίνηση πορνογραφικού υλικού ,η διαδικτυακή τρομοκρατία ,οι επιθέσεις παρενόχλησης κ.α. . Το 2007 ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί. Σήμερα οι υπολογιστές χρησιμοποιούνται σε όλες τις καθημερινές μας δραστηριότητες και τα προσωπικά μας δεδομένα ,οι τραπεζικοί μας λογαριασμοί και οτιδήποτε κάνουμε αποθηκεύεται στο πληροφοριακό σύστημα .Το νέο αυτό περιβάλλον χαρακτηρίζεται από την ανάπτυξη του ηλεκτρονικού εμπορίου ,την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου ,ευνοώντας ταυτόχρονα την επικοινωνία μέσα από τα κοινωνικά δίκτυα και τέλος την εξ αποστάσεως εκπαίδευση ,την πραγματοποίηση τηλεδιασκέψεων , τηλεργασιών, τηλεϊατρικής κ.α. (Ζαννή,2005)

1.2.4 Πως ξεκίνησαν οι έρευνες των εγκλημάτων στο διαδίκτυο

- → Μία έρευνα απαγωγής στο Maryland των Η.Π.Α. το 1994 είχε αποτέλεσμα να ανακαλυφθεί ότι οι παιδόφιλοι συναντιούνταν στο Internet.
- → Το 1995, μια νέα επιχείρηση από πράκτορες FBI ξεκίνησε με σκοπό την αποκάλυψη και την τιμωρία των παιδόφιλων που δραστηριοποιούνταν μέσω του διαδικτύου(Λάζος,2001)

1.3 Μορφές Ηλεκτρονικού Εγκλήματος

1.3.1 Εισαγωγή για Μορφές Ηλεκτρονικού Εγκλήματος

Στις μέρες μας το ηλεκτρονικό έγκλημα έχει εισχωρήσει με πολύ γρήγορους ρυθμούς στην δομή και οργάνωση των αναπτυγμένων κοινωνιών. Συνεχώς εμφανίζονται νέες μορφές και οι ήδη υπάρχουσες συνεχώς αναπτύσσονται και εξελίσσονται με πολύ γρήγορους ρυθμούς. Τα εγκλήματα που τελούνται με οποιαδήποτε συσκευή ηλεκτρονικής επεξεργασίας δεδομένων περιλαμβάνονται στο ηλεκτρονικό έγκλημα. Οι νέες τεχνολογίες και κυρίως οι ηλεκτρονικοί υπολογιστές και τα δίκτυα διεύρυναν σε μεγάλο βαθμό τα μέσα διάπραξης πολλών εγκλημάτων που περιλαμβάνονται ήδη στο κοινό Ποινικό Δίκαιο, πολύ πιο πριν από την εμφάνιση των συσκευών (που προαναφέρθηκαν) ηλεκτρονικής επεξεργασίας δεδομένων.

Δύο είναι οι βασικές κατηγορίες με τις οποίες μπορούμε να καταγράψουμε και να αναλύσουμε τις βασικότερες μορφές ηλεκτρονικού εγκλήματος:

- Αρχικά διακρίνουμε τα εγκλήματα που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και των δικτύων, τα οποία τα χαρακτηρίζουμε ως «γνήσια».
- Επιπλέον διακρίνουμε τα εγκλήματα τα οποία προϋπήρχαν και πριν την εμφάνιση ηλεκτρονικών υπολογιστών, τα οποία όμως τελούνται με τη βοήθεια ή τη χρήση των ηλεκτρονικών υπολογιστών και των δικτύων.

(http://www.goonline.gr/ebusiness/specials/article.html?article_id=341)

Υπάρχουν πολλές μορφές ηλεκτρονικού εγκλήματος. Πιο αναλυτικά θα αναφερθούμε στη συνέχεια στις κυριότερες μορφές ηλεκτρονικού εγκλήματος οι οποίες είναι:

- Απάτη στο διαδίκτυο
- Κλοπή ταυτότητας
- Ξέπλυμα χρήματος
- Διακίνηση πορνογραφικού υλικού

- Διαδικτυακή τρομοκρατία
- Επιθέσεις παρενόχλησης (Βλαχόπουλος,2007)

Στις υπόλοιπες μορφές ηλεκτρονικού εγκλήματος θα αναφερθούμε επιφανειακά ενημερώνοντας κυρίως για την ύπαρξη τους, χωρίς να δώσουμε βάση στην ανάλυσή τους. (Βλαχόπουλος,2007)

1.3.2 Εγκλήματα που τελούνται με τη χρήση Ηλεκτρονικού Υπολογιστή

Στο κοινό Ποινικό Δίκαιο υπάρχουν εγκλήματα τα οποία ως βασική προϋπόθεση της τέλεσής τους χρειάζονται την χρήση ηλεκτρονικού υπολογιστή, ο οποίος μπορεί να χρησιμοποιηθεί ποικιλοτρόπως για την τέλεση των εγκλημάτων αυτών:

- Στην αποθήκευση δεδομένων που αφορούν πρόσωπα και αντικείμενα που εμπλέκονται σε παράνομη δραστηριότητα, π.χ προσωπικά στοιχεία εμπόρων όπλων.
- Στην εύρεση πληροφοριών που αφορούν παράνομη δραστηριότητα, π.χ. κατασκευή βόμβας.
- Στην διάδοση πληροφοριών, π.χ συκοφαντικές πληροφορίες για ένα προϊόν ή εταιρία.
- Στην τέλεση μέρους της εγκληματικής πράξης, π.χ. αγορά αγαθών με χρήση πιστωτικής κάρτας που έχει κλαπεί με φυσικό τρόπο
- Στη διακίνηση παράνομου οπτικοακουστικού υλικού, π.χ. παιδική πορνογραφία. (Βλαχόπουλος,2007)

1.3.3 Μορφές Ηλεκτρονικού Εγκλήματος

1.3.3.1 Απάτη στο Διαδίκτυο

Στον κόσμο του διαδικτύου είναι ένα σύνηθες φαινόμενο αυτού του είδους τα εγκλήματα. Η ανάπτυξη του Διαδικτύου μεγάλωσε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η εξάπλωση του ηλεκτρονικού εμπορίου που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου βοήθησε στην αύξηση αυτών των νέων μορφών απάτης με χρήση διαδικτύου. (Βλαχόπουλος, 2007)

Κυριότερες μορφές απάτης μέσω Διαδικτύου:

Απάτη με e-mail: Πρόκειται για την πιο συχνή μορφή επιθέσεως, έναντι των χρηστών του διαδικτύου. Οι επαγγελματίες του είδους για να εξαπατήσουν τους ανυποψίαστους χρήστες , χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail), προβάλλουν διάφορες δικαιολογίες για να αποσπάσουν χρηματικά ποσά ή προσωπικά στοιχεία. Οι πιο συχνές μορφές απάτης με e-mail είναι:

• Phishing

• Pharming

• Spam

• Scam

• Blog

• Διαδικτυακός τζόγος

- **Phishing**

Τρόπος δράσης : Ένα e-mail φτάνει στο υποψήφιο θύμα, π.χ από την υπηρεσία Ηλεκτρονικής Τραπεζικής της τράπεζας που χρησιμοποιεί, όπου τον ενημερώνει ότι πραγματοποιούνται κάποιες εργασίες συντήρησης του συστήματος και τον προτρέπει να επισκεφτεί την υπηρεσία Ηλεκτρονικής Τραπεζικής επιλέγοντας τον σύνδεσμο, που ο δράστης έχει επισυνάψει στο μήνυμα και να επιβεβαιώσει τους κωδικούς πρόσβασης της υπηρεσίας. Το ανυποψίαστο θύμα εφόσον επιλέξει τον σύνδεσμο , θα τον οδηγήσει σε μία τοποθεσία-αντίγραφο της πραγματικής (mirror), όπου όταν πληκτρολογήσει τα προσωπικά του στοιχεία αυτά θα υποκλαπούν από τον επιτιθέμενο (hacker). (Βλαχόπουλος,2007)

Το "Ψάρεμα" είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων. Το "Phishing" είναι ένας τύπος εξαπάτησης που έχει σχεδιαστεί για την κλοπή της ταυτότητάς των

ανυποψίαστων χρηστών. Οι επιτήδειοι της ηλεκτρονικής απάτης πλησιάζουν τους χρήστες- θύματα με ψεύτικα προσχήματα και προσπαθούν να τους πείσουν να κοινοποιήσουν σημαντικές προσωπικές πληροφορίες όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή δεδομένα του λογαριασμού τους. Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου ενώ διακινούνται μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων που εμφανίζονται χωρίς να το επιλέξει ο χρήστης με την μορφή επιπρόσθετων παραθύρων στο ήδη ανοιχτό παράθυρο το οποίο επέλεξε ο χρήστης- θύμα (pop up windows, Instant messaging). Επομένως οι χρήστες πρέπει να είναι πολύ προσεχτικοί στην χρήση αυτών των αναδυόμενων παραθύρων διότι δεν είναι ασφαλές να εισάγουν προσωπικές ή οικονομικές πληροφορίες στα συγκεκριμένα παράθυρα. Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου όταν κάποιος κάνει κλικ σε ένα ηλεκτρονικό μήνυμα ψαρέματος. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεται ο χρήστης. Ακόμη και εάν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγεται η εισαγωγή ευαίσθητων προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελεγχτεί η πιστοποίηση ασφάλειας. Ενδείξεις όπου ένα ηλεκτρονικό μήνυμα πιθανόν να είναι πλαστό είναι πολλές φορές οι γενικές προσφωνήσεις όπως "Αγαπητέ πελάτη" αντί για το όνομά του χρήστη. Ζητούν από τον χρήστη να κάνει κλικ σε κάποιο σύνδεσμο, με φρασεολογία που δίνει την εντύπωση του επείγοντος ή του ζητούν να επιβεβαιώσει κάποιες προσωπικές του πληροφορίες. (http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

Μια παραλλαγή των επιθέσεων phishing αποτελούν οι επιθέσεις Pharming

Απάτη με Pharming (παραπλάνηση): Ο σκοπός του εγκλήματος είναι και εδώ ο ίδιος με τις επιθέσεις phishing, η απόσπαση ευαίσθητων δεδομένων από το θύμα. Η διαφορά εντοπίζεται στην τεχνική η οποία χρησιμοποιείται κάθε φορά από έναν hacker. Ο hacker επεμβαίνει στην προσωπική ηλεκτρονική διεύθυνση που εκπέμπει ο κάθε χρήστης όταν εισέρχεται στο διαδίκτυο(DNS) και όταν ο ανυποψίαστος χρήστης πληκτρολογήσει την διεύθυνση που χρησιμοποιεί χωρίς να το γνωρίζει μεταφέρεται σε άλλο δικτυακό τόπο (mirror), όπου ο κακόβουλος θα επιχειρήσει να αποσπάσει

το όνομα χρήστη και τον κωδικό πρόσβασης του θύματος χρησιμοποιώντας τον μετά ποικιλοτρόπως για προσωπική του χρήση. (Αργυρόπουλος ,2006)

- **pharming**

Κάποιος ο οποίος θέλει να παραπλανήσει το θύμα του, να κατευθύνει τον browser του σε κάποια άλλη ιστοσελίδα μπορεί να το πραγματοποιήσει τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS" κατά την οποία, όπως αναφέραμε παραπάνω, κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε στην ψεύτικη ιστοσελίδα πριν προλάβει να αποκτήσει το θύμα πρόσβαση σε αυτή που τελικά επιθυμούσε. Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό firewall (τείχος προστασίας) που χρησιμοποιούν προστατεύει και από την παραπλάνηση (pharming). Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις. Η φύση της παραπλάνησης υποδεικνύει όμως το αντίθετο αλλά, ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία, είναι καλή ιδέα να αναζητήσει ο χρήστης προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσει και εμπιστευτεί κάποιες λύσεις λογισμικού. Πολλές φορές δεν μπορούμε να αναγνωρίσουμε εάν μία ιστοσελίδα είναι ψεύτικη μετακινώντας μόνο το δείκτη πάνω από τα link και παρατηρώντας εάν ο κώδικας μας οδηγεί σε κάποιο εμφανώς άσχετο σημείο εκτός ιστοσελίδα. Διότι πολλές φορές οι ψεύτικες ιστοσελίδες που χρησιμοποιούνται στις απάτες παραπλάνησης συνήθως "πλαστογραφούν" τα link τους έτσι ώστε να μοιάζουν ακριβώς με αυτά που αναμέναμε να δούμε, ακόμη και στον κώδικα που εμφανίζεται όταν το ποντίκι περάσει πάνω από αυτά. Επίσης, οι ιστοσελίδες πιθανόν να αλλάζουν τον κώδικα των δικών τους links αρκετά συχνά και για διάφορους λόγους, όπως όταν αναβαθμίζουν το λογισμικό τους, την πλατφόρμα του διακομιστή τους ή τις μεθόδους ανάλυσης των στατιστικών κίνησης της ιστοσελίδαστους.(http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

- **Spam**

Μια άλλη μορφή απάτης στο διαδίκτυο είναι το Spam: Το e-mail spam είναι ανεπιθύμητο διαφημιστικό ηλεκτρονικό μήνυμα. Το spam είναι ενοχλητικό, γιατί πιθανόν να εμπεριέχει απάτη ή να μολύνει τον υπολογιστή σας με ιό ή άλλο κακόβουλο λογισμικό. Εάν ένας χρήστης λάβει ένα ηλεκτρονικό μήνυμα που πιθανόν να είναι ανεπιθύμητο, δεν θα πρέπει να απαντήσει σε αυτό, να κάνει κλικ ή να το προωθήσει. Εάν είναι δυνατόν θα πρέπει να το αναφέρει και να το διαγράψει χωρίς να το ανοίξει ή να κάνει κλικ σε κάποιο σύνδεσμο μέσα σε αυτό. Γιατί είναι ενοχλητικό ένα ηλεκτρονικό ανεπιθύμητο μήνυμα;

Μερικά βήματα που μπορείτε να ακολουθήσει ένας χρήστης ώστε να προστατευτεί από τα ανεπιθύμητα μηνύματα είναι τα ακόλουθα:

• Να μην δίνει σε οποιονδήποτε την ηλεκτρονική του διεύθυνση.

• Να χρησιμοποιεί ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων.

• Ποτέ μην ανοίγει τα συνημμένα των μηνυμάτων εκτός και αν γνωρίζετε περί τίνος πρόκειται.

• Να αναφέρει στις αρμόδιες αρχές τους αποστολείς των ανεπιθύμητων μηνυμάτων. (http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

- **Scam**

Το scam είναι επίσης μια ακόμη μορφή απάτης στο διαδίκτυο. Μέχρι πρόσφατα, οι επαγγελματίες απατεώνες περιορίστηκαν στη χρήση αργών και αναποτελεσματικών τηλεφωνημάτων και έντυπων αγγελιών για να προωθήσουν τις απάτες τους. Σήμερα, τα ίδια χαρακτηριστικά που κάνουν το Διαδίκτυο τόσο βολικό για όσους αναζητούν εργασία, δηλαδή η παγκοσμιότητα, η ευχρηστία και η ταχύτητα, διευκολύνουν τους εγκληματίες να επιδίδονται σε απάτες με θέμα την απασχόληση, διατρέχοντας μικρότερο κίνδυνο. Αυτό μπορεί να γίνει με δύο τρόπους.

- Αρχικά προσφέροντας στους χρήστες ψεύτικες ευκαιρίες απασχόλησης. Δημιουργώντας λοιπόν ψεύτικες αγγελίες θέσεων εργασίας που μοιάζουν με τις αληθινές και, συχνά, δημοσιεύοντάς τις σε νόμιμες ιστοσελίδες εύρεσης εργασίας, οι απατεώνες ελπίζουν να παραπλανήσουν τους πρόθυμους και ανυποψίαστους που αναζητούν εργασία και να τους πείσουν να στείλουν τα προσωπικά τους στοιχεία (το γνωστό ψάρεμα). Αυτές οι ψεύτικες αγγελίες εύρεσης εργασίας γίνονται όλο και πιο κομψές και, συχνά, χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία. Πολλές φορές, διαθέτουν και συνδέσμους προς πλαστές ιστοσελίδες που εμφανίζονται ως τοποθεσίες πραγματικών εταιρειών. Κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δεν θα παράσχουν ποτέ. Τυπικά, μετά από μερικές μέρες, οι κλέφτες κλείνουν το scam και εξαφανίζονται.
  (Βλαχόπουλος,2007)
- Ένας άλλος τρόπος απάτης στο διαδίκτυο με τη μορφή scam είναι τα παράνομα γραφεία ευρέσεως εργασίας. Ακόμα, εκτός από τη σάρωση προσωπικών ιστοσελίδων και τη δημοσίευση ανακοινώσεων σε δημόσιες ιστοσελίδες, οι επαγγελματίες απατεώνες συχνά εμφανίζονται ως γραφεία ευρέσεως εργασίας που διαθέτουν ευκαιρίες απασχόλησης και στέλνουν ανεπιθύμητη αλληλογραφία (ή spam) σε πιθανούς υποψηφίους ή νόμιμα γραφεία ευρέσεως εργασίας. Ένας επαγγελματίας δράστης τέτοιου είδους θα προσπαθήσει να κερδίσει την εμπιστοσύνη του θύματος, χρησιμοποιώντας ψεύτικο προσωπικό για να αποσπάσει προσωπικά στοιχεία, ακόμη και από το τηλέφωνο. Είναι σημαντικό να γνωρίζουν οι ενδιαφερόμενοι πως τέτοια στοιχεία θα τους ζητηθούν μόνον σε προσωπική συνέντευξη.

(http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

- **Blog**

Μια ακόμη πολύ συνηθισμένη μορφή απάτης με e-mail είναι η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, η οποία

μεγαλώνει δραματικά ειδικά ανάμεσα στους έφηβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους. Σύμφωνα με κάποιες πρόσφατες μελέτες έδειξαν πως τα μισά από τα ημερολόγια blog σήμερα δημιουργούνται από εφήβους με δύο στους τρεις να δημοσιοποιούν την ηλικία τους, τρεις στους πέντε να αποκαλύπτουν την τοποθεσία τους και έναν στους πέντε να αποκαλύπτει το πλήρες όνομα του. Αυτό συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών λεπτομερειών. Και καθώς πολλά νεαρά παιδιά δημιουργούν όλο και περισσότερα ημερολόγια blog, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή. Μερικές φορές αυτό μπορεί να οδηγήσει τα παιδιά να δημοσιεύσουν ακατάλληλο υλικό όπως προκλητικές εικόνες των εαυτών τους ή των φίλων τους. Αν και η διατήρηση ενός ημερολογίου blog προσφέρει πιθανά οφέλη, όπως την βελτίωση των ικανοτήτων στη γραφή και στην επικοινωνία, είναι σημαντικό να εκπαιδευτούν οι χρήστες των blog και ιδιαίτερα οι ανήλικοι χρήστες σχετικά με το Διαδίκτυο και τη δημιουργία ημερολογίων πριν ακόμη ξεκινήσουν. (http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

- **Διαδικτυακός τζόγος**

Τέλος ο δικτυακός τζόγος είναι μια πολύ διαδεδομένη μορφή απάτης στο Διαδίκτυο όπου οι χρήστες, και ιδιαίτερα τα παιδιά, απολαμβάνουν να χρησιμοποιούν το Internet για να ανακαλύπτουν δραστηριότητες ψυχαγωγίας, όπως τα διαδικτυακά παιχνίδια. Πολλές φορές όμως , ενώ αναζητούν μια νέα ιστοσελίδα με παιχνίδια μπορεί να βρουν ιστοσελίδες με στοιχήματα και τυχερά παιχνίδια. Ενώ η χρήση των περισσότερων παιχνιδιών και δραστηριοτήτων από ανηλίκους είναι νόμιμη, η χρήση των τυχερών παιχνιδιών δεν είναι.

(http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

Είτε είναι νόμιμα λοιπόν είτε όχι τα τυχερά παιχνίδια στο διαδίκτυο ελκύουν συγκεκριμένες κατηγορίες ατόμων. Σύμφωνα με μια μελέτη, τα άτομα τα οποία επισκέπτονται τα παραδοσιακά καζίνα είναι πολύ πιο πιθανό να συμμετάσχουν σε online τυχερά παιχνίδια από ότι τα άτομα τα οποία δεν επισκέπτονται τα παραδοσιακά καζίνα. Τα άτομα τα οποία έχουν δοκιμάσει την τύχη τους στα τυχερά παιχνίδια του διαδικτύου είναι πιθανό να συνεχίσουν να συμμετάσχουν σε αυτά απορρίπτοντας τα παραδοσιακά καζίνα. Συγκρίνοντας του παίχτες που παίζουν στα παραδοσιακά καζίνα με τους παίχτες που παίζουν στα τυχερά παιχνίδια του διαδικτύου, αυτοί που ανήκουν στην δεύτερη κατηγορία συνήθως είναι άτομα μικρότερης ηλικίας, που τους αρέσει να δοκιμάζουν καινούρια πράγματα, με υψηλότερο μορφωτικό επίπεδο και είναι πρόθυμοι να ποντάρουν online. Μια άλλη μελέτη επικεντρώνεται περισσότερο σε μια άλλη διαφορά μεταξύ των online παιχτών και των παιχτών των παραδοσιακών καζίνων, διαπιστώνοντας ότι οι online παίχτες είναι οικονομικά πιο ευσταθείς. Είναι πιο πιθανό να σταματήσουν να παίζουν, αν τους τελειώσουν τα χρήματα που αρχικά είχαν αποφασίσει να χρησιμοποιήσουν. αλλά οι παραδοσιακοί παίχτες είναι πιο πιθανό να συνεχίσουν να παίζουν όταν τους τελειώσουν τα χρήματα ακόμη και αν χρειαστεί να δανειστούν χρήματα για να μπορέσουν να συνεχίσουν να παίζουν. Τέλος ο τζόγος στο διαδίκτυο μπορεί να είναι πιο εθιστικός, καθώς είναι ένας εύκολος, διασκεδαστικός , μοναχικός και ανώνυμος τρόπος για να παίξει κάποιος τυχερά παιχνίδια. (Thio,2008)

Διαφορά ανάμεσα στις τοποθεσίες παιχνιδιών και τις τοποθεσίες τυχερών παιχνιδιών

Οι κυριότερες διαφορές μεταξύ αυτών των δύο τύπων ιστοσελίδων είναι οι εξής:

• Οι τοποθεσίες παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή πάζλ, με αυτόματη παρακολούθηση και προβολή του σκορ.

• Δεν γίνεται ανταλλαγή χρημάτων, αληθινών ή ψεύτικων. Οι τοποθεσίες τυχερών παιχνιδιών μπορούν να περιέχουν σενάρια, στα οποία οι άνθρωποι

κερδίζουν ή χάνουν κάποιο τεχνητό νόμισμα. Οι τοποθεσίες Τζόγου συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

πηγή Microsoft(http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf)

- **Παιχνιδομηχανές**

Μία άλλη μορφή ηλεκτρονικού εγκλήματος παρόμοια με αυτή του δικτυακού τζόγου είναι οι παιχνιδομηχανές. Οι σύγχρονες παιχνιδομηχανές (Play Station 2, XBOX και ιδιαίτερα οι καινούριες PSP) εκδηλώνουν ιδιαίτερο ενδιαφέρον για τις διωκτικές αρχές . Η ενσωμάτωση σε αυτές της τεχνολογίας WiFi (ασύρματη πρόσβαση) και εξελιγμένων δυνατοτήτων επεξεργασίας δεδομένων, σε συνδυασμό με τη χρήση ειδικών προγραμμάτων, επιτρέπουν να χρησιμοποιηθούν για hacking ή απομακρυσμένη διαχείριση υπολογιστή. Παρόμοιες δυνατότητες φέρουν και οι υπολογιστές, που προορίζονται για χρήση σε αυτοκίνητα. (Αργυρόπουλος ,2006)

1.3.3.2Απάτη με Πιστωτικές Κάρτες

Η χρήση πιστωτικών καρτών στο Διαδίκτυο, για τη διεκπεραίωση πάσης φύσης συναλλαγών που πραγματοποιούν οι χρήστες του Διαδικτύου, έχει δημιουργήσει νέες δυνατότητες για τη διάπραξη εγκλημάτων. Η άγνωστη ταυτότητα του πωλητή- δράστη και η μη αυτοπρόσωπη παρουσία του αγοραστή- θύμα έχουν συμβάλει στην αύξηση των περιπτώσεων απάτης, με τη χρήση πιστωτικών καρτών στο Διαδίκτυο. Με τη χρήση των σύγχρονων τεχνολογιών είναι πλέον πολύ εύκολο να αποκτήσει κάποιος τον αριθμό μιας πιστωτικής κάρτας και να πραγματοποιήσει αγορές μέσω Διαδικτύου. Με την τεχνολογία «websniffer», παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα οι δεκαεξαψήφιοι αριθμοί των πιστωτικών καρτών. Επιπλέον, είναι δυνατή η αγορά μέσω Διαδικτύου , αριθμών πιστωτικών καρτών που έχουν υποκλαπεί. Τέλος, υπάρχουν και εφαρμογές λογισμικού που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών, χρησιμοποιώντας διάφορους λογάριθμους. (Βλαχόπουλος,2007)

1.3.3.3 Κλοπή Ταυτότητας

Ένα από τα πλέον σοβαρότερα εγκλήματα του Διαδικτύου είναι η κλοπή ταυτότητας. Στην εποχή που διανύουμε τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς. Είναι εύκολο λοιπόν για κάποιον που το επιθυμεί να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την πραγματοποίηση πάσης φύσεως συναλλαγών. (Βλαχόπουλος,2007)

Πιο συγκεκριμένα κλοπή ταυτότητας στο Διαδίκτυο ονομάζεται η πρακτική του να χρησιμοποιεί κανείς την εικονική ταυτότητα ενός άλλου ατόμου, χρησιμοποιώντας το όνομα χρήσης και τον κωδικό πρόσβασής του σε διάφορες διαδικτυακές υπηρεσίες. Σκοπός όσων επιχειρούν κλοπή ταυτότητας μπορεί να είναι η οικονομική εξαπάτηση, αλλά και ο εξευτελισμός ή η διάδοση φημών για ένα άτομο στο διαδικτυακό του περιβάλλον. Οι συνέπειες και φυσικά οι εκπλήξεις με τις οποίες μπορεί κανείς να έρθει αντιμέτωπος είναι πολλαπλές. Μπορεί κανείς να συναντήσει μηνύματα που στέλνονται εξ ονόματός του, σχόλια σε blog και forum. Σε ότι αφορά στους νέους, η κλοπή ταυτότητας τις περισσότερες φορές πραγματοποιείται κατά κύριο λόγο στις υπηρεσίες κοινωνικής δικτύωσης και γενικά στις εφαρμογές και τα εικονικά περιβάλλοντα στα οποία επικοινωνούν με τους ηλεκτρονικούς τους φίλους. (http://www.fititis.gr/fititis2/index.php?option=com_content&task=view&id=3392&Itemid=11)

Μια πρόσφατη έρευνα από Javelin Strategy & Έρευνας του Pleasanton ανέφερε ότι η απάτη ταυτότητας, ως ποσοστό του πληθυσμού των Ηνωμένων Πολιτειών ενηλίκων μειώθηκε σε 4 τοις εκατό μεταξύ 2003 και 2006. Επιπλέον, η έκθεση υποστηρίζει επίσης ότι το 90 τοις εκατό αυτής κλοπή ταυτότητας γίνεται μέσω των παραδοσιακών καναλιών χωρίς σύνδεση και δεν μέσω του Διαδικτύου. (http://translate.google.gr/translate?hl=el&langpair=en%7Cel&u=http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp)

Υπάρχουν δύο στάδια για την ολοκλήρωση του εγκλήματος της κλοπής της ταυτότητας.

- Ø Στο πρώτο στάδιο, ο επιτιθέμενος προσπαθεί με διάφορους τρόπους να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου, από:
- ü Κλοπές πορτοφολιών- τσαντών
- ü Από το ταχυδρομείο του θύματος (δηλώσεις τραπεζών και πιστωτικών καρτών, προ-εγκεκριμένες προσφορές πιστωτικών καρτών, τηλεφωνικές τηλεπικοινωνιακές κάρτες και φορολογικές πληροφορίες),
- ü Κλοπές προσωπικών πληροφοριών που δίνει το θύμα σε μη ασφαλισμένη ιστοσελίδα στο Ιντερνέτ,
- ü Από τα αρχεία επιχειρήσεων ή προσωπικού στην εργασία,
- ü Ψάχνοντας στα σκουπίδια για προσωπικά δεδομένα,
- ü Παριστάνοντας ότι είναι κάποιος που χρειάζεται νόμιμα τις πληροφορίες για το θύμα, όπως κάποιος εργοδότης ή σπιτονοικοκύρης, ή
- ü Αγοράζουν προσωπικές πληροφορίες από «εσωτερικές» πηγές. Για παράδειγμα, ένας κλέφτης ταυτότητας μπορεί να πληρώσει κάποιον υπάλληλο του καταστήματος για να του δώσει πληροφορίες για το θύμα που υπάρχουν σε αίτησή του για αγορά αγαθών, υπηρεσιών, ή πίστωσης.(http://retirement.gov/multilanguage/Greek/10064-GR.pdf)
- Ø Το επόμενο βήμα του επιτιθέμενου είναι να χρησιμοποιήσει τα κλεμμένα στοιχεία προς όφελος του. Αυτό μπορεί να γίνει:
- ü Ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, οι οποίοι θα χρησιμοποιηθούν για αγορές μέσω του διαδικτύου.
- ü Ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους θα χρεώσει με ακάλυπτες επιταγές.
- ü Δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος,

- Υποβάλλοντας ψευδής φορολογικές δηλώσεις (και μέσω διαδικτύου), εισπράττοντας την επιστροφή φόρου. (http://retirement.gov/multilanguage/Greek/10064-GR.pdf)

1.3.3.4 Ξέπλυμα Χρήματος

ΤΙ ΕΙΝΑΙ ΓΕΝΙΚΑ ΤΟ ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΩΝ

Το ξέπλυμα χρήματος περιγράφεται ως "συμπεριφορά ή ενέργεια σχεδιασμένη γενικά ή εν μέρει για να κρύψει ή να μεταμφιέσει τη φύση, τη θέση, την πηγή, την ιδιοκτησία ή τον έλεγχο των χρημάτων (μπορεί να είναι νόμισμα ή ισοδύναμα, π.χ. επιταγές ηλεκτρονικές συναλλαγές κ.τ.λ.) για να αποφύγει μια απαίτηση για την υποβολή εκθέσεων συναλλαγής από το κράτος ή τον ομοσπονδιακό νόμο ή για να παραποιήσει το γεγονός ότι τα χρήματα αποκτήθηκαν με παράνομα μέσα". Το ξέπλυμα χρημάτων περιλαμβάνει το κρύψιμο, τη διακίνηση, και την επένδυση των εισπράξεων της εγκληματικής συμπεριφοράς. Ακόμη και τα νόμιμα χρήματα μπορούν να γίνουν παράνομα, παραδείγματος χάριν, εάν διακινούμενα παραβιάζουν τους ελέγχους ξένου συναλλάγματος μιας χώρας ή άλλους οικονομικούς κανονισμούς. Τα καθαρά χρήματα μπορούν επίσης να παράγουν τα βρώμικα χρήματα μέσω της φορολογικής διαφυγής. . (Λάζος,2001)

ΣΤΑΔΙΑ ΓΙΑ ΤΗΝ ΟΛΟΚΛΗΡΩΣΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΓΙΑ ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

- Επιχειρείται η μετατροπή των χρημάτων, που προέρχονται από παράνομες δραστηριότητες, σε μια νέα μορφή η οποία θα είναι λιγότερο ύποπτη από τις διωκτικές αρχές. Τα χρήματα που προέρχονται από παράνομες δραστηριότητες μοιράζονται σε ιδρύματα ή διοχετεύονται στο λιανεμπόριο. (Λάζος,2001)
- Έπειτα, μέσα από πολλαπλές οικονομικές συναλλαγές επιχειρείται ο διαχωρισμός του χρήματος από την πρωταρχική του παράνομη πηγή. (Λάζος,2001)

- Τέλος η διαδικασία ολοκληρώνεται όταν το παράνομο χρήμα πάρει την μορφή εισοδήματος το οποίο θα φαίνεται ότι έχει προέλθει από νόμιμες επαγγελματικές δραστηριότητες. (Λάζος,2001)

ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η κοινή παρατήρηση ότι το Διαδίκτυο παρέχει νέες και μη ανιχνεύσιμες μεθόδους ξεπλύματος χρημάτων δεν έχει καμία θέση στη σοβαρή εκτίμηση κοινών σημείων μεταξύ του ξεπλύματος χρημάτων και της τεχνολογίας. Εξάλλου, δεν υπάρχει άμεση αντιστοιχία ή ευθεία σχέση αιτίου (τεχνολογία) - αποτελέσματος (έγκλημα) μεταξύ τους. Στην ουσία, το Διαδίκτυο δεν είναι τίποτα περισσότερο από ένα σύστημα μηνυμάτων. Για να διακινηθούν τα χρήματα, οι τράπεζες διακινούν τις πληροφορίες μέσω οποιουδήποτε διαθέσιμου συστήματος μηνυμάτων κινώντας πλάκες χρυσού από μια θέση σε άλλη κατά τη διεξαγωγή ελέγχων. Σε αυτό το πλαίσιο, το Διαδίκτυο είναι απλά ένα ενημερωμένο σύστημα ελέγχου ή ένας αποδοτικότερος, φτηνότερος και ασφαλέστερος τρόπος διακίνησης οικονομικών πληροφοριών. Ο προσδιορισμός των πελατών είναι το αρχικό πρόβλημα που προκύπτει από τη χρήση Διαδικτύου, και εκείνο το πρόβλημα είναι ακριβώς το ίδιο με οποιαδήποτε σχέση που διεξάγεται από απόσταση. Παρόλα αυτά , μερικοί χρησιμοποιούν το ξέπλυμα χρημάτων μέσω Διαδικτύου ως δικαιολογία για να κινηθούν προς πιο εκτενείς ρυθμίσεις του Διαδικτύου. Ακόμα κι αν ήταν δυνατό να δημιουργηθεί ο αποτελεσματικός κανονισμός του Διαδικτύου μια τέτοια επιχείρηση θα μεγάλωνε τα εμπόδια για την είσοδο των φτωχών εθνών. Το Διαδίκτυο μπορεί να ωφελήσει μεγάλα μέρη του κόσμου με χαμηλότερο κόστος με τη μείωση της απομόνωσης και παρέχοντας στις μακρινές κοινότητες τη δυνατότητα να παρέχουν υπηρεσίες και να δημοσιεύουν καταλόγους τοπικών αγαθών. Αυστηρότερος κανονισμός θα επιδεινώνει μόνο “ψηφιακή διαίρεση“ μεταξύ των πλουσίων και αναπτυσσόμενων οικονομιών. Οι τράπεζες αποτελούν την πρωταρχική ανησυχία όσον αφορά αυτή την εγκληματική δραστηριότητα αλλά εξαιτίας του ότι όλο και περισσότερες τράπεζες και χρηματοδοτικοί οργανισμοί προσφέρουν τις υπηρεσίες τους

στο Διαδίκτυο ή μέσω κάποιας μορφής ηλεκτρονικού μέσου, η τεχνολογία που χρησιμοποιείται για να προσδιορίσει και να επικυρώσει τους πελάτες μπορεί να παραβιαστεί ακριβώς όπως οποιαδήποτε βασισμένη στο Διαδίκτυο ασφάλεια. (Βλαχόπουλος,2007)

ΠΡΑΞΕΙΣ ΠΟΥ ΣΥΝΙΣΤΟΥΝ ΞΕΠΛΥΜΑ ΒΡΩΜΙΚΟΥ ΧΡΗΜΑΤΟΣ ΓΕΝΙΚΑ

Ανακεφαλαιώνοντας λοιπόν, σκόπιμο είναι να παρουσιαστούν συγκεντρωτικά όλες εκείνες οι πράξεις που διώκονται ποινικά και αποτελούν ξέπλυμα βρώμικου χρήματος. Περίπου είκοσι είναι λοιπόν οι εγκληματικές δραστηριότητες που εμπίπτουν στις αυστηρές διατάξεις της νομοθεσίας περί ξεπλύματος μαύρου χρήματος, καθώς στις 19 που προέβλεπε ο νόμος, προστέθηκαν και οι σοβαρές φορολογικές παραβάσεις και η μη απόδοση στα ταμεία ασφαλιστικών εισφορών, εφόσον το ποσό υπερβαίνει τις 150.000 ευρώ.(www.banksafeonline.org.uk)

1. Η εγκληματική οργάνωση

2. Οι τρομοκρατικές πράξεις

3. Η χρηματοδότηση της τρομοκρατίας

4. Η παθητική δωροδοκία

5. Η εμπορία ανθρώπων

6. Η απάτη με υπολογιστή

7. Η σωματεμπορία

8. Η εμπορία ναρκωτικών

9. Η εμπορία όπλων, πυρομαχικών, εκρηκτικών υλών κ.τ.λ.

10. Εμπορία αρχαιοτήτων (αρχαιοκαπηλία)

11. Παράβαση της νομοθεσίας περί προστασίας εξ ιοντοζουσών ακτινοβολιών

12. Παράβαση της νομοθεσίας για την είσοδο και παραμονή αλλοδαπών στην Ελληνική επικράτεια.

13. Παράβαση της νομοθεσίας για την προστασία των οικονομικών συμφερόντων των Ευρωπαϊκών Κοινοτήτων

14. Η δωροδοκία αλλοδαπού δημοσίου λειτουργού

15. Η δωροδοκία υπαλλήλων των Ευρωπαϊκών Κοινοτήτων ή των κρατών-μελών της Ευρωπαϊκής Ένωσης

16. Η κατάχρηση αγοράς, είτε συντελείται με κατάχρηση προνομιακής πληροφορίας είτε με χειραγώγηση της αγοράς.

17. Κάθε πράξη σε βαθμό κακουργήματος, εφόσον από την τέλεσή της προέκυψε περιουσία αξίας τουλάχιστον 4.000 ευρώ 18. Κάθε πράξη σε βαθμό πλημμελήματος, εφόσον τιμωρείται με ποινή φυλάκισης τουλάχιστον τριών (3) μηνών και από την τέλεση της προέκυψε περιουσία αξίας τουλάχιστον 4.000 ευρώ

19. Η φοροδιαφυγή πάνω από 150.000 ευρώ

20. Οι οφειλές προς Ταμεία πάνω των 150.000 ευρώ (www.banksafeonline.org.uk)

1.3.3.5 Διακίνηση Πορνογραφικού Υλικού

ΕΙΣΑΓΩΓΗ

Παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς(Βλαχόπουλος,2007)

Πορνογραφικό υλικό συνιστά κάθε περιγραφή είτε πραγματική είτε εικονική, σε οποιοδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση σε οποιοδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο(Βλαχόπουλος,2007)

Η παιδική εκμετάλλευση δεν είναι ένα νέο έγκλημα, υπήρξε από τα αρχαία, ακόμα, χρόνια ενώ τα δίκτυα παραβατών που επικοινωνούσαν πριν την ανακάλυψη των προσωπικών υπολογιστών και του Διαδικτύου ήταν μέρος της καθημερινής ζωής αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης των ανηλίκων. Πριν το 1995, κάποιος ο οποίος θα επιδίωκε τη σεξουαλική επαφή με ένα παιδί, είτε θα γινόταν ιερέας, δάσκαλος, κλόουν, πατέρας, θείος, οδηγός λεωφορείων ή θα κρυβόταν γύρω από τη παιδική χαρά της γειτονιάς. Πριν από την ευρεία χρήση του Διαδικτύου, η ταχυδρομική υπηρεσία ήταν ο αρχικός τρόπος διανομής του υλικού της παιδικής πορνογραφίας ενώ το κόστος και ο κίνδυνος ήταν συνυφασμένος με αυτή αφού το παράνομο υλικό διατίθεντο σε περιορισμένη ποσότητα και πωλούταν σε ιδιαίτερη υψηλή τιμή. Πριν από τη χρήση του διαδικτύου, οι παιδόφιλοι επικοινωνούσαν με τα υποψήφια θύματα τους είτε μέσω του ερασιτεχνικού ραδιοφώνου είτε μέσω οργανώσεων που επικοινωνούσαν μεταξύ τους και προσέφεραν διάφορες υπηρεσίες στα μέλη τους, π.χ. ενίσχυση για τους παιδόφιλους και μια σταθερή πηγή για νέες φιλίες και ανεφοδιασμό νέων θυμάτων. Μια τέτοια οργάνωση ήταν και η Childhood Sensuality Circle – CSC. (Βλαχόπουλος,2007)

ΔΙΑΚΙΝΗΣΗ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Η πορνογραφία στο διαδίκτυο , ή κυβερνοπορνογραφία, δεν είναι καινούριο φαινόμενο. Η είσοδος και η ευρεία χρήση του διαδικτύου , παρέχει πλέον στους θύτες ένα νέο τόπο συναντήσεως για την εκμετάλλευση παιδιών, μειώνοντας τα αντικίνητρα με την παροχή ανωνυμίας και διευκολύνοντας την ανάπτυξη της φαντασίας δίνοντας στους θύτες ευκολότερη πρόσβαση σε ομάδες ομοϊδεατών περιορίζοντας την αίσθηση της περιθωριοποίησης. Έτσι λοιπόν, με την χρήση του διαδικτύου από τους θύτες και από τα θύματα αυξάνονται και οι τρόποι επικοινωνίας μεταξύ θύτη και θύματος καθώς και θύτη με κάποιον άλλο θύτη, διευκολύνοντας ακόμη περισσότερο την διανομή παιδικού πορνογραφικού υλικού μέσα από:

- Τα δωμάτια Συνομιλίας
- Στιγμιαίο Μήνυμα (IM)
- Το ηλεκτρονικό ταχυδρομείο (e-mail)
- Τις ηλεκτρονικές ομάδες (e-groups)
- Τους κατάλογους ηλεκτρονικών διευθύνσεων
- Τις ομάδες πληροφόρησης
- Τους πίνακες δελτίων (BBS)

(Βλαχόπουλος,2007)

Το πορνογραφικό υλικό που διακινείται μέσω του διαδικτύου μπορεί να έχει τη μορφή φωτογραφίας, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσου. Ο καθένας εύκολα μπορεί να έχει πρόσβαση σε αυτά χωρίς να χρειαστεί να αποκαλύψει την ταυτότητά του. Η εύρεση αυτού του υλικού βρίσκεται σε διάφορους δικτυακούς τόπους. (Βλαχόπουλος,2007)

Στατιστικές μελέτες έχουν καταδείξει ότι η διακίνηση πορνογραφικού υλικού μέσω διαδικτύου, αποτελεί πλέον μία από τις πιο συχνές μορφές εγκλήματος. Πιο συγκεκριμένα έχουν καταγραφεί:

- Δικτυακοί τόποι με πορνογραφικό υλικό 4,2 εκατομμύρια
- Σελίδες με πορνογραφικό υλικό 372 εκατομμύρια
- Αιτήματα για πορνογραφικό υλικό 68 εκατομμύρια

σε μηχανές αναζήτησης (ανά ημέρα)

25% του συνόλου

- E-mail με πορνογραφικό περιεχόμενο 4,5 ανά χρήστη
- Δικτυακοί τόποι που προσφέρουν

  παιδική πορνογραφία 100 χιλιάδες

- Μέσος όρος ηλικίας πρώτης επαφής

  με την πορνογραφία 11 ετών

- Μεγαλύτερη κατανάλωση πορνογραφίας 12-17 ετών
- Ποσοστό παιδιών ηλικίας 7-17 ετών που δίνουν ελεύθερα την δ/νση κατοικίας τους 20%
- Σεξουαλική παρενόχληση νέων σε δωμάτια συζητήσεων 89%

(Βλαχόπουλος,2007)

1.3.3.6 Δικτυακή Τρομοκρατία

Πολλές τρομοκρατικές δραστηριότητες σχεδιάζονται και εκτελούνται μέσα από το διαδίκτυο. Είναι ένα φαινόμενο που παρουσιάζει ιδιαίτερη έξαρση τα τελευταία χρόνια. Στο πέρασμα του χρόνου έχουν καταγραφεί αιματηρές τρομοκρατικές επιθέσεις με χιλιάδες θύματα. Η χρήση του διαδικτύου αποτελεί βασικό εργαλείο των τρομοκρατών, γιατί τους προσφέρει μια σειρά από πλεονεκτήματα. Βασικά είναι φθηνότερο από τις παραδοσιακές τρομοκρατικές μεθόδους, οι ενέργειες τους είναι δύσκολο να εντοπιστούν, μπορούν να αποκρύψουν την τοποθεσία τους, δεν υπάρχουν φυσικά εμπόδια ή σημεία ελέγχου τα οποία πρέπει να διέλθουν, μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και μπορούν να επιτεθούν, ταυτόχρονα, σε πολλούς στόχους. (Βλαχόπουλος,2007)

Η μεγαλύτερη τρομοκρατική απειλή παγκοσμίως, θεωρείται η οργάνωση Al-Kaida. Προκειμένου να σχεδιαστούν και να εκτελέσουν τις τρομοκρατικές τους δραστηριότητες , τα μέλη της τρομοκρατικής οργάνωσης Al-Kaida χρησιμοποιούν το διαδίκτυο για την μεταξύ τους

επικοινωνία. Η διαδικασία που χρησιμοποιούν για την μεταξύ τους επικοινωνία είναι πολύ απλή και γρήγορη: Ορισμένα μηνύματα αναρτώνται κωδικοποιημένα μέσω του διαδικτύου σε διάφορες ιστοσελίδες. Άλλα μηνύματα μεταδίδονται ηλεκτρονικά. Μετά από την αποστολή και την ανάγνωση αυτών των μηνυμάτων από τον παραλήπτη, ολόκληρη η επικοινωνία και τα αντίστοιχα αρχεία διαγράφονται, προκειμένου να προφυλαχτεί η μυστικότητα. Να σημειωθεί ότι για λόγους ασφαλείας και ανωνυμίας των αποστολέων και των παραληπτών, οι διευθύνσεις των ηλεκτρονικών ταχυδρομείων χρησιμοποιούνται συνήθως μόνο μία ή δύο φορές. (Βλαχόπουλος,2007)

Συμπερασματικά, διαπιστώνουμε πως στο σημερινό κόσμο που κυβερνάται από τους ηλεκτρονικούς υπολογιστές, οι τρομοκράτες δε χρειάζεται να παραβιάσουν τα εδάφη ή τον εναέριο χώρο μίας χώρας προκειμένου να βλάψουν τους πόρους τους και να διαλύσουν τις ζωές των πολιτών τους. Αυτό μπορεί να επιτευχτεί ευκολότερα για τους λόγους που προαναφέραμε απλά και μόνο με την χρήση ηλεκτρονικών υπολογιστών. (Βλαχόπουλος,2007)

Χαρακτηριστικό μπορεί να θεωρηθεί το παράδειγμα , όπου ένας κυβερνο-τρομοκράτης μπορεί με την βοήθεια ενός υπολογιστή, να εισβάλλει σε ένα σύστημα ελέγχου εναέριας κυκλοφορίας, να το παραποιήσει και να προκαλέσει τη σύγκρουση αεροσκαφών με αποτέλεσμα τον θάνατο εκατοντάδων ανθρώπων. Τέτοιου είδους τρομοκρατικές επιθέσεις μέσω του διαδικτύου δεν έχουν συμβεί ακόμα, αλλά είναι πολύ πιθανόν να συμβούν. (Βλαχόπουλος,2007)

Βλέπουμε λοιπόν πως οι τρομοκράτες με τη χρήση διαδικτύου, θα έχουν τη δυνατότητα να παραβιάσουν τα συστήματα ελέγχου κρίσιμων υποδομών μιας χώρας, εκτιμώντας λοιπόν πως το βασικότερο όπλο των τρομοκρατών του μέλλοντος θα είναι ο ηλεκτρονικός υπολογιστής. (Βλαχόπουλος,2007)

1.3.3.7 Επιθέσεις Παρενόχλησης

Με τον όρο παρενόχληση περιγράφεται μία εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως είναι το διαδίκτυο και τα κινητά τηλέφωνα, επιθυμεί να παρενοχλήσει τα θύματα του εκβιάζοντας τα, απειλώντας τα ή εκφοβίζοντας τα με σκοπό να τα εκδικηθεί, να λύσει προσωπικές διαφορές και για πολλούς ακόμη διάφορους λόγους. Η συμπεριφορά αυτή προϋπήρχε, απλά με τη διάδοση του διαδικτύου έχει λάβει πλέον τεράστιες διαστάσεις, με αποτέλεσμα το μεγαλύτερο ποσοστό αυτών των εγκλημάτων, να πραγματοποιείται με τη χρήση του διαδικτύου. (Βλαχόπουλος,2007)

Σύμφωνα με τον Maxwell, η παρενόχληση που διαπράττεται μέσω του διαδικτύου, διακρίνεται σε δύο κατηγορίες:

1. Στην άμεση παρενόχληση, όπου ο επιτιθέμενος αποστέλλει απευθείας στο θύμα προσβλητικά ή απειλητικά μηνύματα ασχέτως αν οι απειλές αυτές πραγματοποιηθούν.
2. Στην έμμεση παρενόχληση, όπου ο επιτιθέμενος δεν στέλνει απευθείας στο θύμα τα μηνύματα με προσβλητικό ή απειλητικό περιεχόμενο, αλλά επιλέγει να τα στείλει σε τυχαίους χρήστες του διαδικτύου δυσφημίζοντας ή προσβάλλοντας το θύμα στους τυχαίους χρήστες του διαδικτύου. (Βλαχόπουλος,2007)

Αυτός ο τρόπος επίθεσης μπορεί να αποτελέσει το μέσο έκφρασης συναισθημάτων μίσους από τον επιτιθέμενο προς άλλους ανθρώπους, αλλά και το μέσο έκφρασης προκαταλήψεων και διακρίσεων εναντίον των μειονοτήτων στον κυβερνοχώρο. Η ανωνυμία του διαδικτύου επιτρέπει στους χρήστες να κρατούν την προσωπική τους ταυτότητα κρυφή, εκφράζοντας τις προκαταλήψεις τους ευκολότερα και χωρίς τον κίνδυνο αντεκδίκησης. (Glaser & Kahn,2005) Αυτές λοιπόν οι ομάδες μίσους και προκατάληψης έχουν εξαπλωθεί στο διαδίκτυο. Παρόλα αυτά γίνονται προσπάθειες για την αντιμετώπισή τους, και ιδιαίτερα των προκαταλήψεων, από διάφορες Οργανώσεις όπως η AntiDefamation Geague (Ένωση Κατά

της Συκοφαντίας των Εβραίων), το Southern Poverty Law Center και το Simon Wiesenthal Center έχουν δημιουργήσει δικτυακούς τόπους όπου εντοπίζουν τις προκαταλήψεις και προάγουν την ανεκτικότητα. Ακόμη πολλές εταιρίες λογισμικών προσφέρουν διάφορα προγράμματα που φιλτράρουν τις ιστοσελίδες και προστατεύουν τα παιδιά από την είσοδο τους σε δικτυακούς τόπους όπου εκφράζονται ρατσιστικές αντιλήψεις.(Thio, 2008)

Πολλές φορές όμως μέσω της ανωνυμίας, το διαδίκτυο επηρεάζει τις προκαταλήψεις με αντιφατικό τρόπο. Από την μία ο φανατικός προκατειλημμένος χρήστης μπορεί να εκφράσει τις ρατσιστικές του απόψεις εις βάρος μειονοτήτων με την χρήση της ανωνυμίας της ταυτότητας που μπορεί να του προσφέρει το διαδίκτυο, αλλά από την άλλη η ανωνυμία της ταυτότητας στο διαδίκτυο μπορεί να λειτουργήσει θετικά προς τα μέλη ομάδων μειονοτήτων τα οποία κρατώντας την ανωνυμία τους μπορούν να κάνουν αίτηση για μια θέση εργασίας ή για ένα στεγαστικό δάνειο μην έχοντας να αντιμετωπίσουν την προκατάληψη του εργοδότη ή του υπεύθυνου του δανείου ο οποίος δεν θα γνωρίζει προσωπικά των αιτούντα. Επομένως στον κυβερνοχώρο τα άτομα είναι πιο πιθανό να εκφράσουν τις προκαταλήψεις τους, αν έχουν, αλλά είναι λιγότερο πιθανό να κάνουν πράξη τις διακρίσεις τους.(Thio, 2008).

CYBERBULLYING ΣΤΟ ΧΩΡΟ ΤΟΥ ΣΧΟΛΕΙΟΥ

Το cyberbullying είναι και αυτό μια μορφή εγκλήματος που συμπεριλαμβάνεται στην κατηγορία των επιθέσεων παρενόχλησης. Πιο συγκεκριμένα:

Το cyberbullying συμβαίνει όταν ένα πρόσωπο ή μια ομάδα έχουν ως σκοπό να απειλούν, να τρομοκρατούν με άμεση απειλή κινδύνου η να εξαναγκάζουν κάποιον σε πράξη – παράλειψη –ανοχή με τη χρήση νέων τεχνολογιών. Το cyberbullying είναι ιδιαίτερα αναγνωρισμένο και χρησιμοποιείται συχνά στον χώρο του σχολείου από παιδιά του δημοτικού μέχρι και παιδιά του λυκείου. Αυτή η εξάπλωση του συγκεκριμένου

ηλεκτρονικού εγκλήματος αποτελεί αύξηση της αγωνίας και του φόβου τόσο των γονέων όσο και τον εκπαιδευτικών.

(http://kids.dart.gov.gr/KidsNewsInner.aspx?new_id=168&nwc_id=24)

Εκείνοι που συμμετέχουν στο cyberbullying συνήθως είναι μια ομάδα φίλων οι οποίοι κακοποιούν ψυχικά ή και σωματικά τα θύματά τους. Σκοπός τους είναι ο ευτελισμός και η τρομοκρατία του συμμαθητή τους! (http://kids.dart.gov.gr/KidsNewsInner.aspx?new_id=168&nwc_id=24)

Το Cyberbullying μπορεί να πάρει πολλές μορφές. Πρόκειται δε για μια εξελισσόμενη μόδα. Οι συμπεριφορές που μπορεί να προκύψουν περιλαμβάνουν:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με κακό περιεχόμενο(instant messengers και τα chatrooms)
- Η κακόβουλη δημοσίευση φωτογραφιών(social networking sites) ή μηνυμάτων σε ιστολόγια (blogs) ή άλλες ιστοσελίδες με σκοπό μοναδικό την παρενόχληση
- Χρήση του ονόματος (θύματος) από τρίτο κακόβουλο πρόσωπο με σκοπό τη διάδοση φημών και ψευδών γεγονότων
- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή!

Η αποστολή ειδικών προγραμμάτων Trojan Horses (Δούρειοι Ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών ενός π.χ Msn messenger, ο οποίος ανήκει σε συμμαθητή τους.(http://kids.dart.gov.gr/KidsNewsInner.aspx?new_id=168&nwc_id=24)

ΥΠΟΚΕΦΑΛΑΙΟ 2: Άλλες μορφές ηλεκτρονικού εγκλήματος

2.1 Κινητή Τηλεφωνία

Στις προηγμένες χώρες η κινητή τηλεφωνία έχει αναπτυχθεί ιδιαίτερα τα τελευταία χρόνια. Αρχικά τα κινητά τηλέφωνα χρησιμοποιήθηκαν ως μια επέκταση των σταθερών τηλεφώνων, με το πέρασμα του χρόνου άρχισαν να ενσωματώνουν στις λειτουργίες τους και άλλες υπηρεσίες. Έτσι σε πολύ σύντομο χρονικό διάστημα τα κινητά άρχισαν να παρέχουν διαδικτυακές υπηρεσίες , με τη χρήση νέων πρωτόκολλων επικοινωνίας μετατρέποντας τα από απλά κινητά τηλέφωνα σε κινητούς ηλεκτρονικούς υπολογιστές, κληρονομώντας όμως εκτός από τα πλεονεκτήματα και τα μειονεκτήματα ενός ηλεκτρονικού υπολογιστή. Έτσι ένα κινητό μπορεί να μολυνθεί και αυτό πλέον από ιούς, σκουλήκια και άλλα κακόβουλα προγράμματα όπως ακριβώς και ένας ηλεκτρονικός υπολογιστής. (Βλαχόπουλος,2007)

Προβλήματα ασφαλείας αντιμετωπίζουν τα κινητά τηλέφωνα που χρησιμοποιούν το Bluetooth interface. Όλη η εσωτερική μνήμη του κινητού (τηλεφωνικός κατάλογος, κλήσεις ,φωτογραφίες κ.α) μπορούν να ανακτηθούν από μακριά εφόσον το κινητό έχει το Bluetooth σε λειτουργία εμφάνισης. Να σημειωθεί ότι το κινητό μπορεί να ελεγχθεί από απόσταση και να πραγματοποιήσει κλήσεις με σκοπό την υπερχρέωση ή την υποκλοπή των ομιλιών και πολλά άλλα. Όλα αυτά μπορούν να πραγματοποιηθούν , εφόσον στηθούν κατάλληλες υποδομές κεραιών, για τον εντοπισμό ατόμων που φέρουν τη συσκευή του κινητού μαζί τους. (Βλαχόπουλος,2007)

2.2 Τηλεπικοινωνιακά Δίκτυα

Οι επιθέσεις σε τηλεπικοινωνιακά δίκτυα αποτέλεσαν τις πρώτες ηλεκτρονικές απειλές. Οι νέες τεχνολογίες που χρησιμοποιήθηκαν στον τομέα των τηλεπικοινωνιών και η επέκταση της χρήσης του πρωτόκολλου IP (Internet Protocol) που αναμένεται να κυριαρχήσει τα επόμενα χρόνια στον τομέα των τηλεπικοινωνιών , δημιουργούν νέες δυνατότητες διάπραξης εγκλημάτων. Μέσω του πρωτοκόλλου IP μεταφέρεται φωνή, βίντεο –τηλεόραση, εικόνες, κείμενα και μουσική. Οι πρώτες μορφές επιθέσεων στις νέες υπηρεσίες έχουν ήδη κάνει την εμφάνισή τους,

(υποκλοπή επικοινωνιών, εντοπισμός θέσης χρήστη κ.α) (Βλαχόπουλος,2007)

2.3 Μηχανήματα Αυτόματης Ανάληψης Μετρητών

Στόχος επιθέσεων με τη χρήση διάφορων τεχνικών έχουν γίνει πολλές φορές και οι χρήστες των μηχανημάτων αυτόματης ανάληψης μετρητών (ATM). Έχουν καταγραφεί πολλές περιπτώσεις μηχανισμών οι οποίοι στόχο έχουν να μπλοκάρουν τις πιστωτικές κάρτες , πολλές τοποθετήσεις μικρο-καμερών οι οποίες τοποθετούνται σε σημεία που δεν γίνονται αντιληπτές από το χρήστη του ATM και καταγράφουν το PIN του αλλά και όλες τις ενδείξεις που εμφανίζονται στην οθόνη του μηχανήματος. Τέλος τοποθετούνται πρόσθετα πληκτρολόγια πανομοιότυπα με τα πραγματικά για την απόσπαση των κωδικών των καρτών. (Βλαχόπουλος,2007)

ΥΠΟΚΕΦΑΛΑΙΟ 3: Προφίλ Θύματος

3.1 Προφίλ Θυμάτων

3.1.1 Προφίλ Θύματος

Σε όλες τις χώρες του κόσμου και στην Ελλάδα είναι δεδομένο πως οι άνθρωποι πέφτουν θύματα κάποιας απάτης κάποιων επιτήδειων. Μια νέα επιστημονική έρευνα από τη Σχολή Ψυχολογίας του βρετανικού πανεπιστημίου του Έξετερ, για λογαριασμό μιας κρατικής υπηρεσίας της Βρετανίας, ασχολήθηκε ακριβώς με αυτό και διαπίστωσε ότι τα θύματα αυτά συχνά έχουν κοινά χαρακτηριστικά . (Καρακώστας ,2001)

Ακόμα και αν κάποιος έχει καλή γνώση και εμπειρία σχετικά με κάποιο θέμα που αφορά κάποια "ευκαιρία" ή προσφορά ,που στην πραγματικότητα δεν είναι παρά απάτη, δεν μπορεί να θεωρηθεί ότι έχει τις κατάλληλες άμυνες και προστασίες. Αντίθετα, η γνώση και εμπειρία οδηγούν στο να έχει υπερβολική εμπιστοσύνη στον εαυτό του, γεγονός που αυξάνει τον κίνδυνο να πέσει θύμα. Η έρευνα δείχνει ότι γενικά τα θύματα δεν μπορούν να θεωρηθούν ότι πάσχουν από έλλειψη ικανότητας στην λήψη αποφάσεων (άλλωστε, όπως αποδείχτηκε από όλα τα μεγάλα πρόσφατα διεθνή

οικονομικά σκάνδαλα, συχνά τα θύματα δεν ήταν αδαείς μικρο-επενδυτές, αλλά έμπειροι και *μεγάλο*-επενδυτές). (Καρακώστας ,2001)

Αναφορικά τα θύματα έχουν κάποια κοινά χαρακτηριστικά όπως η έλλειψη συναισθηματικού ελέγχου κάνει κάποιον υπερβολικά παρορμητικό παγιδεύοντας τον σε απάτες . (Καρακώστας ,2001)

Μεγάλο ρόλο παίζει η έλλειψη πληροφόρησης και η κοινωνική απομόνωση, είτε επειδή κάποιος ζει μόνος του, είτε επειδή απλώς δεν θέλει να ζητήσει συμβουλές και να μοιραστεί με κάποιον άλλο τις αποφάσεις του (π.χ. για κάποια αγορά ή επένδυση).Έτσι μειώνεται η ικανότητά του να αντιληφθεί την ύποπτη φύση της συναλλαγής στην οποία πρόκειται να εμπλακεί. (Καρακώστας ,2001)

Ορισμένοι άνθρωποι είναι απλώς κατ' εξακολούθηση - θύματα. Περίπου το 10 - 20% του πληθυσμού υπολογίζεται ότι είναι συστηματικά ευάλωτο σε απάτες και έχει ιστορικό συνεχούς και διαδοχικής θυματοποίησης. (Καρακώστας ,2001)

Ακόμα ορισμένοι άνθρωποι είναι ψυχικά πιο ευάλωτοι στις απάτες, άλλοι πείθονται εύκολα όταν αναπτύξουν διαπροσωπική σχέση με τον απατεώνα (π.χ. μέσω τηλεφωνημάτων), άλλοι εντυπωσιάζονται από τα σύμβολα (λέξεις, ρούχα κλπ) και τα πρόσωπα που έχουν τον "αέρα" της εξουσίας, άλλοι νιώθουν ψυχαναγκαστικά την ηθική υποχρέωση να ανταποδώσουν σε κάποιο μικρό δώρο που έλαβαν .. (Καρακώστας ,2001)

Αντίθετα σύμφωνα με την έρευνα, ορισμένοι άνθρωποι δεν διαβάζουν καν τα γράμματα-παγίδες που τους στέλνουν οι απατεώνες ή κλείνουν αμέσως το τηλέφωνο ή αποφεύγουν τις "ύποπτες" συζητήσεις κλπ. (Καρακώστας ,2001)

3.1.2 Θυματοποίηση Ανηλίκων (Πορνογραφία)

Η θυματοποίηση των ανηλίκων από την έκθεση σε πορνογραφικό και παράνομο υλικό, είναι ευρεία, σύμφωνα με τις έρευνες παγκοσμίως

Τα ποιοτικά χαρακτηριστικά αυτών των εγκλημάτων αυξάνουν τον κίνδυνο θυματοποίησης και μειώνουν τις πιθανότητες αποτελεσματικής πρόληψης

και αντιμετώπισης. Οι δράστες αποκλίνουν από το «παραδοσιακό» προφίλ των εγκληματιών, άρα δύσκολα εντοπίζονται και συλλαμβάνονται .Τα μέτρα πρόληψης που πρέπει να ληφθούν ώστε να προστατευτούν οι ανήλικοι θα πρέπει να έχουν ως στόχο την προστασία τους από την ανεξέλεγκτη πρόσβαση τους σε πληροφορίες πορνογραφικού είδους , την μη παρουσία των ίδιων ως μέρος αυτού του περιεχομένου και την η αυτό-προστασία των ίδιων ανηλίκων. (Μυλωνόπουλος,2007)

Τέλος οι νέες μορφές θυματοποίησης απαιτούν νέες παρεμβάσεις πρόληψης, πέρα των παραδοσιακών ποινικών μέτρων που στόχο έχουν την μείωση του κινδύνου θυματοποίησης . Θα πρέπει να υπάρξει γενική πρόληψη και ευαισθητοποίηση των ανθρώπων ώστε να γνωρίσουν το πρόβλημα και να λάβουν μέτρα για την αντιμετώπιση του . (Μυλωνόπουλος,2007)

3.2 Προτάσεις για την πρόληψη της θυματοποίησης

- Ενημέρωση χρηστών- γενικού πληθυσμού
- Ανάπτυξη τεχνολογικής προστασίας
- Εκπαιδευτικά προγράμματα ενημέρωσης και ευαισθητοποίησης της οικογένειας, των σχολικών συμβούλων κ.α. για τους κινδύνους των ανηλίκων χρηστών
- Ενδυνάμωση και επέκταση όλων των σχετικών δράσεων των μη κυβερνητικών οργανώσεων (π.χ. Web Police)
- Συνεργασία, συνέργεια, συντονισμός(Μυλωνόπουλος,2007)

3.3 Αποτελέσματα Έρευνας σχετικά με τη Θυματοποίηση

- Κατά μέσο όρο στον κόσμο διακινούνται ηλεκτρονικά πάνω από 3,5 δισεκατομμύρια δολάρια το λεπτό. Οι χρήστες είναι «εν δυνάμει» θύματα.
- Η θυματοποίηση των ανηλίκων από την έκθεση σε πορνογραφικό και παράνομο υλικό, είναι ευρεία, σύμφωνα με τις έρευνες παγκοσμίως

- Τα ποιοτικά χαρακτηριστικά αυτών των εγκλημάτων αυξάνουν τον κίνδυνο θυματοποίησης και μειώνουν τις πιθανότητες αποτελεσματικής πρόληψης και αντιμετώπισης
- Οι δράστες αποκλίνουν από το «παραδοσιακό» προφίλ των εγκληματιών, άρα δύσκολα εντοπίζονται και συλλαμβάνονται.(Ζαννή,2005)

ΥΠΟΚΕΦΑΛΑΙΟ 4:Προφίλ δραστών

4.1 Δράστες Ηλεκτρονικών Εγκλημάτων

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τις κατηγορίες των δραστών των ηλεκτρονικών εγκλημάτων και θα προσπαθήσουμε να δώσουμε ένα πιθανό προφίλ του.

4.2 Κατηγορίες Δραστών Ηλεκτρονικών Εγκλημάτων

4.2.1 Σχετικά με οικονομικά εγκλήματα

Τους εγκληματίες του κυβερνοχώρου μπορούμε να τους διακρίνουμε σε δυο κατηγορίες :

1. σε αυτούς που "επιτίθενται" (εισβάλουν) στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος.

Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη "εισβάλουν " σε υπολογιστή δια της χρήσεως του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία,

2. σε αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη κατηγορία ανήκουν αυτοί που δεν " εισβάλουν " απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμότους.
   (http://sexualities.sagepub.com/cgi/content/abstract/1/4/425)

Σύμφωνα με Anderson (Furnell, 2006), υπάρχουν οι εξής κατηγορίες δραστών ηλεκτρονικών εγκλημάτων:

• Εξωτερικοί δράστες: Πρόσωπα προερχόμενα από τον εξωτερικό χώρο της επιχείρησης – στόχου τους, που πετυχαίνουν πρόσβαση στο σύστημα της δίχως να έχουν εξουσιοδότηση. Αυτή είναι η κατηγορία η οποία ανταποκρίνεται περισσότερο στην παραδοσιακή εικόνα του χάκερ – δεν έχουν νόμιμο σκοπό και ως εκ τούτου δεν έχουν ρόλο να παίξουν στο σύστημα. (Furnell,2006)

• Εσωτερικοί δράστες: χρήστες του συστήματος, που έχουν εξουσιοδότηση και αποκτούν πρόσβαση σε δεδομένα, πηγές ή προγράμματα δίχως να έχουν τέτοιο δικαίωμα. (Furnell,2006)

Οι υποκατηγορίες τους έχουν ως εξής:

Μεταμφιεσμένοι: χρήστες, που δρουν χρησιμοποιώντας την ταυτότητα άλλου χρήστη.

Κρυφοί χρήστες: χρήστες, που επιτυγχάνουν παράνομη πρόσβαση σε αρχεία με σκοπό τον έλεγχο και την εξέταση του περιεχομένου τους.

Έκπτωτοι: χρήστες, που έχουν την άδεια να χρησιμοποιούν το σύστημα και τις πηγές του στις οποίες αποκτούν πρόσβαση, αλλά έχουν απολέσει τα προνόμιά τους. Αυτή η ομάδα είναι τυπικά η πιο δύσκολα αναγνωρίσιμη, επειδή τα πρόσωπα έχουν νόμιμη πρόσβαση στο σύστημα και γνωρίζουν πώς να το χρησιμοποιούν. (Furnell,2006)

4.3 Πιο Συγκεκριμένα το Προφίλ του Εγκληματία του Κυβερνοχώρου

Ο "εγκληματίας του κυβερνοχώρου" διαφέρει ουσιωδώς από τον "κοινό εγκληματία". Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. Ο δράστης πρέπει να διαθέτει:

- ειδικές γνώσεις,
- τεχνική επιδεξιότητα,
- τεχνικά μέσα.

Ο εγκληματίας του κυβερνοχώρου, (cyber-crook), δεν μπορεί να υποστηρίξει ότι ενήργησε "από ανάγκη" δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής

οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο. (Τσουραμάνης , 2005).

Σε ειδική έρευνα που έγινε στη Βρετανία από την ``επιτροπή πρόβλεψης και πρόληψης εγκλήματος`` (Foresight Crime Prevention Panel) για το ``ποιόν`` (``who is who``) του μελλοντικού εγκληματία διαπιστώθηκε ότι:

Το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμα δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον ``ξεγελούν`` με την ανάλογη κατασκευή φακών επαφής (Τσουραμάνης, 2005).

4.4 Το Προφίλ των Δραστών που ασχολούνται με τα Τυχερά Παιχνίδια

Σύμφωνα με μία μελέτη τα άτομα τα οποία επισκέπτονται τα παραδοσιακά καζίνα έχουν μεγαλύτερες πιθανότητες να ασχολούνται και με τα online τυχερά παιχνίδια από ότι τα άτομα τα οποία δεν επισκέπτονται τα παραδοσιακά καζίνα. Συνήθως οι online παίχτες είναι μικρότερης ηλικίας από ότι οι παραδοσιακοί παίχτες τυχερών παιχνιδιών. Επίσης έχουν υψηλότερο μορφωτικό επίπεδο και είναι πιο πρόθυμοι να ποντάρουν online. (http://www.cababstractsplus.org/abstracts/Abstract.aspx?AcNo=20053078010) Μια άλλη μελέτη μας τονίζει περισσότερο τις διαφορές που υπάρχουν ανάμεσα στους online παίχτες και στους παραδοσιακούς παίχτες τυχερών παιχνιδιών. Μια σημαντική διαφορά σε αυτές τις δύο κατηγορίες παιχτών είναι ότι οι online παίχτες είναι οικονομικά πιο ευσταθείς. Έχουν μεγαλύτερες πιθανότητες να σταματήσουν να παίζουν αν τους τελειώσουν τα χρήματα που αρχικά είχαν αποφασίσει να διαθέσουν να παίξουν από ότι οι παραδοσιακοί παίχτες οι οποίοι μπορεί να δανειστούν για να συνεχίσουν να παίζουν. Η έλλειψη οικονομικού ελέγχου που εμφανίζεται στους παραδοσιακούς παίχτες αντανακλά προφανώς το χαμηλό μορφωτικό τους

επίπεδο που προαναφέραμε. Μία άλλη διαφορά έγκειται στο βαθμό εθισμού που υπάρχει ανάμεσα στον παραδοσιακό τζόγο και στον τζόγο του διαδικτύου. Ο τζόγος του διαδικτύου είναι πιο εθιστικός καθώς είναι ένας εύκολος, διασκεδαστικός, μοναχικός και ανώνυμος τρόπος για να παίξει κάποιος. (http://www.eou.edu/~jdense/griffithsparke.pdf)

4.5 Το Προφίλ των Δραστών του Εγκλήματος της Παιδικής Πορνογραφίας

ΠΑΙΔΟΦΙΛΟΙ

Παιδόφιλος είναι εκείνος ο ενήλικας που σεξουαλικά προσελκύεται από παιδιά. Τα διαγνωστικά κριτήρια για ένα παιδόφιλο περιλαμβάνουν :

1. Επαναλαμβανόμενες και έντονες σεξουαλικά φαντασίες, ωθήσεις ή συμπεριφορές που αφορούν σεξουαλικές πράξεις με ένα προεφηβικό παιδί.

2. Το άτομο έχει δράσει με τέτοιες σεξουαλικές ωθήσεις ή αυτές οι σεξουαλικές ωθήσεις και φαντασίες είναι τα αίτια μιας διαπροσωπικής δυσκολίας.

3. Το άτομο είναι 16 ετών ή μεγαλύτερο και έχει τουλάχιστον 5 χρονών ηλικιακή διαφορά από το παιδί (http://sexualities.sagepub.com/cgi/content/abstract/1/4/425)

Είναι αναγκαίο να επισημανθεί ότι δεν υφίσταται ομοιογένεια ανάμεσα στους δράστες παιδικής πορνογραφίας διότι διαφοροποιούνται συχνά ως προς τα κίνητρά τους. Για παράδειγμα, στην κατηγορία των συλλεκτών και διαχειριστών πορνογραφικού υλικού παιδιών στο ιντερνέτ ανήκουν άτομα που χαρακτηρίζονται από ψυχοσεξουαλική διαταραχή και ειδικότερα παιδοφιλία «πελάτες» του διαδικτύου που επιζητούν την απόκτηση καινούργιων σεξουαλικών εμπειριών, αλλά και «επαγγελματίες» που αποσκοπούν στο κέρδος μέσω της διακίνησης και (ανα)παραγωγής του εν λόγω υλικού καθώς και άλλοι. Συνεπώς, οποιαδήποτε απόπειρα γενίκευσης αναφορικά με τα χαρακτηριστικά των δραστών χρήζει σημαντικής προσοχής. (Jenkins ,2001)

Ιδιαίτερα ενδιαφέρουσα είναι η κατάταξη που έχει επιχειρήσει σε σχετική έρευνά του το **Ινστιτούτο Εγκληματολογίας της Αυστραλίας:**
Οι δράστες του εγκλήματος της πορνογραφίας ανηλίκων στο διαδίκτυο τίθενται σε κατηγορίες ανάλογα με τα κίνητρά τους, ξεκινώντας από αυτούς που δεν έχουν άμεση εμπλοκή με τον ανήλικο και καταλήγοντας σε αυτούς που επιδιώκουν τη σεξουαλική συναναστροφή με αυτόν. (http://sax.sagepub.com/cgi/content/refs/19/4/449)

Ειδικότερα, στο πλαίσιο της συγκεκριμένης έρευνας, περιγράφονται οχτώ τύποι δραστών:

1) Ο πρώτος αποτελεί το άτομο που κάνει χρήση του διαδικτύου και δίχως τη θέλησή του (επί παραδείγματι με τη μέθοδο του spamming) συναντά παιδικό πορνογραφικό υλικό και, παρά το γεγονός ότι δε το επιδίωξε, δέχεται να το κρατήσει, (http://sax.sagepub.com/cgi/content/refs/19/4/449)

2) Ο δεύτερος τύπος χρήστη περιγράφει το άτομο που φαντασιώνεται σεξουαλικά ανηλίκους, αποτυπώνει σε ψηφιακής μορφής κείμενα τις συγκεκριμένες του φαντασιώσεις στον υπολογιστή του ή κάνει προσωπική χρήση ψηφιακών φωτογραφιών, δίχως, όμως, να προτίθεται να τις διανέμει σε άλλους, (http://sax.sagepub.com/cgi/content/refs/19/4/449)

3) Τον τρίτο τύπο αποτελεί ο «αλιευτής», που επιζητεί υλικό παιδικής πορνογραφίας ενεργά, επικοινωνώντας για το σκοπό αυτό και με άλλους χρήστες με συναφείς προτιμήσεις,

4) Τον τέταρτο τύπο χαρακτηρίζει η ανασφάλεια και για τον λόγο αυτό αποτελεί τον «επισφαλή» συλλέκτη, ο οποίος κάνει χρήση πορνογραφικού υλικού το οποίο περιέχεται σε διαδικτυακούς τόπους ή chat rooms, όπου δεν απαιτούνται κωδικοί ασφαλείας, εγγραφές και οτιδήποτε άλλο σχετικό για να αποκτήσει πρόσβαση. Ο συγκεκριμένος χρήστης λαμβάνει ιδιαίτερα υψηλό ρίσκο ως προς την αποκάλυψη των στοιχείων του.

5) Ο επόμενος τύπος, εν αντιθέσει με τον προηγούμενο, χρησιμοποιεί πάντα εχέγγυα. Επί παραδείγματι, ορισμένα δίκτυα ανταλλαγής υλικού απαιτούν, προτού ολοκληρωθεί η διαδικασία εγγραφής καινούργιων μελών, να

κατατεθεί από τα τελευταία μερίδα των προσωπικών τους συλλογών, «κλειδώνοντας» με τον τρόπο αυτό τα μέλη τους,

6) Ο έκτος τύπος αποτελεί τον λεγόμενο groomer, ο οποίος προσελκύει μέσω του ίντερνετ ανηλίκους, ώστε να τους κακοποιήσει σεξουαλικά. Η χρήση παιδικού πορνογραφικού υλικού υλοποιείται εν προκειμένω, ώστε ο ανήλικος να προετοιμαστεί για την ειδική περίσταση και να αμβλυνθεί η συστολή του.

7) Ο έβδομος τύπος τελεί σεξουαλικά εγκλήματα εις βάρος ανηλίκων. Για τον συγκεκριμένο, η παιδική πορνογραφία χρησιμοποιείται ως πλαίσιο της εν λόγω δραστηριότητάς του, καθώς ο ίδιος παράγει το υλικό με την κακοποίηση του παιδιού και εν συνεχεία το διακινεί στο διαδίκτυο. Δεν αποκλείεται να πείθει και τα ίδια τα παιδιά να διαθέσουν τις φωτογραφίες τους.

8) Ο τελευταίος τύπος περιγράφει αυτόν που πωλεί το πορνογραφικό υλικό στο σύνολο των ανωτέρω, επιδιώκει δηλαδή μέσω αυτής του της πράξεις να αποκομίσει οικονομικό όφελος. Ο ίδιος ενδέχεται να έχει σεξουαλικό ενδιαφέρον για παιδιά, αλλά αυτό μπορεί κιόλας να μη συμβαίνει. (http://sax.sagepub.com/cgi/content/refs/19/4/449)

Αν και από τα παραπάνω συνάγεται το συμπέρασμα ότι οι δράστες παρουσιάζουν αρκετές διαφορές μεταξύ τους, υφίστανται ορισμένα στοιχεία που εμφανίζουν πολλοί από αυτούς, όπως:

- ότι τα συγκεκριμένα άτομα δυσκολεύονται στο να συμμεριστούν τον πόνο του άλλου (στην «ενσυναίσθηση» όπως χαρακτηριστικά ονομάζεται).
- Επιπρόσθετα, πολλοί παιδόφιλοι είχαν υποστεί στο παρελθόν σεξουαλική κακοποίηση.
- Η ψυχολογική ανωριμότητα, ανάλογη τα παιδιά – θύματα, αποτελεί, επίσης, ένα σύνηθες χαρακτηριστικό τους.
- Σημαντικό, επιπλέον, ότι οι χρήστες παιδικής πορνογραφίας είναι πολύ πιθανό να έχουν κάποια ερωτική σχέση,

- ορισμένο επάγγελμα,
- υψηλό δείκτη νοημοσύνης,
- πανεπιστημιακή μόρφωση,
- καθώς και λευκό ποινικό μητρώο και για το λόγο αυτό είναι ιδιαίτερα δυσχερής η σκιαγράφηση του εγκληματικού τους στερεοτύπου. Εκείνοι που έχουν κατηγορηθεί για τέλεση εγκλημάτων παιδικής πορνογραφίας στο διαδίκτυο είναι οδοντίατροι, δάσκαλοι, ακαδημαϊκοί καθηγητές, σταρ του ροκ, επαγγελματίες στρατιώτες και αξιωματικοί της αστυνομίας, οδηγοί ταξί
- έχουν σχετικά χαλαρούς δεσμούς με τη θρησκεία
- το 70% της κυκλοφορίας σε αυτούς τους δικτυακούς τόπους γίνεται κατά τη διάρκεια των ωρών εργασίας
- περισσότεροι θεατές πορνογραφικού υλικού είναι λευκοί άντρες
- Ηλικίας από 30 έως 50 ετών (Jenkins ,2001)

Είναι αξιοσημείωτο, τέλος, ότι, από πορίσματα ερευνών που διεξήχθησαν σε δείγμα ανδρών που είχαν κατηγορηθεί για κατοχή παιδικού πορνογραφικού υλικού, προέκυψε ότι μέσω της συλλογής παιδικής πορνογραφίας δεν επιδιωκόταν η σεξουαλική διέγερση και ικανοποίηση. Έχει προκύψει, λοιπόν, ότι σε κάποιες περιπτώσεις ο συλλέκτης επιδιώκει τον εμπλουτισμό της συλλογής του με κάτι πρωτόγνωρο. Από τη συγκεκριμένη συμπεριφορά αναδεικνύεται ο ρόλος που διαδραματίζει η πορνογραφία ανηλίκων ως προϊόν προς πώληση και ταυτόχρονα ως «τρόπαιο». (Jenkins ,2001)

4.6 Προφίλ Δραστών που ασχολούνται με την Ηλεκτρονική Παραβίαση Αρχείων ή Hacking

Τις περισσότερες φορές οι δράστες δεν μοιάζουν με αυτό που ονομάζουμε «σπασίκλες» και δεν έχουν εξαιρετικές ικανότητες στους ηλεκτρονικούς υπολογιστές. Αντίθετα, πρόκειται για μέσους μαθητές, οι οποίοι εκμεταλλεύονται την χαλαρή ασφάλεια και την εύκολη πρόσβαση στα συστήματα των ηλεκτρονικών υπολογιστών. Συνήθως οι δράστες είναι συμμορίες οργανωμένου εγκλήματος σε σχετικά φτωχές χώρες στις οποίες

δεν υπάρχει η απαραίτητη νομοθεσία για την αντιμετώπιση του χάκινγκ ή αν υπάρχει δεν εφαρμόζεται. Τα μέλη αυτών των καινούριων συμμοριών που ασχολούνται με το χάκινγκ είναι είτε έξυπνοι έφηβοι ή απογοητευμένοι άντρες από είκοσι έως σαράντα ετών. Σε πολλές περιπτώσεις ο δράστης για να συλλέξει πληροφορίες που θα τον βοηθήσουν στην πραγματοποίηση του εγκλήματός του, συνήθως για την εισβολή αρχείων μιας εταιρείας, παριστάνει ότι είναι συνάδελφος ή κάποιος άλλος έμπιστος υπάλληλος της εταιρείας. (Newton,2004)

Το πιο εντυπωσιακό πράγμα σχετικά με το χάκινγκ είναι ότι πρόκειται κυρίως για μία μορφή νεανικής παρέκκλισης. Συνήθως οι νεανικοί παραβάτες:

- Άντρες , με αναλογία στους άντρες και στις γυναίκες δράστες να είναι 99 προς 1.
- Άτομα τα οποία προέρχονται από δυσλειτουργικές οικογένειες, όπου βιώνουν την αδιαφορία των γονέων τους ,να έχουν αλκοολικούς γονείς, γονείς οι οποίοι τους κακοποιούν κα
- Άτομα που πολλές φορές συγχρωτίζονται με μια ομάδα συνομηλίκων τους και εμπλέκονται σε δραστηριότητες που η ομάδα αυτή τους ενθαρρύνει, όπως η συμμετοχή σε έναν διαγωνισμό όπου ο ένας προσπαθεί να παραβιάσει τα ηλεκτρονικά αρχεία του άλλου. (Yount, 2006).
- Έχουν το δικό τους έμβλημα
- Το ντύσιμό τους είναι casual και συνήθως αφήνουν μακριά μαλλιά και γένια
- Διαβάζουν πολλά βιβλία
- Παίζουν παιχνίδια που έχουν να κάνουν με την ευφυΐα, όπως σκάκι τάβλι κλπ
- Απεχθάνονται τον αθλητισμό, με εξαίρεση ορισμένα ατομικά αθλήματα και το βόλεϊ.
- Σε όλες τις δραστηριότητες τους με τους υπολογιστές χρησιμοποιούν την Αγγλική γλώσσα

- Ενδιαφέρονται για την τέχνη την οποία προσαρμόζουν στον δικό τους ψηφιακό κόσμο
- Η σχέση τους με τη θρησκεία είναι ουδέτερη (Yount, 2006).

Παρόλα αυτά οι χάκερς μοιάζουν με «φυσιολογικά» παιδιά και δεν διαφέρουν σε τίποτα από τους συνομηλίκους τους. Αξίζει επίσης να σημειωθεί ότι η κουλτούρα τους δεν ακολουθείται πιστά από όλους. (Newton,2004)

ΥΠΟΚΕΦΑΛΑΙΟ 5: Ασφάλεια στο Διαδίκτυο

5.1 Χρήσιμες Συμβουλές και Προληπτικά Μέτρα για την Προστασία των Χρηστών

5.1.1 Όρος Ασφάλεια

«Ο όρος ασφάλεια στα πληροφοριακά συστήματα σχετίζεται με την πρόληψη ,την ανίχνευση και την αντίδραση ,όπου αποτελούν τον γενικότερο σχεδιασμό της ασφάλειας ενός οργανισμού και ονομάζεται πολιτική ασφάλεια .Λίγο πιο αναλυτικά υπάρχει πρόληψη δηλαδή προστασία δεδομένων από μη εξουσιοδοτημένες ενέργειες έναντι ενός συστήματος ,ανίχνευση από κάθε είδους επιθέσεων και τέλος η αντίδραση δηλαδή η λήψη μέτρων για την αποκατάσταση των ζημιών που προκλήθηκαν στο πληροφοριακό σύστημα από τον επιτιθέμενο» .

(Λάζος,2001)

5.1.2 Εισαγωγή για Ασφάλεια

Το Διαδίκτυο είναι ένα μέσο με απεριόριστα οφέλη για όλους (μικρούς και μεγάλους). Τα αποτελέσματά του, θετικά ή αρνητικά, εξαρτώνται από την χρήση που εμείς οι ίδιοι κάνουμε.

Κανείς δεν είναι απροστάτευτος στο Διαδίκτυο. Υπάρχουν δικαιώματα, τρόποι πρόληψης, φορείς και αρχές για την προστασία των χρηστών.

Η δημιουργική και ασφαλής χρήση του Διαδικτύου είναι το νέο εργαλείο για την βελτίωση της ποιότητας ζωής μας που όλοι πρέπει να μάθουμε ώστε να απολαύσουμε ισότιμα τα οφέλη της νέας εποχής. (Βλαχόπουλος,2007)

Ένα πληροφοριακό σύστημα για να θεωρείται ασφαλές θα πρέπει να διαθέτει:

1. Εμπιστευτικότητα
2. Ακεραιότητα
3. Διαθεσιμότητα

Εμπιστευτικότητα Με την έννοια εμπιστευτικότητα αναφερόμαστε στην προστασία των δεδομένων μας από την μη εξουσιοδοτημένη πρόσβαση άλλων ατόμων σε αυτά . (Βλαχόπουλος,2007)

Ακεραιότητα Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. (Βλαχόπουλος,2007)

Διαθεσιμότητα Η διαθεσιμότητα περιλαμβάνει την δυνατότητα πρόσβασης του χρήστη στα δίκτυα και τα δεδομένα ώστε να είναι διαθέσιμα όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευόμενοι πόροι είτε προσωρινά είτε μόνιμα. (Βλαχόπουλος,2007)

5.1.3 Μέτρα Πρόληψης για τον Έλεγχο του Διαδικτυακού Εγκλήματος

Τα μέτρα πρόληψης που έχουν ληφθεί κατά του διαδικτυακού εγκλήματος κλίνουν υπέρ μιας ποινικής πρόληψης που ανάλογα με τη νομοθεσία και το εθιμικό δίκαιο της κάθε χώρας αποσκοπεί σε ήπιες ή αυστηρές μορφές .Πιο συγκεκριμένα στα πλαίσια της αποτροπής εγκληματικών δραστηριοτήτων εμφανίζονται δύο προσεγγίσεις. Η πρώτη προσέγγιση επιδιώκει την επιβολή αυστηρών μέτρων πρόληψης και αντιμετώπισης και η δεύτερη προσέγγιση

τη επιβολή των ήπιων μέτρων. Όσο αφορά την πρώτη περίπτωση υποστηρίζεται από όσους το επιδιώκουν, αυξανόμενη εξουσία των διωκτικών μηχανισμών και των κυβερνητικών βιομηχανιών λογισμικού και κατασκοπείας .Πρόκειται για δικανικές ρυθμίσεις όπου έχουν προταθεί και εφαρμοστεί από όλα τα επίσημα όργανα για την διεθνή πρόληψη και αντιμετώπιση του διαδικτυακού εγκλήματος .Η δεύτερη περίπτωση ,περιλαμβάνει κίνητρα ενάντια στην εγκληματική δραστηριότητα μέσα από εννοιολογικούς ορισμούς των ποινικών αδικημάτων και την δημόσια ευαισθητοποίηση και εκπαίδευση σχετικά με τη σχέση ανθρώπου και τεχνολογίας(μη δικανικές ρυθμίσεις). (Ζαννή,2005)

5.1.4 Δικαιϊκές ρυθμίσεις –αυστηρή πρόληψη

Οι δικαιϊκές ρυθμίσεις που προτείνονται έχουν σχέση με τις ακόλουθες τεχνικές:

1. ΣΥΣΤΗΜΑΤΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

«Το Echelon είναι το πρώτο σύστημα παρακολούθησης η ύπαρξη του οποίου ταυτίστηκε με την ανάγκη ασφάλειας του διαδικτύου . Αποτελεί τμήμα ενός παγκόσμιου κατασκοπευτικού συστήματος, επιτρέπει την υποκλοπή και την ανάλυση, μέσω ενός δικτύου δορυφόρων, κάθε διεθνούς τηλεπικοινωνίας. Τις πληροφορίες που συλλέγονται μέσω του Echelon, εκμεταλλεύονται οι μυστικές υπηρεσίες NSA (National Security Agency, Εθνική Υπηρεσία Ασφαλείας) των Η.Π.Α. και GCHQ (Government Communications Headquarters, Κεντρική Διοίκηση Κυβερνητικών Επικοινωνιών) της Μεγάλης Βρετανίας.» (Ζαννή,2005 σελ.88)

2. ΤΕΧΝΙΚΑ ΜΕΣΑ

α)Κρυπτογραφία

Κάθε πακέτο δεδομένων που στέλνεται μέσω του Internet διασχίζει πολλά δημόσια δίκτυα, γεγονός που σημαίνει ότι η πρόσβαση σε αυτά τα πακέτα δεν είναι ιδιωτική. Με τον όρο κρυπτογραφία εννοούμε την μετατροπή αρχικού κειμένου σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο) με τη χρήση κάποιας μαθηματικής συνάρτησης

από τον αποστολέα. Ο παραλήπτης του μηνύματος αποκρυπτογραφεί το κείμενο στην αρχική του μορφή έχοντας γνώση του τρόπου κρυπτογράφησης. Η κρυπτογραφία βοηθάει στο να παραμείνει εμπιστευτικό το μήνυμα και να μη διαβάζεται από ανεπιθύμητους τρίτους. Πολλά σύνθετα κρυπτογραφικά συστήματα χρησιμοποιούν αυτό το είδος της απόκρυψης και της αποκωδικοποίησης χρησιμοποιώντας κλειδιά τα οποία είναι μυστικοί αριθμοί που χρησιμοποιούν οι υπολογιστές σε συνδυασμό με σύνθετους μαθηματικούς τύπους που ονομάζονται αλγόριθμοι για την κωδικοποίηση και αποκωδικοποίηση των μηνυμάτων. (Λάζος,2001)

β) Ψηφιακή υπογραφή

Ένα άλλο τεχνικό μέσο είναι η ψηφιακή υπογραφή η οποία αποτελεί μία μέθοδο προστασίας των οικονομικών συναλλαγών που λαμβάνουν χώρα στο διαδίκτυο .Συγκεκριμένα η ηλεκτρονική ψηφιακή υπογραφή είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Η ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του περιεχομένου των ηλεκτρονικών εγγράφων. Βοηθά τον παραλήπτη να βεβαιωθεί ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις και πως μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα και όχι ανεπιθύμητοι τρίτοι. (Λάζος,2001)

γ)Πρωτόκολλα επικοινωνίας

«Το πρωτόκολλο επικοινωνίας είναι μια δέσμη κανόνων στους οποίους στηρίζεται η επικοινωνία των συσκευών (συνήθως, αλλά όχι πάντα, υπολογιστών) σε ένα δίκτυο. Οι κανόνες αυτοί καθορίζουν τη μορφή, το χρόνο και τη σειρά μετάδοσης των πληροφοριών στο δίκτυο. Εκτελούν, επίσης, έλεγχο και διόρθωση σφαλμάτων στη διάρκεια μετάδοσης των πληροφοριών. Τα πρωτόκολλα που είναι περισσότερο διαδεδομένα είναι το TCP/IP, το NETBEUI και το IPX/SPX». (Λάζος,2001 σελ.76)

δ)Ανώνυμη ηλεκτρονική αλληλογραφία

Μια άλλη τεχνική προστασίας που είναι ιδιαίτερη χρήσιμη στην περίπτωση παραβίασης του ηλεκτρονικού ταχυδρομείου είναι η ανώνυμη αλληλογραφία .Η οποία είναι χρήσιμη σε περιπτώσεις όπως να αποσταλούν e-mail σε ομάδες ενδιαφερόντων χωρίς να διατρέχει κάποιος να βλάψει την φήμη του ,να επικοινωνήσει με άλλους για ιατρικής φύσεως θέματα ,να βοηθήσει ανώνυμα την αστυνομία ,να καταγγείλει ανεπάρκεια ή διαφθορά δημοσίων προσώπων ,να επικοινωνήσει με ασφάλεια σε περίπτωση ύπαρξης καταπιεστικών καθεστώτων κ.α. Φυσικά και η τεχνική της ανώνυμης ηλεκτρονικής αλληλογραφίας θεωρείται μια τεχνική όπου μπορεί να χρησιμοποιηθεί τόσο για την απόκρυψη επικοινωνίας μεταξύ εγκληματικών ομάδων όσο και για τον έλεγχο της ιδιωτικότητας . (Λάζος,2001)

5.1.5 Μη Δικαιϊκές Ρυθμίσεις – Ήπια Πρόληψη και Αντιμετώπιση

«Οι υποστηρικτές της ήπιας πρόληψης υποστηρίζουν ότι οι εγκληματικές καταστάσεις που δημιουργούνται στο διαδίκτυο μπορούν να διευθετηθούν μέσω της αυτορρύθμισης δηλαδή των κανόνων συμπεριφοράς , που οι ρυθμιστές του διαδικτύου σε τεχνολογικό και δεοντολογικό επίπεδο μπορούν να επιβάλλουν (δημιουργία και τήρηση κανόνων δεοντολογίας ,δημιουργία συστήματος επίβλεψης επικίνδυνης συμπεριφοράς χρηστών ,συστήματα διαιτησίας ,τήρηση αρχείων κίνησης ως χρήση για αποδεικτικά μέσα και τέλος την καταγραφή των ενεργειών των παράνομων δραστών μέσω συστημάτων παρακολούθησης ». (Ζαννή,2005 σελ. 93)

5.2 Προληπτικά Μέτρα Προστασίας που Πρέπει να Λαμβάνονται πάντα από τους Χρήστες του Διαδικτύου

- Οι χρήστες που εισέρχονται από dial-up σύνδεση θα πρέπει να κλείνουν με κωδικό που έχουν προμηθευτεί από τον Ο.Τ.Ε.
- Ασφαλής παραμετροποίηση του λειτουργικού συστήματος και των εγκατεστημένων εφαρμογών

- Προστασία του Η/Υ με τα τελευταία patches, security updates και Hotfixes που αντιμετωπίζουν τα κενά σε επίπεδο λειτουργικού ή εφαρμογών
- Χρήση προγραμμάτων κρυπτογράφησης και συστημάτων ασφαλείας
- Λογισμικά φίλτρα (http://www.dart.gov.gr/?q=node/28)

5.2.1 Μέτρα Προστασίας κατά την Πρόσβαση στο Διαδίκτυο

- Να μην αποκαλύπτονται προσωπικά ευαίσθητα δεδομένα σε τρίτους,
- Να μην υπάρχει εμπιστοσύνη σε e-mails ή ιστοσελίδες που δεν έχουν αποδείξει την ταυτότητα τους,
- Να αποφεύγεται η συμπλήρωση φορμών με διάφορα οικονομικά στοιχεία, π.χ. Α.Φ.Μ, και η αποστολή τους μέσω e-mail χωρίς να είναι κρυπτογραφημένες,
- Να αποφεύγεται η επίσκεψη σε ύποπτα sites,
- Για τις online συναλλαγές, οι χρήστες θα πρέπει να βεβαιώνονται ότι το ηλεκτρονικό σύστημα με το οποίο συναλλάσσονται είναι αξιόπιστο,
- Να χρησιμοποιούνται χρεωστικές ή προπληρωμένες πιστωτικές κάρτες εφόσον είναι απαραίτητο,

- Οι χρήστες θα πρέπει να είναι ιδιαίτερα προσεχτικοί όσον αφορά τις πληροφορίες που αποκαλύπτουν και τα άτομα στα οποία τις αποκαλύπτουν. (Λάζος,2001)

5.3 Πιο Συγκεκριμένα για τον κάθε Χρήστη

5.3.1 Συμβουλές για Χρήστες ATM

- Πριν ξεκινήσετε τη συναλλαγή ελέγξτε προσεκτικά το χώρο γύρω σας για τυχόν ύποπτες κινήσεις
- Μην επιτρέπεται σε άγνωστα άτομα να σας πλησιάσουν κατά τη διάρκεια της συναλλαγής
- Βεβαιωθείτε ότι δεν υπάρχει κάποιο πρόσθετο εξάρτημα στο ATM
- Αν παρουσιαστεί οποιαδήποτε βλάβη, π.χ. εμπλοκή κάρτας επικοινωνήσετε μόνο με τα τηλέφωνα της Τράπεζας

- Μην εμπιστεύεστε αγνώστους που προθυμοποιούνται να σας βοηθήσουν
- Όταν πληκτρολογείτε τον κωδικό σας PIN «προστατέψτε» το πληκτρολόγιο,(http://www.dart.gov.gr/?q=node/28)

5.3.2 Προστασία από το Spam

- Να μην απαντάτε ποτέ σε ένα spam e-mail
- Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails.
- Να μην παρασύρεστε ποτέ από δελεαστικούς τίτλους
- Να μην δίνετε εύκολα την διεύθυνση του ηλεκτρονικού ταχυδρομείου (e-mail)
- Να έχετε μια πρόχειρη διεύθυνση για τα SPAM • (http://www.dart.gov.gr/?q=node/28)

5.3.3 Συμβουλές για Ασφαλείς Οικονομικές Συναλλαγές

- Αποφεύγετε να πραγματοποιείται οικονομικές συναλλαγές μέσω Διαδικτύου από Internet Café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές. Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας.
- Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.
- Αποφεύγετε να χρησιμοποιείται ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα.
- Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπή τους θα διευκολύνετε πολύ τους δράστες.
- Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μία κάρτες σας.
- Μη δίνετε τον κωδικό πρόσβασής σας σε οποιονδήποτε κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό

πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτήν την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.

- Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet Banking.
- Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.
- Κάνετε αγορές μόνο από γνωστές εταιρίες που σας παρέχουν εγγυήσεις ασφάλειας.
- Αν κάνετε συχνά αγορές από το Διαδίκτυο, χρησιμοποιείτε μία κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.
- Φροντίστε να διατηρείται σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας. (http://www.dart.gov.gr/?q=node/28)

5.4 Συμβουλές για τους Γονείς

Ενημερώστε τα παιδιά σας

- κίνδυνοι όταν συνομιλούν με αγνώστους στο διαδίκτυο
- να μην δίνουν προσωπικές τους πληροφορίες
- να αρνούνται να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. (http://www.dart.gov.gr/?q=node/28)

Ελέγξτε τα παιδιά σας:

- Τοποθετήσετε τον Η/Υ σας σε χώρους, όπου έχετε τη δυνατότητα να επιβλέπεται
- Κάντε την πλοήγηση στο Διαδίκτυο μία οικογενειακή δραστηριότητα
- Χρησιμοποιείστε ειδικά φίλτρα προστασίας
- Ελέγξτε το οπτικοακουστικό υλικό, που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους
- Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.

- Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο
- Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρίες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείται και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του.
- Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχθείτε κατά τις περιηγήσεις σας στο Διαδίκτυο.
- Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών. (http://www.dart.gov.gr/?q=node/28)

5.4.1 Πώς θα αντιληφθούν οι γονείς ότι κάτι περίεργο συμβαίνει :

- το παιδί λαμβάνει ανεξήγητα ή ύποπτα δώρα, από ανθρώπους που δεν γνωρίζουν ή δεν έχουν ακούσει ποτέ,
- το παιδί λαμβάνει τηλεφωνήματα από ενήλικους ή από μεγαλύτερους εφήβους που δεν γνωρίζουν,
- το παιδί ξοδεύει ιδιαίτερα μεγάλο χρονικό διάστημα στο Διαδίκτυο,
- το παιδί γρήγορα αλλάζει το παράθυρο που έχει ανοιχτό στην οθόνη του υπολογιστή του ή τον κλείνει τελείως καθώς μπαίνει ο γονιός στο δωμάτιο του,
- το παιδί λαμβάνει ανεξήγητα και ύποπτα δώρα, ιδιαίτερα ψηφιακά, όπως φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεφωνικές κάρτες, υπολογιστές ή λεφτά,

- το παιδί γίνεται επιθετικό, τρέχει μακριά από το σπίτι ή ξεκινάει κάποια εγκληματική δραστηριότητα

- οι συνήθειες καλλωπισμού του παιδιού ή οι συνήθειες υγιεινής αλλάζουν. Αλλαγές στο ντύσιμο έτσι ώστε να κρύβουν το παιδικό του σώμα ή να το κάνουν να εμφανίζεται μη ελκυστικό θα πρέπει να προσεχθούν **. (**http://www.dart.gov.gr/?q=node/28)

5.5 Συμβουλές για Παιδιά

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο Διαδίκτυο.
- Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο Διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.
- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο Διαδίκτυο.
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα.
- Μην εμπιστεύεστε ότι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι. (http://www.dart.gov.gr/?q=node/28)

5.6 Συμβουλές για Νέους

- Μη δίνετε σε κανέναν, ακόμη και στον καλύτερό σας φίλο, τον κωδικό πρόσβασης στο Διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τον κωδικό είναι οι γονείς σας.
- Μην απαντάτε σε ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεστε «άβολα».
- Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάσετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε.
- Αν αισθανθείτε άβολα την ώρα που συνομιλείτε μέσω chatroom, διακόψτε αμέσως τη συνομιλία.
- Αποφύγετε να στέλνετε τη φωτογραφία σας και τα προσωπικά στοιχεία σας μέσω Διαδικτύου σε άγνωστο.
- Σκεφθείτε πολύ καλά πριν αποφασίσετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο Διαδίκτυο. Ζητείστε την άποψη των γονιών σας σχετικά με αυτό το θέμα.
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με τον ¨διαδικτυακό σας φίλο». Ενημερώστε τους γονείς σας ή κάποιο άτομο που εμπιστεύεστε και φροντίστε αυτή η συνάντηση να γίνει σε δημόσιο χώρο.
- Αναπτύξτε κριτική διάθεση σε ότι διαβάζετε στο Διαδίκτυο. Μην εμπιστεύεστε αμέσως ότι δείτε.
- Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν «σερφάρετε» στο Internet.(http://www.dart.gov.gr/?q=node/28)

5.7 Συμβουλές για όσους αναζητούν Εργασία μέσω Διαδικτύου

- Ποτέ μην δίνετε κανένα προσωπικό στοιχείο που να μην σχετίζεται με τη δουλειά, όπως στοιχεία ταυτότητας, τον αριθμό φορολογικού μητρώου, τον αριθμό της πιστωτικής σας κάρτας, την ημερομηνία γέννησης και την οικογενειακή σας κατάσταση στο Διαδίκτυο, μέσω e-mail, από το τηλέφωνο, σε φαξ ή στο βιογραφικό σας.
- Να δημοσιεύσετε το βιογραφικό σας μόνον σε ιστοσελίδα εύρεσης εργασίας που εφαρμόζει πολιτική προστασίας προσωπικών

δεδομένων και επιτρέπει την πρόσβαση στα βιογραφικά μόνον σε πιστοποιημένα γραφεία εύρεσης εργασίας.

- Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη, επαγγελματία ή γραφείου εύρεσης εργασίας και μέσω δεύτερης πηγής ή του τηλεφωνικού καταλόγου και, στη συνέχεια, απευθυνθείτε στον εργοδότη απευθείας. Ο καλύτερος τρόπος να διασταυρώσετε τα στοιχεία ενός ενδεχόμενου εργοδότη είναι να επισκεφθείτε τα γραφεία της εταιρείας του, σε ώρες εργασίας.
- Εάν κάποιος ενδεχόμενος εργοδότης ή γραφείο εύρεσης εργασίας θελήσει να κάνει έλεγχο των στοιχείων σας, να το δεχθείτε μόνον αφού συναντηθείτε με τον εργοδότη στα γραφεία της εταιρείας, σε ώρες εργασίας.
- Να μην εμπιστεύεστε όσους σας ζητούν χρήματα εκ των προτέρων για να σας βρουν δουλειά.
- Ποτέ να μην δεχθείτε να πληρώσετε για "αποκλειστικές" πληροφορίες για θέσεις εργασίας ή για να πάρετε κάποια συγκεκριμένη θέση. Εάν πληρώσετε για υπηρεσίες εύρεσης εργασίας, μην δώσετε τα στοιχεία της πιστωτικής σας κάρτας ή του τραπεζικού σας λογαριασμού και μην κάνετε καμία συναλλαγή σε μετρητά με οποιονδήποτε επαγγελματία ή γραφείο ευρέσεως εργασίας, εκτός εάν το κάνετε αυτοπροσώπως, επιτόπου.
- Να αξιολογείτε προσεκτικά τα στοιχεία επαφής που δίνονται σε αγγελίες εργασίας ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες, κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας ή εάν η περιοχή ή ο ταχ. κώδικας δεν είναι παντού τα ίδια.
- Να πληκτρολογείτε τις διευθύνσεις των ιστοσελίδων (URL) στο browser αντί να χρησιμοποιείτε links όταν ελέγχετε τις πηγές των θέσεων εργασίας και να προσέχετε ακόμη μια νέα μορφή απάτης που μοιάζει με το phishing και λέγεται "pharming" (παραπλάνηση) και η οποία κάνει ανακατεύθυνση των χρηστών από τις νόμιμες τοποθεσίες Web σε απομιμήσεις, με σκοπό την κλοπή προσωπικών στοιχείων.

- Να δημιουργήσετε διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν λογαριασμό για όλες τις μη προσωπικές επικοινωνίες.
- Αν και δεν υπάρχει καμία μέθοδος να εντοπίσετε τις ψεύτικες αγγελίες εργασίας που να προστατεύει απολύτως από τις απάτες, να προσέχετε εάν υπάρχουν πολλά ορθογραφικά λάθη και άλλες ανακρίβειες, καθώς αυτό αποτελεί συνηθισμένη ένδειξη.
- Να εμπιστεύεστε το ένστικτό σας και να δίνετε ιδιαίτερη προσοχή όταν απευθύνεστε σε εταιρείες που βρίσκονται έξω από τη χώρα σας.
- Εάν κάποια ευκαιρία υπόσχεται υπερβολικά πολλά ή κάτι άλλο δεν φαίνεται σωστό, μάλλον πρόκειται για παραπλανητικό μήνυμα. • (http://www.dart.gov.gr/?q=node/28)

5.8 Συμβουλές για Δημιουργούς Blog

Οι ακόλουθες συμβουλές είναι ένα καλό σημείο εκκίνησης για παιδιά που ενδιαφέρονται να δημιουργήσουν ημερολόγια blog.

- Μην παρέχετε ποτέ προσωπικές πληροφορίες όπως επώνυμο, πληροφορίες επικοινωνίας, διεύθυνση κατοικίας, αριθμούς τηλεφώνων, όνομα σχολείου, ηλεκτρονική διεύθυνση, επώνυμο φίλων ή συγγενών, όνομα άμεσης επικοινωνίας, ηλικία ή ημερομηνία γέννησης.
- Μην δημοσιεύετε ποτέ προκλητικές φωτογραφίες του εαυτού σας ή κάποιον άλλο και βεβαιωθείτε πως όποια φωτογραφία δημοσιεύεται δεν αποκαλύπτει κάποιες προσωπικές πληροφορίες.
- Επίσης να θυμάστε να κοιτάτε πάντα στο background της φωτογραφίας.
- Θεωρείστε πως ότι δημοσιεύεται στο Διαδίκτυο είναι μόνιμο. Οποιοσδήποτε μπορεί στο Διαδίκτυο να εκτυπώσει ένα ημερολόγιο ή να το αποθηκεύσει στον υπολογιστή του.
- Χρησιμοποιήστε τοποθεσίες παροχής ημερολογίων blog με ξεκάθαρους όρους χρήσης, και βεβαιωθείτε πως μπορείτε να προστατέψετε με κωδικό πρόσβασης και τα ενεργά ημερολόγια blog

και όχι μόνο τους λογαριασμούς. (Εάν όχι, είναι καλύτερο να θεωρήσετε πως οποιοσδήποτε μπορεί να το δει).

- Αποφεύγετε να υπερβάλετε ή να ανταγωνίζεστε με άλλους δημιουργούς ημερολογίων (bloggers).
- Διατηρήστε τα ημερολόγια blog θετικά και μην τα χρησιμοποιείτε για να δυσφημήσετε ή να επιτεθείτε σε άλλους. (http://www.dart.gov.gr/?q=node/28)

5.9 Ασφάλεια μέσω Λογιστικών Φίλτρων

Ένα φίλτρο είναι ένα πακέτο λογισμικού το οποίο μπορεί να αποκλείσει την προσπέλαση σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο. Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από το πόσο ανανεωμένες είναι οι λίστες με τους απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό περιεχόμενο. Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να αποκλείει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε περιεχόμενο με βία η ρατσισμό. Κάποιοι από τους παροχείς υπηρεσιών Ιντερνέτ έχουν ήδη εγκαταστήσει λογισμικά φίλτρα στις υπηρεσίες τους. Σε αυτή την περίπτωση δεν είναι αναγκαία η εγκατάσταση άλλων φίλτρων. Στο διαδίκτυο επίσης μπορείτε να βρείτε δωρεάν φίλτρα στις **διευθύνσεις http://www.wiasa.org, http://childsafe.com/index.html,http://www.microweb.com/pepsite/Software/filters.html. Ενδεικτικά**, επίσης στην ιστοσελίδα **http://www.sip-bench.eu** μπορείτε να βρείτε ιστοχώρους φίλτρων που αξιολογήθηκαν από το Ευρωπαϊκό πρόγραμμα SIP-BENC.
(http://www.dart.gov.gr/?q=node/28)

5.10 Τι να κάνετε αν πέσετε Θύματα Απάτης

Βήμα 1: Κλείστε όλους τους λογαριασμούς που επηρεάζονται

Επικοινωνήστε με την αρχική εταιρεία ή τον οργανισμό εάν πιστεύετε πως δώσατε ευαίσθητες πληροφορίες σε άγνωστη πηγή, η οποία προσποιήθηκε πώς ήταν η πραγματική εταιρεία ή οργανισμός. Εάν επικοινωνήσετε αμέσως με την πραγματική εταιρεία, ίσως μπορέσουν να περιορίσουν τη ζημιά προς εσάς και προς τους υπολοίπους. Κατόπιν:

- **Επικοινωνήστε με το τμήμα ασφάλειας ή απάτης** κάθε τράπεζας ή πιστωτικού ιδρύματος με το οποίο συνεργάζεστε, συμπεριλαμβανομένων των εταιριών πιστωτικών καρτών, οργανισμών κοινής ωφέλειας, εταιρειών παροχής υπηρεσιών Internet και άλλων τοποθεσιών όπου χρησιμοποιείτε την πιστωτική σας κάρτα, για κάθε ύποπτη πρόσβαση ή άνοιγμα λογαριασμού. (http://www.dart.gov.gr/?q=node/28)

- **Στη συνέχεια**, στείλτε μία επιστολή και κρατήστε και ένα αντίγραφο για εσάς. Όταν ανοίξετε νέους λογαριασμούς χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης, όχι δηλαδή το γένος της μητέρας σας και έναν νέο αριθμό λογαριασμού. (http://www.dart.gov.gr/?q=node/28)

Βήμα 2: Αλλάξτε τους κωδικούς πρόσβασης σε όλους σας τους λογαριασμούς στο Internet.

Όταν αλλάξετε τους κωδικούς ή όταν ανοίξετε νέους λογαριασμούς, χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης

Βήμα 3: Προσθέστε ειδοποίηση απάτης στους πιστωτικούς λογαριασμούς

Στις Ηνωμένες Πολιτείες, μπορείτε να επικοινωνήσετε με αυτά τα τρία γραφεία υπηρεσιών πίστωσης:

- Equifax (800) 525-6285
- Experian (888) 397-3742

- TransUnion (800) 680-7289

Για κάθε γραφείο υπηρεσιών πίστωσης:

- **Ζητήστε ένα αντίγραφο της αναλυτικής κατάστασης του λογαριασμού σας** (τα θύματα κλοπής στοιχείων ταυτότητας μπορούν να λάβουν αντίγραφα των αναλυτικών καταστάσεων των πιστωτικών τους λογαριασμών δωρεάν) και ζητήστε να μην γίνει καμία νέα πίστωση του λογαριασμού χωρίς την έγκρισή σας. (http://www.dart.gov.gr/?q=node/28)
- **Βεβαιωθείτε πως ο λογαριασμός σας διαθέτει** επισήμανση "ειδοποίησης απάτης" και "δήλωση θύματος" και επιμείνετε ώστε η προειδοποίηση να παραμείνει ενεργή για εφτά χρόνια το μέγιστο.
- **Στείλτε τις αιτήσεις γραπτώς** και φυλάξτε αντίγραφα για εσάς.
- **Εξετάστε προσεκτικά τις αναλυτικές καταστάσεις.** Ψάξτε για ερωτήσεις που δεν κάνατε, λογαριασμούς που δεν ανοίξατε και ανεξήγητες χρεώσεις.

Εκτός των Η.Π.Α., επικοινωνήστε με την τράπεζά σας ή το χρηματοπιστωτικό ίδρυμα και ζητήστε από κάποιον πληροφορίες για τον αρμόδιο οργανισμό ή την υπηρεσία. • (http://www.dart.gov.gr/?q=node/28)

Βήμα 4: Επικοινωνήστε με τις αρμόδιες αρχές

Εντός των Ηνωμένων Πολιτειών, επικοινωνήστε με την Federal Trade commission (FTC- Ομοσπονδιακή επιτροπή εμπορίου).

- **Καταθέστε μια καταγγελία.** Εάν πέσατε θύμα οποιουδήποτε είδους κλοπής ταυτότητας, μπορείτε να το καταγγείλετε τηλεφωνώντας χωρίς χρέωση στη γραμμή Identity Theft Hotline της FTC, (877) ID-THEFT ή (877) 438-4338. Ειδικοί σύμβουλοι θα σας παράσχουν καθοδήγηση για το πώς μπορείτε να αντιμετωπίσετε τυχόν προβλήματα που μπορεί να προκύψουν σε σχέση με την πιστοληπτική σας ικανότητα λόγω της κλοπής της ταυτότητάς σας.• (http://www.dart.gov.gr/?q=node/28)
- **Κάντε λήψη και τυπώστε την ένορκη βεβαίωση κλοπής ταυτότητας της FTC.** Συμπληρώστε την και στείλτε την σε όλα τα οικονομικά ιδρύματα που ενέχονται, για να μειώσετε τις ευθύνες σας για χρέη που προέρχονται από αυτούς που έκλεψαν την ταυτότητά σας. Η υπόθεση σας θα καταχωριστεί στην εθνική βάση δεδομένων της FTC "Consumer Sentinel" για τις υποθέσεις κλοπής ταυτοτήτων, που βοηθά τις αρχές ασφαλείας να εντοπίσουν εγκληματικά κυκλώματα και να συλλάβουν τους κλέφτες. • (http://www.dart.gov.gr/?q=node/28)
- **Κάντε αναφορά στο τοπικό αστυνομικό τμήμα.** Ζητήστε αντίγραφο της αναφοράς

της αστυνομίας για να ενημερώσετε την τράπεζα, την εταιρεία της πιστωτικής κάρτας και τους υπόλοιπους πιστωτές ότι είστε θύμα απάτης και όχι καταχραστής της πίστωσης.

Ανάλογα με τον τόπο διαμονής σας, ίσως χρειαστεί να καταθέσετε αναφορά στην επικράτεια όπου διαπράχθηκε το έγκλημα. (http://www.dart.gov.gr/?q=node/28)

Βήμα 5: Να καταχωρίζετε και να αποθηκεύετε τα πάντα

Καθώς ολοκληρώνετε τα απαραίτητα βήματα για να διασαφηνίσετε το πρόβλημα, πάντα να δημιουργείτε εκτυπωμένα αντίγραφα των εγγράφων για εσάς περιλαμβανομένων των ηλεκτρονικών μηνυμάτων, των γραπτών απαντήσεων και να τηρείτε αρχείο των τηλεφωνικών σας κλήσεων, τα οποία θα πρέπει να φυλάτε σε κάποιο ασφαλές μέρος. http://www.dart.gov.gr/?q=node/28

Για τηλεφωνικές ή κατ' ιδίαν συνομιλίες, επανέλθετε με επιστολές επιβεβαίωσης προς τους οργανισμούς και φυλάξτε ένα αντίγραφο. Αναφέρετε στην επιστολή ότι ειπώθηκε κατά τη συνομιλία και καταγράψτε κάθε στοιχείο που ακολουθεί και για το οποίο δεσμευτήκατε εσείς ή ο εκπρόσωπός σας κατά την συζήτηση. (http://www.dart.gov.gr/?q=node/28)

5.11 Εποπτικές Αρχές για την Προστασία του Διαδικτύου στην Ελλάδα

Οι αρχές που εποπτεύουν σε ζητήματα ασφαλείας του Διαδικτύου και των επικοινωνιών γενικότερα στην Ελλάδα είναι :

1. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία έχει ως αποστολή την εποπτεία τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο . (http://www.dart.gov.gr/?q=node/28)
2. Η Αρχή Διασφάλισης του Απορρήτου των επικοινωνιών (Α.Δ.Α.Ε.), σκοπός της οποίας είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο και
3. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), η οποία χορηγεί άδειες σε Παρόχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών

Διαδικτύου (ISP's), ενώ ρυθμίζει και ελέγχει τον τομέα των τηλεπικοινωνιών, εποπτεύοντας παράλληλα την τηλεπικοινωνιακή αγορά. • (http://www.dart.gov.gr/?q=node/28)

4. Η SafeLine.: Η SafeLine είναι μια Ανοικτή Γραμμή που δέχεται καταγγελίες για δικτυακούς τόπους ή άλλες διαδικτυακές υπηρεσίες
5. Η Δίωξη Ηλεκτρονικού Εγκλήματος.: Η Δίωξη Ηλεκτρονικού Εγκλήματος ερευνά υποθέσεις που έχουν σχέση με το Διαδικτυακό Έγκλημα.

(http://www.dart.gov.gr/?q=node/28)

ΥΠΟΚΕΦΑΛΑΙΟ 6: Χαρακτηριστικά Γνωρίσματα του Εγκλήματος στον Κυβερνοχώρο

6.1 Τα Χαρακτηριστικά Γνωρίσματα του Εγκλήματος στον Κυβερνοχώρο

Το ηλεκτρονικό έγκλημα φέρει ορισμένα χαρακτηριστικά .Επιγραμματικά μπορούμε να αναφέρουμε τα ποιοτικά χαρακτηριστικά αυτής της νέας μορφής εγκλήματος που το διαφοροποιούν από το συμβατικό έγκλημα .

Ποιοτικά χαρακτηριστικά:

- Η δομή του διαδικτύου και ο παγκόσμιος χαρακτήρας του
- Η δυσκολία εύρεσης του δράστη
- Η ανωνυμία
- Το τεράστιο πλήθος των παράνομων πληροφοριών
- Ο μεγάλος αριθμός των αποδεκτών –χρηστών
- Ευκολία πρόσβασης
- Ευκολία διάπραξης (δομή των ευκαιριών) εγκληματικής δράσης
- Ταχύτητα εγκληματικής δράσης
- Δυσκολία αντίδρασης από τις διωκτικές αρχές
- Η αδυναμία ρύθμισης του διαδικτύου

(Μυλωνόπουλος, 2008)

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη λόγων των χαρακτηριστικών που την διακρίνουν . Είναι γεγονός ότι το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων χωρίς να το αντιληφθεί αρκετές φορές ακόμα και το ίδιο το θύμα.

(Μυλωνόπουλος, 2008)

Λόγω της δυσκολίας διερεύνησης το ηλεκτρονικό έγκλημα έχει εισάγει νέους νομοθετικούς προβληματισμούς καθώς καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος , η διερεύνηση και ο εντοπισμός του δράστη. Συγκεκριμένα υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην (Α) χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες. Οι «εγκληματίες του Κυβερνοχώρου» πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα (e-mail) με ψευδή στοιχεία. (Ζαννή, 2005)

Η εισβολή σε κάποιο υπολογιστικό σύστημα και η διάπραξη της απάτης είναι πολύ εύκολη και δεν απαιτεί πάντα εξειδικευμένες γνώσεις ,ενώ τα ίχνη που αφήνει είναι μόνο ψηφιακά. (Ζαννή, 2005)

Επιπλέον το διαδίκτυο προσφέρει την δυνατότητα επικοινωνίας μέσω του ηλεκτρονικού ταχυδρομείου ,των δωματίων συζητήσεων και των ομάδων ειδήσεων όπου επιτρέπουν σε πολλά άτομα να επικοινωνούν γρήγορα .Αυτή η εξέλιξη της επικοινωνίας έδωσε τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms.

Επιπλέον το έγκλημα είναι διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους. (Ζαννή, 2005)

Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία).

Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνο κράτους είναι σπάνια. (Ζαννή, 2005)

Τέλος η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι αδιερεύνητο, από ότι το κοινό έγκλημα . (Ζαννή, 2005)

ΥΠΟΚΕΦΑΛΑΙΟ 7: Η Παρέκκλιση στον Κυβερνοχώρο σε Παγκόσμιο Επίπεδο

7.1 Μία Παγκόσμια Προσέγγιση της Παρέκκλισης στον Κυβερνοχώρο

Η παρέκκλιση στον κυβερνοχώρο είναι ένα παγκόσμιο φαινόμενο και μπορεί εύκολα να διασχίσει τα εθνικά σύνορα με τον ένοχο να βρίσκεται σε μια χώρα εξαπατώντας ή καταστρέφοντας με οποιονδήποτε άλλον τρόπο το θύμα που βρίσκεται σε μια άλλη χώρα .Κλασική περίπτωση είναι η νιγηριανή απάτη στο πλαίσιο της οποίας κλάπηκαν πέντε δισεκατομμύρια δολάρια από τους Αμερικανούς πολίτες από τις αρχές τις δεκαετίας του ΄80 έως το 1996 .Αυτή η μορφή απάτης συνεχίζει και ως σήμερα ,αν και σε μικρότερο βαθμό από ότι στο παρελθόν .Στο πλαίσιο αυτής της απάτης οι δράστες αποστέλλουν ένα e-mail σε ένα μεγάλο αριθμό Αμερικανών πολιτών ,ζητώντας τους να στείλουν μερικές χιλιάδες δολάρια με την δελεαστική αλλά ψευδή υπόσχεση ότι θα κερδίσουν εκατομμύρια δολάρια από την επένδυση τους σε ένα καινούργιο χρυσορυχείο σε κάποια χώρα της Αφρικής .Επίσης σε μια άλλη περίπτωση ,μια ομάδα ναρκομανών στον Καναδά έκλεβαν συστηματικά αριθμούς πιστωτικών καρτών ,αριθμούς κοινωνικής ασφάλισης και άλλες προσωπικές πληροφορίες και στη συνέχεια μέσω της συνομιλίας κειμένου πουλούσαν την λεία τους σε

εγκληματίες σε μακρινές χώρες όπως η Ρουμανία ,η Αυστρία και η Αίγυπτος .(Thio,2008)

Η απάτη μέσω του διαδικτύου ,αποτελεί την πιο συνηθισμένη μορφή παρέκκλισης στο διαδίκτυο παγκοσμίως. Όπως δείχνει ο πίνακας η απάτη αποτελεί το 26% όλων των μορφών της παρέκκλισης στο διαδίκτυο που έχουν αναφερθεί στην international web police .Ένα άλλο σημαντικό στοιχείο για την παρέκκλιση στο διαδίκτυο διεθνώς είναι η τεράστια αύξηση των περιστατικών .Σύμφωνα με την ίδια αστυνομική αρχή το 1993 είχαν αναφερθεί μόνο 640 εγκλήματα στο διαδίκτυο αλλά ο αριθμός τους το 2002 είχε φτάσει στα 1.351.897.(Thio,2008)

7.2 Παράγοντες Αύξησης Εγκληματικότητας στο Διαδίκτυο

Η αύξηση των περιστατικών εγκληματικότητας στο διαδίκτυο αποδίδεται σε δύο σημαντικούς παράγοντες . Ο ένας παράγοντας , είναι η πρωτοφανής αύξηση της χρήσης ηλεκτρονικών υπολογιστών και του διαδικτύου κατά τη διάρκεια της τελευταίας δεκαετίας .Ο άλλος παράγοντας είναι η σχετική έλλειψη εφαρμογής των νόμων κατά της εγκληματικότητας στο διαδίκτυο σε όλο τον κόσμο .Μεγαλύτερο πρόβλημα αντιμετωπίζουν στην Ρωσία ,στις χώρες της Ανατολικής Ευρώπης και σε άλλες χώρες με εκτεταμένη ανεργία στις οποίες πολλοί νέοι ,ευφυΐες στους ηλεκτρονικούς υπολογιστές ,στρατολογούνται από εγκληματικές ομάδες μέσω των δωματίων ανοιχτής επικοινωνίας στο διαδίκτυο .Στην Νότια Κορέα ένα συνδικάτο του οργανωμένου εγκλήματος με σκοπό και να στρατολογήσει έτσι τους πιο πολλά υποσχόμενους από τους διαγωνιζόμενους χρησιμοποίησε κάποτε ένα δωμάτιο ανοιχτής επικοινωνίας για να διοργανώσει ένα ψεύτικο διαγωνισμό χάκερς .Αναπόφευκτα τα περιστατικά εγκληματικότητας των χάκερς σε αυτή την χώρα αυξήθηκαν από 449 που ήταν το 2000 σε 14.065 το 2003 .Εκτός από τη χαλαρή εφαρμογή των νόμων σε αυτές τις χώρες και την έλλειψη διεθνούς συνεργασίας για τη σύλληψη των εγκληματιών στον κυβερνοχώρο διευκολύνει την διαφυγή και την ατιμωρησία τους .Το 2000 ,για παράδειγμα ένας άντρας στις Φιλιππίνες δημιούργησε τον ιό “I love you”που προκάλεσε ζημιές εκατομμυρίων δολαρίων σε διάφορες χώρες

,αλλά διέφυγε τη σύλληψη .Δεν διώχθηκε ποινικά από την χώρα του λόγω έλλειψης των κατάλληλων νόμων εκεί αλλά ούτε εκδόθηκε στις Ηνωμένες πολιτείες για να δικαστεί λόγω της έλλειψης συνεργασίας ανάμεσα στους φορείς της εφαρμογής του νόμου των δύο χωρών .(Thio,2008)

ΠΟΣΟΣΤΑ ΤΩΝ ΜΟΡΦΩΝ ΠΑΡΕΚΚΛΙΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΠΑΓΚΟΣΜΙΩΣ

Απάτη	26%
Παιδική πορνογραφία	17%
Παραφύλαξη	11%
Απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου	9%
Ενόχληση	9%
Εισβολή με ιό	9%
Παραβίαση της αποκλειστικότητας	4%
Τρομοκρατία	3%
Απάτη μέσω ηλεκτρονικών συνομιλιών	2%
Άλλα	10%
(Συνολικά)	100%

(Thio, 2008 σελ.583)

ΥΠΟΚΕΦΑΛΑΙΟ 8: Νομοθεσία

8.1 Εισαγωγή Νομοθεσίας

8.1.1 Προβλήματα ρύθμισης και νομοθεσίας

Λόγω της γρήγορης εξέλιξης της τεχνολογίας και της πληροφορικής ,η νομοθεσία δεν μπορεί να αντιμετωπίσει άμεσα τις συνέπειες όλης αυτής της ανάπτυξης . Σε γενικές γραμμές οι νομοθέτες όσο και οι μηχανισμοί καταστολής δεν είναι κατάλληλα εξοπλισμένοι για να καταπολεμήσουν την εξάπλωση του παράνομου περιεχομένου και την έκρηξη της πειρατείας. Αν και δεν υπάρχουν πολλά στοιχεία σε παγκόσμιο επίπεδο, ένα παράδειγμα αρκεί για να δείξει τη σοβαρότητα του προβλήματος: σύμφωνα με στοιχεία της οργάνωσης Internet Watch Foundation , ο αριθμός των ιστοσελίδων με πορνογραφικό υλικό έχει αυξηθεί στο δέκα πενταπλάσιο στο διάστημα μεταξύ 1997 και 2005. Έχει γίνει λοιπόν επιτακτική ανάγκη και απαραίτητη η χάραξη μιας στρατηγικής σε ευρωπαϊκή κλίμακα . (Λάζος,2001)

8.1.2 Δικαιοδοσία στο Ίντερνετ

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει πρόσβαση από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. (Καρακώστας ,2001) Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

α) «Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε

περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε». (Καρακώστας,2001 σελ.65)

β)» Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.» (Καρακώστας,2001 σελ.65)

γ) «Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος». (Καρακώστας,2001 σελ.65)

δ) «Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.» (Καρακώστας,2001 σελ.65)

8.2 Θεσμικό Πλαίσιο στην Ελλάδα

Στην Ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών από άποψη ποινικού δικαίου. Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, με το Συμβούλιο της Ευρώπης, καθώς και με άλλους διεθνείς οργανισμούς για την αντιμετώπιση των σχετικών θεμάτων. (Ιγγλεζάκης,2006)

ΣΥΝΟΠΤΙΚΑ:

→ Ο Ν. 1805/88 αφορά εγκλήματα που διαπράττονται με ηλεκτρονικό υπολογιστή (computer crime).Στο βαθμό που τα προβλεπόμενα εγκλήματα (σχετικά άρθρα είναι τα 370Β, 370Γ, 386Α)διαπράττονται και σε περιβάλλον διαδικτύου, τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

→ Ο Ν. 2867/200 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις ο οποίος αντικατέστησε τον Ν.2246/94 για την οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

→ Ο Ν. 2774/99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με τον Ν. 2472/97 για την προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

→ Ο Ν. 2225/94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

→ Επίσης τέθηκε σε ισχύ το Π.Δ. 47/2005, από την ΑΔΑΕ (Αρχή Διασφάλισης Απορρήτου Επικοινωνιών) το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Αναμένεται να τεθεί σε ισχύ η συνθήκη που υπεγράφη στη Βουδαπέστη στις 23-11-2001, όπου υπάρχουν επεξηγήσεις και ρυθμίσεις γι όλα τα ηλεκτρονικά εγκλήματα. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

→ Με το Π.Δ. 100/2004 ιδρύθηκε το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στην Ελληνική Αστυνομία. Η υπηρεσία συνεργάζεται με άλλους συναρμόδιους φορείς (Interpol, Europol, Eurojust, Εισαγγελικές Αρχές, εκπροσώπους hotline γραμμών κ.λ.π.) για την καταπολέμηση του ηλεκτρονικού εγκλήματος και έχει να επιδείξει σημαντικό έργο.
(http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

8.2.1 Νομοθεσία –Ελληνικό Δίκαιο- Αντιμετώπιση Ηλεκτρονικής Εγκληματικότητας

Η αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, ανάλογα με τη μορφή που αυτή λαμβάνει, μπορεί να γίνει από το Ελληνικό δίκαιο συνδυάζοντας διάσπαρτες διατάξεις της κείμενης νομοθεσίας. Σε αυτές ανήκουν οι

διατάξεις του Ποινικού Κώδικα περί απάτης με τη χρήση υπολογιστή ,περί αθέμιτης πρόσβασης σε συστήματα πληροφοριών, υποκλοπής και παραβίασης απορρήτων, η ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (ν.2472/1997 όπως τροποποιήθηκε με το ν.3625/2007, ν. 3471/2006), η νομοθεσία περί διασφάλισης του απορρήτου των επικοινωνιών (ν. 3674/2008), οι κανονιστικές αποφάσεις διοικητικών αρχών όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)και ούτω καθεξής. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

8.2.1.1 Ποινική Προστασία του απορρήτου

Η διαδικτυακή εγκληματικότητα, στο μέτρο που οδηγεί σε παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, παραβίαση επαγγελματικών απορρήτων ή παράνομη αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή, τιμωρείται και από τα άρθρα 370Α και 370Β του Ποινικού Κώδικα, που προβλέπουν αντίστοιχες ποινές φυλάκισης κατά των δραστών . Πρόσφατα, ο νόμος 3674/2008 ψηφίστηκε για να ενισχύσει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, θεσπίζοντας ειδικές υποχρεώσεις του παρόχου υπηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της ΑΔΑΕ. (Λάζος,2001)

8.2.1.2 Ποινική προστασία των προσωπικών δεδομένων

«Στην (ποινική) προστασία της ιδιωτικότητας και των προσωπικών δεδομένων αποσκοπούν οι σχετικές διατάξεις του Ν. 2472/97. Το άρθρο 22 του Ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα προβλέπει ποινικές ευθύνες των υπεύθυνων επεξεργασίας για τη μη τήρηση των υποχρεώσεών τους από το νόμο (παράλειψη γνωστοποίησης αρχείων, διατήρηση αρχείου με ευαίσθητα δεδομένα χωρίς άδεια, διασύνδεση αρχείων χωρίς γνωστοποίηση και άδεια) . Τέτοιες πράξεις ηλεκτρονικής παραβατικότητας μπορούν ακόμα να συνιστούν πλαστογραφία, εξύβριση, δυσφήμιση, προσβολή της νομοθεσίας περί απορρήτου, του ν. 2121/1993 περί πνευματικής

ιδιοκτησίας ή του ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών». (Λάζος,2001 σελ.143)

8.2.1.3 Ποινική κύρωση της παραβίασης πνευματικής ιδιοκτησίας

«Την κύρια πηγή του δικαίου της πνευματικής ιδιοκτησίας στην Ελλάδα αποτελεί ο Νόμος 2121/1993 με τίτλο «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα.» Η Ελληνική Νομολογία ενισχύει και αυτή με τη σειρά της, την μάχη κατά της παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, αν και κυρίως εστιάζεται σε θέματα συλλογικής διαχείρισης πνευματικών δικαιωμάτων (π.χ. 687/2003 Απόφαση Μονομελούς Πρωτοδικείου Τρικάλων) και ραδιοτηλεοπτικής φύσεως διενέξεων (π.χ. 1404/2002 Απόφαση του Συμβουλίου της Επικρατείας).Στην Ευρώπη ισχύει η Οδηγία 93/98 περί εναρμονίσεως της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και ορισμένων συγγενών δικαιωμάτων , η Οδηγία 2001/29 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας καθώς και ο Κανονισμός 1383/2003 για την παρέμβαση των τελωνειακών αρχών έναντι εμπορευμάτων που είναι ύποπτα ότι παραβιάζουν ορισμένα δικαιώματα πνευματικής ιδιοκτησίας και για τα μέτρα που πρέπει να λαμβάνονται έναντι των εμπορευμάτων που διαπιστώνεται ότι παραβιάζουν παρόμοια δικαιώματα». (Λάζος,2001 σελ.145)

8.3 Παράνομη «παρέμβαση» στο σύστημα και στα δεδομένα

8.3.1 Νομοθετήματα για Hacking

Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:

1.Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών,

μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173 - CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεση μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

Απάτη μέσω του Διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών . (Ιγγλεζάκης,2006)

Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του διαδικτύου . Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων

κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους» καθώς και από άλλα νομοθετήματα. Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο. (Ιγγλεζάκης,2006)

8.3.2 Νομοθετήματα για την Προστασία Ανηλίκων

Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων-Προστασία από παράνομο και βλαβερό περιεχόμενο.

Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπισης αυτού του είδους εγκληματικότητας.

1. Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ιντερνέτ.(http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

2. Η Σύσταση με αριθμό 98/560/ΕΚ όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης .

(http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

3. Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

4. Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά

μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων.

(http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

5. Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

6. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών. (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

7. Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ.

(http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

8. Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ και

9. Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (Ιντερνέτ) μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα. . (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp)

Ένα ακόμα ζήτημα που τίθεται σχετικά με την χρήση του διαδικτύου από τους ανήλικους είναι η πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα. Είναι γνωστό ότι οποιαδήποτε συναλλαγή με ανήλικο είναι άκυρη και μπορεί να επισύρει ποινή για τον αντισυμβαλλόμενο εφόσον το περιεχόμενό της δεν απευθύνεται σε παιδία και εφήβους. Στην περίπτωση όμως των ηλεκτρονικών συναλλαγών δεν είναι πάντα δυνατή η εξακρίβωση των στοιχείων του καταναλωτή. Για την προστασία των προμηθευτών που

δραστηριοποιούνται μέσω κάποιας ιστοσελίδας είναι απαραίτητη η αναγραφή στους όρους χρήσης του site ότι δεν επιτρέπονται οι συναλλαγές με ανηλίκους και ότι η ιστοσελίδα δεν φέρει καμία ευθύτητα πράγματα άλλαξαν το έτος 2002 όταν συμπληρώθηκε ο εκσυγχρονισμός των εγκλημάτων του Ποινικού Κώδικα σχετικά με τη γενετήσια ζωή. Είναι μάλιστα αξιοσημείωτο ότι ο σχετικός νόμος (3064/2002) ψηφίστηκε από όλα τα κόμματα. (Λάζος,2001)

8.3.3 Γενικά Νομοθετήματα –Ευρωπαϊκή Ένωση

Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος . Στην Ευρωπαϊκή Ένωση ισχύουν :

1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας, (http://www.e-crime.gr/nomothesia.htm)

2. Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.(http://www.e-crime.gr/nomothesia.htm)

3. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής. (http://www.e-crime.gr/nomothesia.htm)

4. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων. (http://www.e-crime.gr/nomothesia.htm)

5. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων . (http://www.e-crime.gr/nomothesia.htm)

6. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος. (http://www.e-crime.gr/nomothesia.htm)

7. Το Σχέδιο Δράσης με αριθμό 97/C 251/01για την καταπολέμηση του οργανωμένου εγκλήματος . (http://www.e-crime.gr/nomothesia.htm)

8.4 Άρθρα- Προεδρικά Διατάγματα-Νόμοι-Αποφάσεις -Συνέδρια

8.4.1 Άρθρα Ποινικού Κώδικα

- Άρθρο 348Α - Πορνογραφία ανηλίκων
- Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
- Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.
- Άρθρο 370Γ - Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.
- Άρθρο 386Α - Απάτη με υπολογιστή.

(http://www.e-crime.gr/nomothesia.htm)

8.4.2 Νόμοι

- Ν. 2225/94 – «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»

- Ν. 2472/97 και 2774/99 – «Περί προσωπικών δεδομένων»
- Ν. 2472/1997 – «Για την προστασία των προσωπικών δεδομένων στο Διαδίκτυο»
- Ν. 2774/1999 – «Για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
- Ν. 2867/2000 - «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών»
- Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»
- Ν. 2225/1994 όπως τροπ. Με Ν. 3115/2003 – «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» -
- Ν. 3411/2006 – «Περί ηλεκτρονικών επικοινωνιών».

(http://www.e-crime.gr/nomothesia.htm)

8.4.3 Προεδρικά Διατάγματα

- Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας»
- Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές»
- Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. (http://www.e-crime.gr/nomothesia.htm)

8.4.4 Οδηγίες Ευρωπαϊκής Ένωσης

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision -ONP). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού

εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). (http://www.e-crime.gr/nomothesia.htm)

- Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών. (http://www.e-crime.gr/nomothesia.htm)

8.4.5 Διεθνείς Συμβάσεις

- Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας

- Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001

- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948

- Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ) (http://www.e-crime.gr/nomothesia.htm)

8.4.6 Αποφάσεις

- Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων». (http://www.e-crime.gr/nomothesia.htm)

- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr» (http://www.e-crime.gr/nomothesia.htm)

- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (http://www.e-crime.gr/nomothesia.htm)

8.4.7 Ανακοινώσεις

- Ανακοίνωση Επιτροπής COM/2001/0298

Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών. (http://www.e-crime.gr/nomothesia.htm)

- Ανακοίνωση Επιτροπής COM/2002/0152

Ανακοίνωση της Επιτροπής με αριθμό COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (Ιντερνετ)

μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα. (http://www.e-crime.gr/nomothesia.htm)

8.4.8 Προτάσεις

- Πρόταση απόφασης πλαισίου COM/2002/0173 - CNS 2002/0086

Πρόταση απόφασης πλαισίου για τις επιθέσεις κατά των συστημάτων πληροφοριών με αριθμό COM/2002/0173 - CNS 2002/0086

(http://www.e-crime.gr/nomothesia.htm)

- Πρόταση Κανονισμού 2003.0063

Πρόταση Κανονισμού 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών. (http://www.e-crime.gr/nomothesia.htm)

8.4.9 Συνέδρια

- Συνέδριο για το Ηλεκτρονικό έγκλημα

Συνέδριο για το Ηλεκτρονικό έγκλημα - Βουδαπέστη 23/11/2001 - Υπογραφή Συνθήκης. (http://www.e-crime.gr/nomothesia.htm)

ΜΕΡΟΣ Β': ΕΡΕΥΝΗΤΙΚΟ

ΚΕΦΑΛΑΙΟ 2- ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

2. ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

Στο κεφάλαιο αυτό παρουσιάζεται η μεθοδολογία της έρευνας, που αφορά τις απόψεις των ειδικών που σχετίζονται με το ηλεκτρονικό έγκλημα. Παρακάτω γίνεται αναφορά στον τύπο της έρευνας που χρησιμοποίησαν οι ερευνήτριες, τους στόχους και τους σκοπούς, τα δεοντολογικά ζητήματα που καθορίζουν την έρευνα καθώς και τη καταγραφή των προσωπικών τους εμπειριών κατά την διάρκεια της διεξαγωγής της έρευνας. Μέσω αυτής της πρωτότυπης έρευνας αισιοδοξούμε να δοθούν νέα ερεθίσματα για παραπάνω σκέψη, για ευρύτερη και αναλυτικότερη εμβάθυνση και ενασχόληση με το πρόβλημα της παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο.

2.1 Είδος έρευνας

Η ποιοτική έρευνα χρησιμοποιεί την μέθοδο της παρατήρησης και των συνεντεύξεων, όπου είναι η μη δομημένη, η ημι-δομημένη, η μη κατευθυντική συνέντευξη και η εστιασμένη συνέντευξη (Cohen & Manion, 1994). Η ημι- δομημένη συνέντευξη αποτελείται από συγκεκριμένες ερωτήσεις οι οποίες μπορούν να τροποποιηθούν ανάλογα με την κρίση του συνεντευκτή, ο οποίος προσπαθεί να τις διαμορφώσει όσο το δυνατόν καταλληλότερα προσαρμόζοντας τες κάθε φορά ανάλογα με τον συνεντευξιαζόμενο που έχει απέναντί του. Αν κάποια ερώτηση δεν γίνει κατανοητή από τον ερωτώμενο ο συνεντευκτής με την ευελιξία που τον διακατέχει θα πρέπει να την διατυπώσει διαφορετικά. Επιπλέον, απαιτείται αντικατάσταση ή ακόμη και αφαίρεση κάποιας ερώτησης αν θεωρηθεί

ακατάλληλη για κάποιο συγκεκριμένο ερωτώμενο. (Ιωσηφίδης & Σπυριδάκης,2006)

Κύριο χαρακτηριστικό της ποιοτικής έρευνας είναι ο τρόπος διεξαγωγής της και η μορφή της. Πιο συγκεκριμένα, η ποιοτική έρευνα παρέχει στην συζήτηση, δίνοντας επιπλέον την δυνατότητα στον ερευνητή να έρθει σε άμεση επαφή με τον συνεντευξιαζόμενο, επιτρέποντας την εις βάθους κατανόηση των όσων έχουν ειπωθεί (Cohen & Manion, 1994). Όλες οι μέθοδοι απαιτούν την ανάπτυξη της επαφής για την υλοποίηση των στόχων, μεταξύ των ατόμων και του ερευνητή . Αυτός είναι και ο κύριος λόγος όπου ένας ερευνητής επιλέγει να χρησιμοποιήσει την ποιοτική μέθοδο για την έρευνά του, καθώς του παρέχει την δυνατότητα της δημιουργίας μιας πιο ισχυρής σχέσης εμπιστοσύνης με τα μέλη του δείγματός του. Στόχος του ερευνητή σε συνέντευξη είναι η κατανόηση των βιωμάτων και των συναισθημάτων από τα οποία διακατέχεται την συγκεκριμένη στιγμή ο συνεντευξιαζόμενος. . (Ιωσηφίδης & Σπυριδάκης,2006)

Ένα από τα κύρια χαρακτηριστικά της ποιοτικής έρευνας είναι ότι βασίζεται σε μικρό αριθμό περιπτώσεων με σκοπό την καταγραφή των απόψεων και αντιλήψεων των ερωτώμενων για το συγκεκριμένο θέμα που διερευνάται αλλά και την ανεύρεση μέσων αντιμετώπισης του φαινόμενου. Ο ερευνητής προσπαθεί να διαμορφώσει μια πιο πλήρη εικόνα του φαινομένου στηριζόμενος στα λεγόμενα των συνεντευξιαζόμενων. (Κυριαζή, 1999).

Η ποιοτική έρευνα θεωρήθηκε καταλληλότερη από τις ερευνήτριες διότι τόσο το θέμα όσο και ο σκοπός της έρευνας απαιτούσαν την ιδιαίτερη επαφή και ευελιξία με τους συνεντευξιαζόμενους, διότι αυτός ο τρόπος έρευνας θα οδηγήσει τις ερευνήτριες σε πιο εμπεριστατωμένα συμπεράσματα.

2.1.1 Στόχοι-Σκοπός έρευνας

Μια έρευνα μπορεί να ασχολείται με παραπάνω από έναν σκοπό, καθώς επίσης ο σκοπός αυτός να αλλάζει κατά την διεξαγωγή της έρευνας. Επιπλέον η αποσαφήνιση του σκοπού και του στόχου της έρευνας είναι δυνατόν να εξυπηρετήσει στην σωστή ταξινόμηση των ερευνητικών ερωτημάτων. (Ιωσηφίδης & Σπυριδάκης,2006)

Σκοπός της παρούσας έρευνας είναι η διερεύνηση, η καταγραφή και η ανάλυση του φαινομένου στα ποιοτικά χαρακτηριστικά του, για την αποσαφήνιση του προβλήματος της παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο με όσο το δυνατόν ακριβέστερα και πληρέστερα στοιχεία σε αυτό το πρόβλημα που έχει πάρει διαστάσεις σε παγκόσμιο επίπεδο. Για αυτό το λόγο στόχος μας είναι η πρόληψη και η προστασία όλων μας από την ηλεκτρονική απάτη μέσω συμβουλών ,προτάσεων και υποδείξεων .Η ραγδαία εξέλιξη ενός σχετικά νέου φαινομένου για την ελληνική πραγματικότητα αποδείχτηκε κινητήριο έναυσμα για την περαιτέρω ερευνά του.

Οι επιμέρους στόχοι της έρευνας είναι οι εξής:

1. Η ανάδειξη του ισχύοντος νομικού καθεστώτος που επικρατεί στην Ελλάδα ως προς την παρεκκλίνουσα συμπεριφορά στο διαδίκτυο.
2. Η διερεύνηση των στάσεων ,των αντιλήψεων ,των εμπειριών και των προτάσεων επαγγελματιών που στελεχώνουν τις αρμόδιες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος καθώς και άλλων ειδικοτήτων όπως προγραμματιστές ,ψυχολόγοι κ.α .
3. Η καταγραφή των μορφών απάτης που παρουσιάζονται με μεγαλύτερη συχνότητα στον κυβερνοχώρο .
4. Η εξακρίβωση της ύπαρξης του φαινομένου της εγκληματικότητας στον κυβερνοχώρο.
5. Η καταγραφή των μέτρων που λαμβάνονται για την αντιμετώπιση του φαινομένου
6. Η καταγραφή προτάσεων και συμβουλών για την ασφάλεια των πολιτών έναντι της ηλεκτρονικής απάτης

2.2 Ερευνητικές Υποθέσεις

Από την αρχή ακόμη της έρευνας ο ερευνητής θα πρέπει να καθορίσει τα ερευνητικά του ερωτήματα, σύμφωνα με το θέμα, τους στόχους και τον σκοπό της έρευνάς του. Τα ερευνητικά ερωτήματα, στην ποιοτική έρευνα, μπορούν να διαφοροποιούνται κατά την διάρκεια της έρευνας και ανάλογα με την αλληλεπίδραση με το δείγμα (Mason, 1996).

Για να θεωρηθούν τα ερευνητικά ερωτήματα μιας έρευνας εύστοχα θα πρέπει να είναι σαφή ώστε να γίνονται εύκολα κατανοητά, συγκεκριμένα, να μπορούν να απαντηθούν, συλλέγοντας τα κατάλληλα δεδομένα, αλληλοσυνδεόμενα, έτσι ώστε να χαρακτηρίζονται ως αξιόλογα και όχι τετριμμένα ερωτήματα (Ιωσηφίδης & Σπυριδάκης,2006).

Τα ερευνητικά ερωτήματα των ερευνητριών στην συγκεκριμένη έρευνα διατυπώθηκαν ως εξής:

1. Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την Υπηρεσία από όπου εργάζεστε;
2. Πως φτάνουν τα θύματα σε εσάς και πως γίνεται η καταγγελία και αν μπορεί να τηρηθεί το απόρρητο;
3. Ποια μέτρα λαμβάνει η Υπηρεσία σας σχετικά με αυτό το φαινόμενο;
4. Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητας;
5. Ποιές οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

Από αυτά τα ερευνητικά ερωτήματα προέκυψαν οι ερωτήσεις της ημι-δομημένης συνέντευξης, οι οποίες είχαν το περιθώριο της εμπλουτισμού ή της αλλαγής τους κατά την διάρκεια της συνέντευξης. Επιπρόσθετα, μέσα από την βιβλιογραφική ανασκόπηση διαπιστώθηκε η πρωτοτυπία του θέματος αφού δεν έχει πιθανά διεξαχθεί παρόμοια έρευνα στο τμήμα Κοινωνικής Εργασίας του ΤΕΙ Πάτρας. Με την χρήση ημι- δομημένων συνεντεύξεων δόθηκε η δυνατότητα στα μέλη του δείγματος να παρουσιάσουν μέσα από την προσωπική εμπειρία και αφήγηση τις

δυσκολίες που αντιμετωπίζουν για την καταπολέμηση του Ηλεκτρονικού Εγκλήματος και να εκφράσουν την άποψή τους σχετικά με το νομοθετικό πλαίσιο που έγκειται του θέματος της Ηλεκτρονικής εγκληματικότητας.

2.3 Πληθυσμός -Δείγμα

Ο πληθυσμός ο οποίος αποτελεί το αντικείμενο της έρευνας είναι εκπρόσωποι φορέων-υπηρεσιών , οι οποίοι στελεχώνουν τις αρμόδιες υπηρεσίες, σύμφωνα με νομοθετικό διάταγμα, που τις κατατάσσει υπεύθυνες για την αντιμετώπιση της δίωξης ηλεκτρονικού εγκλήματος , αλλά και άλλων ειδικοτήτων όπως ψυχολόγοι και προγραμματιστές υπολογιστών.

Πιο συγκεκριμένα, οι συνεντευξιαζόμενοι που έλαβαν μέρος στην έρευνά μας ανήκαν στα ακόλουθα επαγγέλματα:

- Δυο (2) Αστυνομικοί της Δίωξης Ηλεκτρονικού Εγκλήματος
- Δυο (2) Ψυχολόγοι
- Δυο (2) Προγραμματιστές Υπολογιστών
- Μία (1) Νομικός
- Μία (1) Διδάσκουσα του ΑΠΘ

Οι υπηρεσίες – τόποι που επιλέχθηκαν για την διεξαγωγή των συνεντεύξεων, είναι οι εξής:

1. Γ.Α.Δ.Α – ΤΜΗΜΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
2. ΑΣΤΥΝΟΜΙΚΟ ΜΕΓΑΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ- ΤΜΗΜΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
3. Μ.Κ.Ο «ΑΛΛΗΛΕΓΓΥΗ»
4. ΑΣΤΥΝΟΜΙΚΟ ΜΕΓΑΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ-ΠΟΛΥΙΑΤΡΕΙΑ ΑΣΤΥΝΟΜΙΑΣ
5. ΕΛΛΗΝΙΚΗ ΑΝΟΙΧΤΗ ΓΡΑΜΜΗ ΓΙΑ ΤΟ ΠΑΡΑΝΟΜΟ ΠΕΡΙΕΧΟΜΕΝΟ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ (SAFE LINE)
6. Α΄ ΕΠΑΛ ΝΑΟΥΣΑΣ

2.4 Επιλογή εργαλείων έρευνας

Το εργαλείο που θεώρησαν οι ερευνήτριες αρμόδιο για την συλλογή των δεδομένων είναι η ημι-δομημένη συνέντευξη.

Οι λόγοι που επιλέχθηκε η ημι-δομημένη συνέντευξη βασίζεται κυρίως στην δυνατότητα που παρέχει το συγκεκριμένο είδος συνέντευξης ώστε να έχεις μια πιο άμεση επικοινωνία και όχι τυποποιημένη με τον συνεντευξιαζόμενο .Δημιουργείται ένα κλίμα εμπιστοσύνης και κατανόησης αφού πραγματοποιείται πρόσωπο με πρόσωπο και δίνει την δυνατότητα να κατανοήσει κανείς σε βάθος όσα του αφηγείται το άτομο ,κάτι το οποίο δεν είναι εφικτό να γίνει με άλλου είδους ερευνητικά εργαλεία, όπως αυτό του ερωτηματολογίου. Αυτό βοηθάει διότι προσφέρεται η δυνατότητα τροποποίησης της διερευνητικής κατεύθυνσης και συλλογής απαντήσεων με ενδιαφέρον. Με τις προφορικές απαντήσεις οι ερευνητές δεν έχουν τον φόβο της μετάλλαξης των νοημάτων των λεγόμενων του ερωτώμενου(Ιωσηφίδης & Σπυριδάκης,2006) .

Επιπρόσθετα προσφέρει ευελιξία και μπορεί να καλύψει ευρύτερα την θεματολογία, καθορίζεται από συγκεκριμένες ερωτήσεις όπου είναι δυνατόν η διάταξή τους να τροποποιηθεί ανάλογα με την αντίληψη του συνεντευκτή. Μέσω της ημι-δομημένης συνέντευξης υπάρχει η δυνατότητα διαφοροποίησης της ερώτησης ώστε να δοθούν επεξηγήσεις ή για κάποιο ερωτώμενο να μην συμπεριληφθεί ή να αντικατασταθεί (Ιωσηφίδης & Σπυριδάκης,2006).

Βασικές προϋποθέσεις για την επιτυχία της ημι-δομημένης συνέντευξης είναι το περιβάλλον που διεξάγεται, το απόρρητο και η εχεμύθεια .Ο ερευνητής θα πρέπει να κρατάει σημειώσεις και να προσέχει τα όσα εκφράζει ο ερωτώμενος ώστε να μην υπάρξουν ασαφή μηνύματα και να κατανοηθούν πλήρως όλες οι πληροφορίες που λαμβάνει από τον συνεντευξιαζόμενο . (Ιωσηφίδης & Σπυριδάκης,2006)

Οι συνεντεύξεις προϋποθέτουν προσεκτική προετοιμασία και διακανονισμούς για την διεξαγωγή τους και αυτό γιατί απαιτούν πολύ χρόνο και θεωρούνται χρονοβόρες.

Η συνέντευξη δεν αποτελεί εύκολο ερευνητικό εργαλείο συλλογής δεδομένων αλλά παρέχει την δυνατότητα συγκέντρωσης πλούσιου υλικού για την ολοκλήρωση της έρευνας. Τέλος η επιτυχία της συνέντευξης και η συλλογή των απαραίτητων πληροφοριών εξαρτάται κάθε φορά από την εμπειρία του ερευνητή και από τις ικανότητες του. (Ιωσηφίδης & Σπυριδάκης,2006)

2.5 Τόπος και χρόνος έρευνας

Ο τόπος διεξαγωγής της έρευνας πραγματοποιήθηκε στην Αθήνα και στην Θεσσαλονίκη, δύο πόλεις όπου παρουσιάζουν ενδιαφέρον ως προς την πολυμορφία των πληθυσμών τους. Αυτό συμβαίνει εξαιτίας των γεωγραφικών τους θέσεων και λόγω της ύπαρξης των αρμόδιων υπηρεσιών που στελεχώνονται στους αντίστοιχους νομούς των δύο μεγάλων πόλεων . Επίσης πραγματοποιήθηκαν δύο ακόμη συνεντεύξεις από ειδικούς στην περιοχή του Νομού Ημαθίας με αφορμή την ευκολότερη μας πρόσβαση λόγο του 2^{ου} Πανελλήνιου εκπαιδευτικού συνεδρίου Ημαθίας με θέμα «Ψηφιακές και Διαδικτυακές Εφαρμογές στην Εκπαίδευση» που πραγματοποιήθηκε στο 1^{ο} ΕΠΑΛ Νάουσας κατά την ίδια περίοδο συγγραφής της πτυχιακής μας.

2.6 Ζητήματα δεοντολογίας

Ένα από τα σημαντικότερα χαρακτηριστικά που πρέπει να λάβει υπόψη του κάθε επιστήμονας για τη διεξαγωγή μιας έρευνας, είναι η διασφάλιση της συνειδητής συναίνεσης του ατόμου για συμμετοχή, αφού η διαδικασία αυτή βασίζεται στην αρχή της ελευθερίας και της αυτοδιάθεσης, δικαιώματα τα οποία ο κοινωνικός λειτουργός, δεσμεύεται να εκπροσωπεί και να σέβεται. Ο κοινωνικός λειτουργός οφείλει να ενημερώσει το άτομο, πριν την συμμετοχή του, για το δικαίωμά του στο να απαντήσει σε όσες ερωτήσεις επιθυμεί και για το δικαίωμα του να μην λάβει από την αρχή μέρος στην διαδικασία. Επιπλέον, ο ερευνητής οφείλει να ενημερώσει το άτομο για την εχεμύθεια που θα τηρηθεί και να δεσμευτεί επ' αυτού αλλά και για την ανωνυμία απέναντι στο άτομο που συμμετέχει (Cohen & Manion, 1994).

Σύμφωνα με την Αναγνωστοπούλου (2002) θα πρέπει να διασφαλίζεται το απόρρητο όσον αφορά το όνομα και τα στοιχεία του ατόμου. Αποτελεί αδιαμφισβήτητο δικαίωμα κάθε ατόμου ο σεβασμός στον ανακαθορισμό, την αυτονομία και των πληροφοριών.(Αναγνωστοπούλου, 2002). Όλα τα παραπάνω είναι δυνατόν να αποφευχθούν από την σωστή χρήση των ερευνητικών ερωτημάτων και από τις μεθόδους που χρησιμοποιούνται για να απαντηθούν. Για την αποφυγή δημιουργίας κλίματος παραπλάνησης υπάρχουν διάφοροι τρόποι δράσης που μπορούν να χρησιμοποιηθούν από τον ερευνητή για την αποφυγή πιθανόν συγκρούσεων.. (Ιωσηφίδης & Σπυριδάκης,2006)

Για την ευκολότερη προσέγγιση των ερευνώμενων ο ερευνητής οφείλει να συντάξει μια ενημερωτική επιστολή σχετικά με την διεξαγωγή της έρευνάς του και τον σκοπό της (Κυριαζή, 1999).

Στην παρούσα έρευνα δεν χρειάστηκε να συνταχθεί κάποια επιστολή, η οποία θα διευκόλυνε την πρόσβασή μας στις προαναφερόμενες υπηρεσίες και τόπους διότι τα ραντεβού των συνεντεύξεων προγραμματίστηκαν τηλεφωνικά. Παρόλα αυτά οι ερευνήτριες ενημέρωσαν τους συνεντευξιαζόμενους για την προβλεπόμενη διαδικασία που ακολουθείται σε μία έρευνα σύμφωνα με τα ζητήματα δεοντολογίας, όμως οι συνεντευξιαζόμενοι έκριναν πως δεν είναι απαραίτητη η σύνταξη της συγκεκριμένης επιστολής. Για τους παραπάνω λόγους δεν ακολουθήθηκε η προβλεπόμενη διαδικασία.

Επιλέχθηκε κυρίως η υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος της Αθήνας και της Θεσσαλονίκης για την κάλυψη του δείγματος διότι θεωρήθηκαν οι πιο κατάλληλες για τη συλλογή πληροφοριών για το συγκεκριμένο θέμα που επιλέχθηκε για την ερευνά μας. Παρόλα αυτά συνεντεύξεις διεξήχθησαν και σε άλλους τόπος όπου υπήρχαν ειδικοί που θα μπορούσαν να μας ενημερώσουν για το φαινόμενο της Ηλεκτρονικής

Εγκληματικότητας , λαμβάνοντας έτσι μέρος στην ερευνά μας. Ο πληθυσμός βρέθηκε σύντομα και το δείγμα καλύφθηκε άμεσα. Το δείγμα ενημερώθηκε από τις ερευνήτριες για την διεξαγωγή της συγκεκριμένης έρευνας και τηλεφωνικά αλλά και ύστερα από άμεση επικοινωνία μαζί τους. Έπειτα ακολούθησαν οι προκαθορισμένες συνεντεύξεις σε γραφεία διαμορφωμένα κατάλληλα για την διεξαγωγή των συνεντεύξεων.

Η ανωνυμία και η εμπιστευτικότητα διατηρήθηκαν αναφέροντας μόνο την ειδικότητα και τον τόπο διεξαγωγής των συνεντεύξεων χωρίς να αναφερθούν τα ονόματα των ειδικών.

Ο οδηγός συνέντευξης που χρησιμοποιήθηκε βρίσκεται στο παράρτημα.

2.7 Προσβασιμότητα

Δεν αντιμετωπίσαμε κανένα πρόβλημα στην προσβασιμότητα μας στις αρμόδιες υπηρεσίες και τόπους όπου διεξαγάγαμε την ερευνά μας καθώς οι συνεντευξιαζόμενοι που έλαβαν μέρος στην έρευνά μας ήταν πολύ δεκτικοί και πρόθυμοι και συναίνεσαν άμεσα ώστε να μας παραχωρήσουν τις συνεντεύξεις.

ΚΕΦΑΛΑΙΟ 3 - ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΑΛΥΣΗΣ

3.1 Κωδικοποίηση και ανάλυση δεδομένων

Στο συγκεκριμένο υποκεφάλαιο παρουσιάζονται τα αποτελέσματα της έρευνας όπως προέκυψαν μετά την κωδικοποίηση των ευρημάτων. Η κωδικοποίηση σύμφωνα με την Κυριαζή (1999) θεωρείται το κυριότερο σημείο για την ανάλυση των περιεχομένων. Διότι η ανάλυση περιεχομένου, είναι διαδικασία κωδικοποίησης των δεδομένων. Ο σκοπός της έρευνας καθώς και το θεωρητικό της πλαίσιο είναι δύο βασικοί παράγοντες που καθορίζουν τις κατηγορίες που θα δημιουργηθούν (Κυριαζή,1999). Για αυτό το λόγο κατηγοριοποιήθηκαν οι ειδικότητες των συνεντευξιαζόμενων και βάση αυτών δημιουργήθηκαν υποκατηγορίες βάση των ερωτήσεων που τους τέθηκαν κατά την διάρκεια της συνέντευξης ώστε να οδηγηθούμε ευκολότερα στην διεξαγωγή συμπερασμάτων της ερευνάς μας. Παρακάτω επιλέχθηκαν οι απαντήσεις των ειδικών της κάθε κατηγορίας οι οποίες εμπεριέχουν τα πιο βασικά στοιχειά που αφορούν την ερευνά μας.

3.2 Μέθοδος ποιοτικής ανάλυσης

1η ΚΑΤΗΓΟΡΙΑ: ΑΣΤΥΝΟΜΙΚΟΙ ΤΟΥ ΤΜΗΜΑΤΟΣ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Πρώτη Υποκατηγορία:

- Οι συνηθέστερες μορφές απάτης και εγκλήματος στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε.

ΑΡΙΘΜΟΣ ΑΣΤΥΝΟΜΙΚΩΝ	2 Αστυνομικοί
ΟΙΚΟΝΟΜΙΚΕΣ ΑΠΑΤΕΣ	2 Αστυνομικοί αντιμετωπίζουν περισσότερες περιπτώσεις οικονομικής απάτης.
ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ	2 Αστυνομικοί αντιμετωπίζουν συχνά περιπτώσεις προσβολής προσωπικότητας μέσω των κοινωνικών δικτύων
ΔΙΑΚΙΝΗΣΗ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ	1 Αστυνομικός αντιμετωπίζει αρκετά συχνά περιπτώσεις διακίνησης πορνογραφικού υλικού

→ **«ΑΣΤΥΝΟΜΙΚΟΣ 1:** Από τις πιο συνηθέστερες απάτες είναι οι νιγηριανές επιστολές οι οποίες στέλνονται σε ανυποψίαστους παραλήπτες όπου έχουν έδρα το Λονδίνο, το Άμστερνταμ ,την Μαδρίτη. Είναι πολύ πειστικές στέλνουν e-mail όπου σου γνωστοποιούν ότι κέρδισες το λόττο η πως είσαι ο κληρονόμος μιας μεγάλης περιουσίας μιας πάμπλουτης γιαγιάς που πέθανε από το Λονδίνο και όλα αυτά αρκεί να τους καταθέσεις κάποιο ποσό ανάλογα με την περίπτωση ή δίνοντας τον αριθμό της πιστωτικής σου κάρτας ή τον τραπεζικό σου λογαριασμό. Οι συγκεκριμένες επιστολές έχουν καταστρέψει πολύ κόσμο .Μια άλλη μορφή απάτης είναι αυτές που γίνονται μέσω των κοινωνικών δικτύων όπου σου λένε τον τρόπο και την ημερομηνία που θα πεθάνεις η το επίπεδο του iq σου δίνοντας τον αριθμό του τηλεφώνου σου ,αυτό έχει σαν συνέπεια να σε χρεώνουν 15 ευρώ κάθε μήνα .Αυτή είναι μια νέα μορφή καταιγίδας μηνυμάτων ώστε να γραφούν πολλούς συνδρομητές για να πάρουν όσα πιο πολλά χρήματα μπορούν .Αυτές οι εταιρείες τηλεπικοινωνιών έχουν κερδίσει αρκετά εκατομμύρια.

Επίσης μια άλλη μορφή απάτης είναι οι ευκαιριακές ιστοσελίδες όπου κάνουν προσφορές π.χ ταξίδι στην Βραζιλία μόνο με 450Ε πλήρες γεύμα και πληρωμένο το ξενοδοχείο αρκεί να στείλουν πρώτα χρήματα ώστε να κλείσουν τα εισιτήρια τους. Επίσης στήνουν και ψεύτικες παραγωγές στην τηλεόραση όπου διαφημίζουν το συγκεκριμένο ταξιδιωτικό γραφείο που έχει την τάδε προσφορά ,ο πολίτης πείθεται και τρέχει να προλάβει την προσφορά δίνει τα χρήματα και έπειτα αυτοί εξαφανίζονται καθώς το ταξιδιωτικό γραφείο δεν υπάρχει και οι ίδιοι έχουν εξαφανιστεί» .

→ **«ΑΣΤΥΝΟΜΙΚΟΣ 2**: Υπάρχουν τέσσερις μορφές απάτης: οι αγοροπωλησίες μέσω διαδικτύου όπου ζητούν από τους χρήστες οι οποίοι θέλουν να αποκτήσουν κάποιο προϊόν να στείλουν μια προκαταβολή χωρίς ποτέ να λάβουν το προϊόν που παρήγγειλαν, επίσης οι απάτες με πιστωτικές, οι απάτες γνωστές ως νιγηριανές όπου σου στέλνουν για παράδειγμα ένα e-mail και σου λένε ότι κέρδισες το λόττο και πρέπει να δώσεις κάποια στοιχεία σου ή να καταθέσεις κάποιο ποσό για να λάβεις το μεγάλο ποσό που κέρδισες και τέλος είναι οι απάτες με τις τράπεζες όπου σου στέλνουν ένα e-mail και σου λένε ότι υπάρχει κάποιο πρόβλημα με τα στοιχεία του λογαριασμού σου στην τάδε τράπεζα και ότι πρέπει να τα εισάγεις για να ενημερωθεί η τράπεζα. Αυτές είναι οι γνωστές οικονομικές απάτες. Από εκεί και έπειτα άλλα εγκλήματα στο διαδίκτυο με μεγάλη συχνότητα εμφάνισης είναι η προσβολή της προσωπικότητας μέσα από κοινωνικά δίκτυα και πιο συγκεκριμένα από το γνωστό σε όλους μας facebook».

Παραπάνω κατηγοριοποιήσαμε τις συχνότερες μορφές απάτης και εγκλήματος που αντιμετωπίζουν οι Αστυνομικοί που πήραν μέρος στην ερευνά μας, οι οποίοι εκπροσωπούν τα Τμήματα Δίωξης Ηλεκτρονικού Εγκλήματος στην Θεσσαλονίκη και στην Αθήνα . Από τα παραπάνω προέκυψε ότι η μεγαλύτερη συχνότητα εμφάνισης περιπτώσεων ηλεκτρονικού εγκλήματος, σύμφωνα με τους συνεντευξιαζόμενους, αφορά τις οικονομικές απάτες. Στη συνέχεια με μεγάλη εξίσου συχνότητα παραθέτονται τα εγκλήματα που διαπράττονται μέσω των κοινωνικών

δικτύων και αφορούν περιπτώσεις εξύβρισης, συκοφαντίας και υποκλοπής προσωπικών δεδομένων. Τέλος ένας από τους δύο αστυνομικούς ανέφερε ότι επίσης αντιμετωπίζει αρκετά συχνά περιπτώσεις διακίνησης πορνογραφικού υλικού. Όλα τα παραπάνω διαπιστώθηκαν καθώς αναφέρθηκαν από τους συνεντευξιαζόμενους της έρευνας.

Συμπερασματικά, επαληθεύεται ότι οι συχνότερες μορφές απάτης και εγκλήματος στο διαδίκτυο αφορούν τις οικονομικές απάτες, ακολουθώντας με αρκετά μεγάλη συχνότητα εμφάνισης οι απάτες μέσω κοινωνικών δικτύων και η διακίνησης πορνογραφικού υλικού.

1η ΚΑΤΗΓΟΡΙΑ- ΑΣΤΥΝΟΜΙΚΟΙ ΤΟΥ ΤΜΗΜΑΤΟΣ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΔΕΥΤΕΡΗ ΥΠΟΚΑΤΗΓΟΡΙΑ

- ΕΠΑΡΚΕΙΑ Η ΑΝΕΠΑΡΚΕΙΑ ΝΟΜΟΘΕΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΠΟΥ ΕΓΚΕΙΤΑΙ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΑΡΙΘΜΟΣ ΑΣΤΥΝΟΜΙΚΩΝ	Δύο Αστυνομικοί
ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΕΠΑΡΚΕΣ	Μηδέν αστυνομικοί θεωρούν επαρκές το νομοθετικό πλαίσιο
ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΑΝΕΠΑΡΚΕΣ	Μηδέν αστυνομικοί θεωρούν ανεπαρκές το νομοθετικό πλαίσιο
ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΚΑΤΑ ΕΝΑ ΠΟΣΟΣΤΟ ΕΠΑΡΚΕΣ	Δύο αστυνομικοί θεωρούν κατά ένα ποσοστό επαρκές το νομοθετικό πλαίσιο που έγκειται την δίωξη ηλεκτρονικού εγκλήματος .

→ «**ΑΣΤΥΝΟΜΙΚΟΣ Α**: Το νομοθετικό πλαίσιο αυτή την στιγμή στην Ελλάδα κατά ένα ποσοστό είναι επαρκές καθώς εφαρμόζει το ποινικό δίκαιο. Εκεί που έχουμε πρόβλημα είναι στην άρση του απορρήτου .Ο εισαγγελέας λέει πως γίνεται άρση απορρήτου σε όλες τις υποθέσεις ενώ η Α.Δ.Α.Ε συμφώνα με το προεδρικό διάταγμα 47 του 2005 όλο το διαδίκτυο είναι απόρρητο, επιτρέπει την άρση απορρήτου σε συγκεκριμένες υποθέσεις όπως ναρκωτικά ,

ανθρωποκτονίες ,εκβιασμούς και οργανωμένο έγκλημα κατά της εθνικής ασφάλειας. Το ισχύον νομοθετικό πλαίσιο δεν προσφέρει επαρκή προστασία από τη διακίνηση παιδικής πορνογραφίας και τα περιστατικά εκβιασμού μέσω Διαδικτύου, Παραδείγματος χάρη σε περιπτώσεις συκοφαντίας δεν γίνεται άρση απορρήτου ενώ ο εισαγγελέας κάνει άρση. Υπάρχει μια διχογνωμία ,που πιστεύουμε ότι θα λυθεί σύντομα. Με λίγα λόγια οι μισοί εφαρμόζουν αυτά που λέει εισαγγελέας και οι άλλοι την Α..Δ.Α.Ε αλλά σε περιπτώσεις εμβρασμού γίνεται πάντα άρση» .

→ **«ΑΣΤΥΝΟΜΙΚΟΣ Β**: Θεωρώ ότι υπάρχουν κάποιες ελλείψεις στο νομοθετικό πλαίσιο όχι μόνο για τα εγκλήματα και τις απάτες του διαδικτύου αλλά και για τις παραδοσιακές απάτες και τα παραδοσιακά εγκλήματα. Βέβαια το Δεκέμβριο του 2008 . Επίσης ένα άλλο πρόβλημα που αντιμετωπίζουμε είναι ότι το νομοθετικό πλαίσιο σε παγκόσμιο επίπεδο διότι κάτι που θεωρείται παράνομο σε μια χώρα σε κάποια άλλη χώρα μπορεί να μην θεωρείται παράνομο. Επομένως τι κάνουμε σε τέτοιες περιπτώσεις; Συνήθως ο χρήστης που διέπραξε μια παράνομη πράξη δικάζεται σύμφωνα με το νομοθετικό πλαίσιο της χώρας από την οποία διεξήγε η συγκεκριμένη παράνομη πράξη. Για παράδειγμα στην Ελλάδα το στοίχημα είναι παράνομο ενώ στην Αγγλία μπορεί και να μην θεωρείται παράνομο. Εσύ είσαι σπίτι σου στην Ελλάδα και παίζεις παράνομο στοίχημα σε σελίδα της Αγγλίας; Είναι παράνομο αυτό ή όχι; Είναι γιατί η πράξη διαπράχθηκε στην Ελλάδα όπου ο ποινικός μας κώδικας νομοθετεί ότι το στοίχημα είναι παράνομο».

Παραπάνω κατηγοριοποιήσαμε τις απαντήσεις , των αστυνομικών που πήραν μέρος στην έρευνα μας, οι οποίοι εκπροσωπούν τα τμήματα δίωξης ηλεκτρονικού εγκλήματος σε Θεσσαλονίκη και Αθήνα ,όσον αφορά την νομοθεσία .Από τα παραπάνω προέκυψε ότι το νομοθετικό πλαίσιο που έγκειται της δίωξης ηλεκτρονικού εγκλήματος θεωρείται κατά ένα μόνο ποσοστό επαρκές καθώς παρουσιάζει κενά και ελλείψεις και δυσκολεύει

την ικανοποιητική , πλήρη αντιμετώπιση και δίωξη του ηλεκτρονικού εγκλήματος . Όλα τα παραπάνω διαπιστώθηκαν καθώς αναφέρθηκαν από τους συνεντευξιαζόμενους της έρευνας. Τα προβλήματα που παρουσιάζει η νομοθεσία επικεντρώνονται πρώτον στην διχογνωμία που υπάρχει σχετικά με την άρση του απορρήτου, δεύτερον στο νομοθετικό πλαίσιο που έχει θεσπίσει κάθε χώρα και είναι διαφορετικό για την τιμωρία κάθε απάτης και εγκλήματος ενώ θα έπρεπε να έχει θεσπιστεί νομοθετικό πλαίσιο που να ισχύει σε όλες τις χώρες και τρίτον λόγω των ελαστικών μέτρων της μη προφυλάκισης των ενόχων για απάτες ή εγκλήματος άνω των δέκα χρόνων προάγοντας η ίδια εγκληματίες. Ωστόσο θεωρούν ότι όλες υποθέσεις εκδικάζονται και τιμωρούνται οι δράστες άλλοτε αυστηρά και άλλοτε όχι.

1η ΚΑΤΗΓΟΡΙΑ- ΑΣΤΥΝΟΜΙΚΟΙ ΤΟΥ ΤΜΗΜΑΤΟΣ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3η ΥΠΟΚΑΤΗΓΟΡΙΑ

- ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

ΑΡΙΘΜΟΣ ΑΣΤΥΝΟΜΙΚΩΝ	Δύο Αστυνομικοί
ΝΕΟ ΕΠΑΡΚΕΣ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ	Ένας αστυνομικός θεωρεί αρχικά πως πρέπει να νομοθετήσει το κράτος ξανά για την κάλυψη των κενών που υπάρχουν.
ΟΡΓΑΝΩΜΕΝΕΣ ΟΜΑΔΕΣ ΕΙΔΙΚΩΝ	Ένας αστυνομικός προτείνει την δημιουργία ειδικών ομάδων με στόχο την πρόληψη των πολιτών
ΚΑΤΑΛΛΗΛΗ ΜΕΡΙΜΝΑ ΑΠΟ ΤΗΝ ΙΔΙΑ ΤΗΝ ΠΟΛΙΤΕΙΑ	Ένας αστυνομικός αναφέρει πως η ίδια η πολιτεία πρέπει να μεριμνήσει για την αντιμετώπιση του φαινομένου
ΠΡΟΣΩΠΙΚΗ ΥΠΟΘΕΣΗ	Ένας αστυνομικός ανέφερε πως είναι προσωπική υπόθεση του καθενός ώστε να παραφυλαχθεί από το διαδίκτυο.

→ **«ΑΣΤΥΝΟΜΙΚΟΣ Α**: Οι προτάσεις μου είναι οι εξής ,καταρχήν να ισορροπήσει ο νόμος ,να νομοθετήσει το κράτος ώστε να μην υπάρχουν κενά και διχογνωμία σχετικά με την άρση του απορρήτου . Θα είχα δεύτερη άλλα η πρόταση μου θα πραγματοποιηθεί σε ένα μήνα όπου θα γίνουμε διεύθυνση .Στην νέα μας διεύθυνση θα υλοποιηθεί η πρόταση μου ώστε να δημιουργηθεί οργανωμένη ομάδα ειδικών ψυχολόγων ,κοινωνικών λειτουργών και προγραμματιστών που θα ενημερώνει τα σχολεία ,τις νομαρχίες και τους δήμους για το ίντερνετ δίνοντας συμβουλές για ασφαλή πλοήγηση. Είναι ανησυχητική η χρήση του διαδικτύου από εφήβους καθώς αγγίζει τα όρια του εθισμού, χωρίς ωστόσο να υπάρχει η κατάλληλη μέριμνα από την Πολιτεία, ούτε επαρκής ενημέρωση των οικογενειών για την αποτελεσματικότερη προστασία τους. Αυτός ακριβώς θα είναι ο ρόλος τους η πρόληψη. Θα ήθελα να συμπληρώσω πως το διαδίκτυο είναι ότι καλύτερο υπάρχει αυτή τη στιγμή. Χωρίς αυτό δεν μπορεί να λειτουργήσει τίποτα. Εκείνο που επιδιώκουμε είναι να βοηθήσουμε τους ανθρώπους να έχουν ασφαλή πλοήγηση, να προστατέψουμε πολίτη από τους κινδύνους που πιθανόν διατρέχει. Συμβουλή μου λοιπόν είναι οι ίδιοι οι πολίτες να θωρακίζουν τα προσωπικά τους δεδομένα και να μην εκθέτουν την προσωπική τους ζωή στο ίντερνετ» .

→ **«ΑΣΤΥΝΟΜΙΚΟΣ Β:** Τι να σας πω; Δεν υπάρχει τρόπος να προστατευτείς. Το μόνο που μπορούμε να κάνουμε είναι να προστατεύσουμε εμείς οι ίδιοι τον εαυτό μας με το να προσέχουμε σε τι σελίδες μπαίνουμε και να είμαστε πιο υποψιασμένοι με τα διάφορα e-mail που θα φτάνουν σε εμάς από αγνώστους και όχι μόνο».

Παραπάνω κατηγοριοποιήσαμε τις απαντήσεις , των αστυνομικών που πήραν μέρος στην έρευνα μας, οι οποίοι εκπροσωπούν τα τμήματα δίωξης ηλεκτρονικού εγκλήματος σε Θεσσαλονίκη και Αθήνα, όσον αφορά τις προτάσεις τους .Από τα παραπάνω προέκυψε ότι ένας από τους δύο προτείνει την ισορρόπηση του νόμου με την θέσπιση νέου αποτελεσματικότερου νομοθετικού πλαισίου .Δεύτερον ένας στους δύο

προτείνει να δημιουργηθεί οργανωμένη ομάδα ειδικών ψυχολόγων ,κοινωνικών λειτουργών και προγραμματιστών που θα ενημερώνει τα σχολεία ,τις νομαρχίες και τους δήμους για το ιντερνέτ δίνοντας συμβουλές για ασφαλή πλοήγηση. Ακόμα ένας στους δύο θεωρεί πως πρέπει η ίδια η πολιτεία να μεριμνήσει για την αντιμετώπιση του φαινομένου και τέλος ένας στους δύο θεωρεί πως το μόνο που μπορούμε να κάνουμε είναι να προστατεύσουμε εμείς οι ίδιοι τον εαυτό μας με το να προσέχουμε σε τι σελίδες μπαίνουμε και να είμαστε πιο υποψιασμένοι με τα διάφορα e-mail που θα φτάνουν σε εμάς από αγνώστους και όχι μόνο. Στο παράρτημα παρουσιάζεται η πλήρη συνέντευξη και των δύο αστυνομικών .

2η ΚΑΤΗΓΟΡΙΑ: ΨΥΧΟΛΟΓΟΙ ΠΟΥ ΣΥΝΕΡΓΑΖΟΝΤΑΙ ΜΕ ΤΑ ΤΜΗΜΑΤΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Πρώτη Υποκατηγορία

- Οι συνηθέστερες μορφές απάτης και εγκλήματος στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την συνεργασία σας με το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος.

ΑΡΙΘΜΟΣ ΨΥΧΟΛΟΓΩΝ	2 Ψυχολόγοι
ΟΙΚΟΝΟΜΙΚΕΣ ΑΠΑΤΕΣ	2 Ψυχολόγοι απάντησαν πως οι συχνότερες μορφές απάτης στο διαδίκτυο αφορούν τις οικονομικές απάτες.
ΑΥΤΟΚΤΟΝΙΑ	2 Ψυχολόγοι αντιμετωπίζουν πολύ συχνά περιπτώσεις αυτοκτονίας μέσω διαδικτύου
ΣΕΞΟΥΑΛΙΚΗ ΠΑΡΕΝΟΧΛΗΣΗ-ΔΥΣΦΗΜΗΣΗ ΜΕΣΩ ΚΟΙΝΩΝΙΚΩΝ ΔΙΚΤΥΩΝ	2 Ψυχολόγοι αντιμετωπίζουν σε μεγάλη συχνότητα περιπτώσεις σεξουαλικής παρενόχλησης και δυσφήμησης μέσω κοινωνικών δικτύων
ΠΑΙΔΙΚΗ ΗΛΕΚΤΡΟΝΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ	2 Ψυχολόγοι αντιμετωπίζουν περιπτώσεις παιδικής ηλεκτρονικής πορνογραφίας.

→ **«ΨΥΧΟΛΟΓΟΣ Α**: Η εξάπλωση του διαδικτυακού εγκλήματος τα τελευταία χρόνια είναι πολύ μεγάλη με αποτέλεσμα καθημερινά να φτάνουν στην Δίωξη Ηλεκτρονικού Εγκλήματος πολλές περιπτώσεις που να σχετίζονται με το ηλεκτρονικό έγκλημα. Συνήθως η πιο συχνή μορφή απάτης που συναντούμε είναι η οικονομική απάτη. Χωρίς αυτό να σημαίνει πως τα ποσοστά εμφάνισης των άλλων μορφών απάτης στο διαδίκτυο απέχουν με μεγάλη διαφορά από την οικονομική απάτη. Για παράδειγμα συναντούμε και πολλές περιπτώσεις σεξουαλικής παρενόχλησης μέσω διαδικτύου, όπου ενήλικες δημιουργούν ψεύτικα προφίλ στα διάφορα Chat rooms(facebook, msn κτλ)προσπαθώντας να προσεγγίσουν τους ανήλικους χρήστες είτε για να προβούν σε σεξουαλική παρενόχληση είτε στο να τους αποσπάσουν φωτογραφικό υλικό ή κάποιο βιντεάκι που πιθανόν να έχουν , έτσι οδηγούμαστε μετά και στην διακίνηση πορνογραφικού υλικού αλλά και πολλές περιπτώσεις, ιδιαίτερα τελευταία, που σχετίζονται με την αυτοκτονία. Θα λέγαμε πως αποτελεί «μόδα» ή και «παιχνίδι» η προτροπή κάποιου ατόμου στην αυτοκτονία ή η ανακοίνωση ότι κάποιος σκοπεύει να προβεί σε τέτοιου είδους ενέργεια».

→ **«ΨΥΧΟΛΟΓΟΣ Β**: Το διαδικτυακό έγκλημα έχει πάρει τεράστιες διαστάσεις σε παγκόσμιο επίπεδο όπως αντιληφθήκατε και εσείς μέσα από την ερευνά σας διαπράττονται πολλές απάτες η πιο συνήθης είναι η οικονομική εξαπάτηση .Μια από τις απειλητικές μορφές διαδικτυακού εγκλήματος δεδομένου της πρόσβασης των παιδιών στο διαδίκτυο αφορά την παιδική ηλεκτρονική πορνογραφία, την προτροπή σε αυτοκτονία και την σεξουαλική παρενόχληση ανηλίκων ,όπου ενήλικες προσεγγίζουν ανήλικους με ψεύτικο προφίλ παρουσιάζοντας τον εαυτό τους ως συνομήλικους. Εγώ προσωπικά και συνάδελφοι έχουμε συνεργαστεί με την Δίωξη κυρίως σε περιπτώσεις σεξουαλικής παρενόχλησης ανηλίκων κ σε περιπτώσεις αυτοκτονιών» .

Παραπάνω κατηγοριοποιήσαμε τις συχνότερες μορφές απάτης και εγκλήματος που αντιμετωπίζουν οι ψυχολόγοι που πήραν μέρος στην ερευνά μας, οι οποίοι συνεργάζονται με τα Τμήματα Δίωξης Ηλεκτρονικού Εγκλήματος στην Θεσσαλονίκη και στην Αθήνα . Από τα παραπάνω προέκυψε ότι η μεγαλύτερη συχνότητα εμφάνισης περιπτώσεων ηλεκτρονικού εγκλήματος, σύμφωνα με τους συνεντευξιαζόμενους, αφορά τις οικονομικές απάτες. Στη συνέχεια με μεγάλη εξίσου συχνότητα παραθέτονται τα εγκλήματα που διαπράττονται μέσω των κοινωνικών δικτύων και αφορούν περιπτώσεις εξύβρισης, συκοφαντίας και υποκλοπής προσωπικών δεδομένων. Επίσης έμφαση δόθηκε και από τους δυο ψυχολόγους σχετικά μ ε το πολύ συχνό φαινόμενο αυτοκτονίας μέσω κοινωνικών δικτύων που τελευταία έχει αυξηθεί πάρα πολύ. Τέλος και οι δύο ψυχολόγοι ανέφεραν πως αρκετά συχνά εμφανίζονται περιπτώσεις διακίνησης πορνογραφικού υλικού. Όλα τα παραπάνω διαπιστώθηκαν καθώς αναφέρθηκαν από τους συνεντευξιαζόμενους της έρευνας.

Συμπερασματικά, επαληθεύεται ότι οι συχνότερες μορφές απάτης και εγκλήματος στο διαδίκτυο αφορούν τις οικονομικές απάτες, ακολουθώντας με αρκετά μεγάλη συχνότητα εμφάνισης οι απάτες και εγκλήματα μέσω κοινωνικών δικτύων, με έμφαση στην αυτοκτονία και στην σεξουαλική παρενόχληση ανηλίκων με την χρήση ψεύτικων-εικονικών προφίλ των δραστών, καθώς επίσης και η διακίνησης πορνογραφικού υλικού.

<u>Δεύτερη Υποκατηγορία</u>

- **<u>Προτάσεις των ειδικών για την καταπολέμηση του Ηλεκτρονικού Εγκλήματος και για την προστασία των θυμάτων</u>**.

ΑΡΙΘΜΟΣ ΨΥΧΟΛΟΓΩΝ	2 Ψυχολόγοι
ΠΡΟΣΛΗΨΕΙΣ ΚΟΙΝΩΝΙΚΩΝ ΛΕΙΤΟΥΡΓΩΝ ΚΑΙ ΨΥΧΟΛΟΓΩΝ	2 Ψυχολόγοι πρότειναν προσλήψεις κοινωνικών λειτουργών &

ΓΙΑ ΣΤΕΛΕΧΩΣΗ ΤΜΗΜΑΤΩΝ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ	ψυχολόγων στα συγκεκριμένα τμήματα
ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΟΙΝΟΤΗΤΑΣ	2 Ψυχολόγοι θεωρούν πολύ σημαντική την ευαισθητοποίηση της κοινότητας
ΣΤΕΛΕΧΩΣΗ ΓΡΑΜΜΩΝ ΕΝΤΟΠΙΣΜΟΥ & ΑΠΟΤΡΟΠΗΣ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΓΚΛΗΜΑΤΩΝ	2 Ψυχολόγοι προτείνουν την στελέχωση γραμμών εντοπισμού και αποτροπής διαδικτυακών εγκλημάτων με περισσότερα άτομα
ΕΙΣΑΓΩΓΗ ΚΟΙΝΩΝΙΚΩΝ ΛΕΙΤΟΥΡΓΩΝ&ΨΥΧΟΛΟΓΩΝ ΣΤΑ ΣΧΟΛΕΙΑ	2 Ψυχολόγοι προτείνουν την πρόσληψη κοινωνικών λειτουργών και ψυχολόγων στα σχολεία
ΚΑΤΑΣΤΑΛΤΙΚΑ ΜΕΤΡΑ ΑΠΟ ΑΣΤΥΝΟΜΙΚΕΣ ΑΡΧΕΣ	1 Ψυχολόγος προτείνει να ληφθούν κατασταλτικά μέτρα από τις ίδιες τις αστυνομικές αρχές.

→ **«ΨΥΧΟΛΟΓΟΣ Α:** Τώρα μου βάζεις δύσκολα! Σίγουρα θα πρέπει να προσληφτούν περισσότεροι ψυχολόγοι και κοινωνικοί λειτουργοί στην αστυνομία, γιατί εμείς εδώ είμαστε τρία άτομα και προσπαθούμε να καλύψουμε όλες τις περιπτώσεις της αστυνομίας στην περιοχή της Θεσσαλονίκης αλλά και στην ευρύτερη περιοχή της Βόρειας Ελλάδας πράγμα το οποίο είναι αδύνατον και πολλές φορές ζητούμε την βοήθεια και συνεργασία συναδέλφων από άλλες υπηρεσίες. Βασικά αυτό, να γίνουν περισσότερες προσλήψεις ψυχολόγων και κοινωνικών λειτουργών. Επίσης καλό θα ήταν να ευαισθητοποιήσουμε και να ενημερώσουμε την κοινότητα για το διαδικτυακό έγκλημα και τις μορφές τους αλλά και τον τρόπο προστασίας τους με διάφορες εκδηλώσεις και ομιλίες, έτσι ώστε τα εν δυνάμει θύματα να μην φτάσουν να γίνουν θύματα επιτήδειων δραστών. Ιδιαίτερα όσον αφορά τους ανήλικους θα πρέπει να γίνουν ομιλίες σε σχολεία για να ενημερωθούν, τόσο τα παιδιά όσο και οι γονείς και οι εκπαιδευτικοί για το πώς μπορούν να προστατευτούν

από τα εγκλήματα του διαδικτύου. Επίσης θα πρέπει να στελεχωθούν με περισσότερα άτομα οι γραμμές εντοπισμού και αποτροπής διαδικτυακών εγκλημάτων και να δημιουργηθούν και νέες γραμμές αν κρίνεται απαραίτητο. Τέλος καλό θα ήταν τέτοιου είδους συμπεριφορές, είτε ως δράστης είτε ως θύμα, να προλαμβάνονται στο σχολείο με την ύπαρξη ενός ψυχολόγου ή κοινωνικού λειτουργού, ο οποίος θα μπορεί να εντοπίσει μια τέτοια συμπεριφορά».

→ **«ΨΥΧΟΛΟΓΟΣ Β**: Έχω να καταθέσω κάποιες προτάσεις χωρίς να θεωρώ τον εαυτό μου ειδικό στο διαδίκτυο. Θα πρέπει να παρθούν προληπτικά μέτρα ενημερώνοντας αρχικά τους πολίτες για τους τρόπους που θα μπορούσαν να προφυλαχθούν από το διαδίκτυο αλλά και για τις μορφές διαδικτυακού εγκλήματος .Θα πρέπει να δημιουργηθούν διαδικτυακοί τόποι αποτροπής αυτοκτονιών όπου ειδικοί θα συμβουλεύουν μέσω online συνομιλία .Πέρα από τα προληπτικά μέτρα ,θα πρέπει να παρθούν και κατασταλτικά μέτρα όπου πρωταγωνιστικό ρόλο καλούνται να αναλάβουν οι αστυνομικές αρχές ,να διατεθούν από το κράτος τα απαραίτητα μέσα και να αναπτυχθεί το θεωρητικό υπόβαθρο των αστυνομικών για τον εντοπισμό και την σύλληψη των εγκληματιών. Τέλος καλό θα ήταν να ευαισθητοποιηθούν ομάδες ειδικών επαγγελματιών που μπορούν να παίξουν ενεργό ρόλο στην αναγνώριση αυτοκαταστροφικών ατόμων όπως οι εκπαιδευτικοί που έχουν άμεση καθημερινή επαφή με μαθητές».

Παραπάνω κατηγοριοποιήσαμε τις προτάσεις των ειδικών (ψυχολόγων) για την καταπολέμηση του Ηλεκτρονικού Εγκλήματος και για την προστασία των θυμάτων.

Από τα παραπάνω προέκυψε ότι οι ψυχολόγοι προτείνουν αρχικά την στελέχωση των τμημάτων Δίωξης Ηλεκτρονικού Εγκλήματος με Κοινωνικούς Λειτουργούς και Ψυχολόγους για την καλύτερη λειτουργία των συγκεκριμένων τμημάτων. Επίσης πολύ σημαντικό και για τους δύο ψυχολόγους είναι η ευαισθητοποίηση της κοινότητας και η ενημέρωση τους

για το Ηλεκτρονικό Έγκλημα μέσα από διάφορες εκδηλώσεις και ομιλίες, όπως χαρακτηριστικά μας ανέφεραν οι συνεντευξιαζόμενοι. Απαραίτητη κρίνεται η ευαισθητοποίηση και ενημέρωση των ανηλίκων στα σχολεία για την πρόληψη του φαινομένου. Εξίσου σημαντικό και για τους δύο συνεντευξιαζόμενος είναι οι εισαγωγή κοινωνικών λειτουργών και ψυχολόγων στα σχολεία όπου «το μάτι» του ειδικού θα μπορέσει να εντοπίσει προβληματικές συμπεριφορές και να τις προλάβει πριν να έχουν ανεπανόρθωτες συνέπειες. Τέλος και οι δύο ψυχολόγοι προτείνουν την αύξηση προσωπικού από ειδικούς στις γραμμές εντοπισμού και αποτροπής διαδικτυακών εγκλημάτων. Ένας εκ των δύο ψυχολόγων προτείνει επίσης την λήψη κατασταλτικών μέτρων αντιμετώπισης του φαινομένου από τις αστυνομικές αρχές. Όλα τα παραπάνω διαπιστώθηκαν καθώς αναφέρθηκαν από τους συνεντευξιαζόμενους της έρευνας.

Συμπερασματικά, επαληθεύεται η ελλιπής ύπαρξη ειδικών, παρότι κρίνεται αναγκαία η συμβολή τους σε τέτοιου είδους περιπτώσεις. Επίσης με την ευαισθητοποίηση της κοινότητας και των σχολείων είναι πιθανή η μείωση του φαινομένου. Έτσι επαληθεύεται η χρησιμότητα της πρόληψης. Στο παράρτημα παρουσιάζεται η πλήρη συνέντευξη και των δύο ψυχολόγων .

3η ΚΑΤΗΓΟΡΙΑ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ

ΠΡΩΤΗ ΥΠΟΚΑΤΗΓΟΡΙΑ

- **Οι συνηθέστερες μορφές απάτης και εγκλήματος που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε**

ΑΡΙΘΜΟΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ	Δύο Προγραμματιστές
ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ	Δύο στους δύο προγραμματιστές θεωρεί μάστιγα εγκληματικότητας

	τα κοινωνικά δίκτυα.(facebook.hi5)
ΟΙΚΟΝΙΚΕΣ ΑΠΑΤΕΣ	Δύο στους δύο προγραμματιστές κατατάσσει τις οικονομικές άπατες στις συχνότερες μορφές απάτης διαδικτύου
ΔΙΑΚΙΝΗΣΗ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ	Δύο στους δύο προγραμματιστές αναφέρει την διακίνηση πορνογραφικού υλικού από τις συνηθέστερες μορφές εγκλήματος του διαδικτύου

→ **«ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Α**: Η μεγαλύτερη και πιο διαδεδομένη μορφή απάτης στο διαδίκτυο σήμερα θεωρώ ότι είναι τα κοινωνικά δίκτυα και πιο συγκεκριμένα το facebook. Μέσα από αυτό μπορούν να σου κλέψουν προσωπικά σου στοιχεία, να δυσφημίσουν ή να προσβάλλουν κάποιον, να δημιουργήσουν εικονικό προφίλ για να πλησιάσουν ανήλικα και πολλά άλλα. Αυτό επιτυγχάνεται με πολύ εύκολο τρόπο. Όταν ασχολείσαι με το διαδίκτυο και είσαι ένας μέσος χρήστης, όχι απλός χρήστης, τότε μπορείς να χρησιμοποιήσεις προγράμματα τα οποία είναι δωρεάν και με την βοήθεια αυτών των προγραμμάτων να υποκλέβεις την ip διεύθυνση κάποιου. Η ip διεύθυνση είναι η ηλεκτρονική διεύθυνση που εκπέμπει κάθε μόντεμ-ρούτερ και αυτή είναι διαφορετική και μοναδική για τον κάθε χρήστη. Ο μέσος χρήστης που θέλει να βρει το ip σου το κάνει με πολύ εύκολο τρόπο, γιατί μέσω του facebook το εκπέμπεις συνέχεια. Βρίσκοντας λοιπόν κάποιος το ip σου μετά μπορεί να βρει το στίγμα που βρίσκεσαι, το τηλέφωνο σου και όλα αυτά με την βοήθεια προγραμμάτων. Να σημειωθεί ότι εάν έχεις ασύρματο δίκτυο είναι λίγο πιο δύσκολο να σε βρει κάποιος διότι είναι σαν να ψάχνει κινητό τηλέφωνο, δεν είναι όμως ακατόρθωτο απλά θα χρειαστεί ένα συνδυασμό προγραμμάτων αντί για ένα απλό πρόγραμμα. Άλλες πολύ διαδεδομένες μορφές απάτης είναι οι οικονομικές απάτες και η διακίνηση πορνογραφικού υλικού».

→ **<u>ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Β</u>**: Οι συνηθέστερες μορφές απάτης και εγκλήματος αφορούν την παιδική πορνογραφία, αλλά έχουμε μεγάλο όγκο καταγγελιών για συκοφαντικές δυσφημήσεις, εξύβριση και οικονομικές απάτες .Η μεγάλη μάστιγα όμως είναι τα κοινωνικά δίκτυα όπου μέσα από αυτά έχει δημιουργηθεί μια νέα μορφή τρομοκρατίας το κο bullying όπου ο καθένας μπορεί να εκβιάσει και να συκοφαντήσει τον καθένα δημιουργώντας ψεύτικα προφίλ» .

Παραπάνω κατηγοριοποιήσαμε τις απαντήσεις των προγραμματιστών που πήραν μέρος στην έρευνα μας, οι οποίοι εργάζονται στα τμήματα δίωξης ηλεκτρονικού εγκλήματος σε Θεσσαλονίκη και Αθήνα, όσον αφορά τις συνηθέστερες μορφές απάτης και εγκλήματος που γνωρίζουν και έχουν συναντήσει .Από τα παραπάνω προέκυψε ότι δύο στους δύο θεωρεί μάστιγα τα κοινωνικά δίκτυα όπου μέσα από αυτά έχει δημιουργηθεί μια νέα μορφή τρομοκρατίας το κο bullying όπου ο καθένας μπορεί να εκβιάσει, να συκοφαντήσει τον καθένα και να παραπλανήσει ανήλικα δημιουργώντας ψεύτικα προφίλ .Επίσης δύο στους δύο κατατάσσει τις οικονομικές απάτες στις συνηθέστερες μορφές απάτης και τέλος και οι δύο προγραμματιστές αναφέρουν ως αρκετά συνηθέστερη μορφή εγκλήματος τις περιπτώσεις διακίνησης παιδικού πορνογραφικού υλικού .

3η ΚΑΤΗΓΟΡΙΑ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ

ΔΕΥΤΕΡΗ ΥΠΟΚΑΤΗΓΟΡΙΑ

→ **ΤΡΟΠΟΙ ΠΡΟΣΒΑΣΗΣ ΤΩΝ HACKERS ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΜΑΣ ΔΕΔΟΜΕΝΑ**

ΑΡΙΘΜΟΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ	Δύο
ΜΕΣΩ E-MAIL	Δύο στους δύο προγραμματιστές αναφέρουν ως πρώτο τρόπο πρόσβασης των hacker μέσω e-mail.
ΜΕΣΩ ΙΟΥ (TROJAN HORSE)	Δύο στους δύο προγραμματιστές αναφέρουν ως δεύτερο τρόπο πρόσβασης των hacker την αποστολή του συγκεκριμένου ιού .

→ «**ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Α**: Πολύ εύκολα! Απλά στέλνοντας σου ένα e-mail που συνήθως σου ζητά να κάνεις log in για κάποιο λόγο, σε εικονικό site, και έτσι ενεργοποιείται ιός και όποτε ανοίγεις τον υπολογιστή σου, αυτό φαίνεται στον «ενδιαφερόμενο» και είναι σαν να του ανοίγεις την πόρτα για να έχει ελεύθερη πρόσβαση στον υπολογιστή σου και στα προσωπικά σου δεδομένα. Με αυτόν τον τρόπο μπορεί να υποκλέψει τα αρχεία σου ή απλά αν είναι ένας περίεργος hacker θα θέλει να έχει πρόσβαση στο e-mail σου και σε φωτογραφίες σου ή άλλοι hackers εισβάλλουν στον υπολογιστή σου μόνο και μόνο για να σου «κοτσάρουν» έναν ιό και να σου κάψουν τα βασικά σου αρχεία με αποτέλεσμα να μην δουλεύει ο υπολογιστή σου και να θέλει οπωσδήποτε format για να επανέλθει χάνοντας όμως, αν όχι όλα , μεγάλο όγκο των αποθηκευμένων σου αρχείων».

→ **«ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Β**: Υπάρχει ένα μότο για τους hacker τίποτα δεν κλειδώνει .Αν πέσεις στο μάτι κάποιου hacker δεν γλιτώνεις. Μπορώ να σου μιλώ μέχρι αύριο για τους τρόπους που μπορεί να εισβάλει ένας hacker .Υπάρχουν ωστόσο δύο βασικοί τρόποι :Πρώτον να εισβάλλει μέσω του ιού Trojan horse στέλνοντας σου μέσω msn μια φωτογραφία την ώρα που συνομιλείς η όποια περιέχει ένα πρόγραμμα όπου βλέποντας εσύ την φωτογραφία ο hacker έχει πρόσβαση στον υπολογιστή σου .Δεύτερον ένας άλλος τρόπος είναι μέσω e-mail όπου στέλνουν επισυναπτόμενα αρχεία τα οποία όταν ανοιχτούν ανοίγει παράλληλα και ένα πρόγραμμα με το οποίο ο hacker μπορεί να κάνει υποχείριο του τον υπολογιστή σου .Με λίγα λόγια μπορεί να σου αλλάξει τους κωδικούς σου να κλέψει οποιοδήποτε αρχείο έχεις στον υπολογιστή σου, θα μάθει όλη την ιστορία σου και τέλος μπορεί να στον κλειδώσει τελείως ώστε να μην μπορείς να ξαναμπείς» .

Παραπάνω κατηγοριοποιήσαμε τις απαντήσεις των προγραμματιστών που πήραν μέρος στην έρευνα μας, οι οποίοι εργάζονται στα τμήματα δίωξης ηλεκτρονικού εγκλήματος σε Θεσσαλονίκη και Αθήνα, όσον αφορά τους τρόπους πρόσβασης των hacker στα προσωπικά μας δεδομένα . Δύο στους δύο προγραμματιστές αναφέρει ως πρώτο τρόπο πρόσβασης των hacker την αποστολή e-mail που συνήθως σου ζητά να κάνεις log in για κάποιο λόγο, σε εικονικό site ενεργοποιώντας τον ιό , ανοίγοντας την πόρτα για να έχει ελεύθερη πρόσβαση στον υπολογιστή σου και στα προσωπικά σου δεδομένα ο hacker. Με αυτόν τον τρόπο μπορεί να υποκλέψει τα αρχεία σου ή οτιδήποτε έχεις στον υπολογιστή σου .Επίσης δύο στους δύο ως δεύτερο τρόπο πρόσβασης των hacker αναφέρουν την μετάδοση ενός ιό π.χ :Trojan horse.Συγκεκριμένα στέλνοντας σου μέσω msn μια φωτογραφία την ώρα που συνομιλείς η όποια περιέχει ένα πρόγραμμα όπου βλέποντας εσύ την φωτογραφία ο hacker έχει πρόσβαση στον υπολογιστή σου κάνοντας τον υποχείριο του .

3η ΚΑΤΗΓΟΡΙΑ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ

Τρίτη Υποκατηγορία

- Προτάσεις των Προγραμματιστών για την καταπολέμηση του Ηλεκτρονικού Εγκλήματος και για την προστασία των θυμάτων.

ΑΡΙΘΜΟΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ	2 Προγραμματιστές
ΧΡΗΣΗ ΠΡΟΓΡΑΜΜΑΤΩΝ ΠΡΟΣΤΑΣΙΑΣ	2 Προγραμματιστές προτείνουν την χρήση προγραμμάτων προστασίας
ΔΕΝ ΑΝΟΙΓΟΥΜΕ E-MAIL ΑΠΟ ΧΡΗΣΤΕΣ ΠΟΥ ΔΕΝ ΓΝΩΡΙΖΟΥΜΕ	1 Προγραμματιστής προτείνει να μην ανοίγουν οι χρήστες e-mail από άγνωστους χρήστες
ΑΠΟΘΗΚΕΥΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΕΞΩΤΕΡΙΚΑ ΑΠΟΘΗΚΕΥΤΙΚΑ ΜΕΣΑ	2 Προγραμματιστές προτείνουν την αποθήκευση προσωπικών δεδομένων σε εξωτερικά αποθηκευτικά μέσα.
ΑΝΟΙΓΜΑ ΜΟΝΟ ΕΓΚΥΡΩΝ ΣΕΛΙΔΩΝ	1 Προγραμματιστής προτείνει την είσοδο των χρηστών μόνο σε έγκυρες σελίδες
ΚΡΑΤΑΜΕ BACK UP ΑΡΧΕΙΑ ΜΕ ΚΡΥΠΤΟΓΡΑΦΗΣΗ	1 προγραμματιστής προτείνει να κρατάνε οι χρήστες back up αρχεία τα οποία θα κρυπτογραφούν
ΕΝΗΜΕΡΩΝΟΜΑΣΤΕ ΑΠΟ ΕΙΔΙΚΟ ΓΙΑ ΟΤΙΔΗΠΟΤΕ ΜΑΣ ΑΠΑΣΧΟΛΕΙ	1 Προγραμματιστής προτείνει την ενημέρωση των χρηστών από έναν ειδικό για οποιοδήποτε πρόβλημα και αν αντιμετωπίσουν

«ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Α: Χωρίς να θέλω να σας τρομοκρατήσω ο υπολογιστής σας είναι ασφαλής μόνο όταν είναι κλειστός και εκτός πρίζας. Τα antivirus που πουλιούνται στην αγορά προσφέρουν απλά ένα Α ‘ Επίπεδο προστασίας και σίγουρα πρέπει να τα χρησιμοποιούμε αλλά δεν σημαίνει ότι είμαστε απόλυτα ασφαλής εδώ 15 χρόνοι hacker έχουν

εισβάλει στα αρχεία της NASA και του πεντάγωνου φανταστείτε πόσο εύκολα εισβάλλουν στους δικούς μας υπολογιστές .Πρόταση μου είναι να θωρακίζουμε τον υπολογιστή μας να μην έχουμε προσωπικό μας υλικό αποθηκευμένο ,να μην ανοίγουμε e-mail από ξένους και να ενημερωνόμαστε από ειδικούς για οτιδήποτε μας απασχολεί» .

«ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ Β: Βασικά πρέπει να είμαστε πιο προσεκτικοί και να μπαίνουμε μόνο σε έγκυρες σελίδες. Σε σελίδες οι οποίες είναι κλειδωμένες και υπάρχει η προστασία από αυτόν που έχει φτιάξει τη σελίδα. Να είναι πιστοποιημένη η σελίδα. Επίσης για να είμαστε ασφαλείς ότι δεν θα χάσουμε τίποτα από τα δεδομένα μας, θα πρέπει να τα κρατάμε αποθηκευμένα σε εξωτερικά αποθηκευτικά μέσα(εξωτερικός σκληρός δίσκος κ.α) και όταν είμαστε συνδεδεμένοι στο internet να μην έχουμε συνδεδεμένο τον εξωτερικό σκληρό δίσκο, για παράδειγμα, στον υπολογιστή μας. Επιπλέον ένας άλλος τρόπος να προστατέψουμε τα δεδομένα μας είναι να κρατάμε back up αρχεία. Να τα zipπάρουμε και να κρυπτογραφούμε τα αρχεία μας, βάζοντας τους και κωδικό απο zipπαρίσματος. Έτσι και να μας τα κλέψει κάποιος δύσκολα θα καταφέρει να τα ανοίξει. Εντελώς πληροφοριακά η ηλεκτρονική κρυπτογράφηση ξεκίνησε την εποχή του Β’ Παγκοσμίου Πολέμου από τους Άγγλους και έχει μείνει γνωστό ως «αίνιγμα». Παρόλα αυτά και τα συγκεκριμένα αποκωδικοποιήθηκαν. Είναι με το πόσο θέλει να ασχοληθεί ο άλλος. Αν σε βάλει στο μάτι και ασχοληθεί έχει μεγάλες πιθανότητες να το καταφέρει. Για να λέμε και τα πράγματα με το όνομά τους, ένας hacker δεν ξεκινάει να στήσει ένα πρόγραμμα ιού από την αρχή. Η βάση των προγραμμάτων αυτών γίνεται από τις εταιρείες (Microsoft, Linux κ.α), μετά τα παίρνουν οι hackers και τα τροποποιούν σύμφωνα με αυτό που θέλουν να επιτύχουν, είτε να σου καταστρέψουν τον υπολογιστή, είτε να σου κάνουν τον υπολογιστή σου πιο αργό και πολλά άλλα. Και όλα αυτά γίνονται για να πουλάνε οι εταιρείες τα προστατευτικά προγράμματα που προανέφερα όπως antivirus κ.α Καταλαβαίνεις τι γίνεται!»

Παραπάνω κατηγοριοποιήσαμε τις προτάσεις των προγραμματιστών για την καταπολέμηση του Ηλεκτρονικού Εγκλήματος και για την προστασία των θυμάτων.

Από τα παραπάνω προέκυψε ότι οι προγραμματιστές προτείνουν αρχικά την χρήση προγραμμάτων προστασίας, όπως antivirus κ.α, για την προστασία των χρηστών. Παρόλα αυτά μας ενημερώνουν πως οι χρήστες έχουν μερική προστασία ακόμη και με την χρήση των συγκεκριμένων προγραμμάτων. Όπως χαρακτηριστικά μας αναφέρουν οι συνεντευξιαζόμενοι «είναι το πόσο θέλει να ασχοληθεί κάποιος για να εισβάλλει στον υπολογιστή σου». Επίσης ένας από τους προγραμματιστές

αναφέρει πόσο προσεκτικοί πρέπει να είναι οι χρήστες με τα μηνύματα που λαμβάνουν από άγνωστο αποστολέα. Είναι καλύτερο να μην ανοίγονται τέτοιου είδους e-mail. Επιπλέον και οι δύο προγραμματιστές μας τονίζουν την σημαντικότητα του να αποθηκεύουμε τα προσωπικά μας δεδομένα σε εξωτερικά αποθηκευτικά μέσα και κατά την πλοήγηση μας στο διαδίκτυο να μην τα έχουμε συνδεδεμένα στον υπολογιστή μας. Μία ακόμη σημαντική πρόταση –συμβουλή που προτείνεται από έναν από τους προγραμματιστές είναι η αποφυγή εισόδου των χρηστών σε μη έγκυρες σελίδες. Κάτι επίσης σημαντικό που μας πρότεινε ένας εκ των δύο προγραμματιστών είναι το να κρατούν οι χρήστες back up αρχεία τα οποία θα τα κρυπτογραφούν. Έτσι ακόμη και αν κάποιος τους τα κλέψει θα είναι πολύ δύσκολο να τα αποκρυπτογραφήσει και να τα ανοίξει. Τέλος ένας εκ των δύο προγραμματιστών πρότεινε στους χρήστες που αντιμετωπίζουν κάποιο πρόβλημα να μην διστάζουν να ζητήσουν τη συμβουλή από κάποιον ειδικό για το πρόβλημα που αντιμετωπίζουν. Στο παράρτημα παρουσιάζεται η πλήρη συνέντευξη και των δύο προγραμματιστών .

ΚΕΦΑΛΑΙΟ 4

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΕΡΕΥΝΑΣ

Οι περιπτώσεις που μελετήθηκαν στην παρούσα έρευνα, αφορούν τις απόψεις 8 ειδικών σχετικά με το Ηλεκτρονικό Έγκλημα, οι 6 εκ των οποίων αναλύθηκαν εκτενέστερα ενώ οι υπόλοιπες 2 παραθέτονται στο παράρτημα. Ύστερα από την επιλογή των ευρημάτων, δημιουργήθηκε από τις ερευνήτριες ένα πλαίσιο κατηγοριών, όπου κατηγοριοποιήθηκαν οι απόψεις των ειδικών ανάλογα με την ειδικότητά τους καταλήγοντας στις εξής κατηγορίες:

→ Αστυνομικοί
→ Ψυχολόγοι
→ Προγραμματιστές

Ύστερα από την κατηγοριοποίηση τα δεδομένα των συνεντεύξεων αναλύθηκαν και προέκυψαν τα ακόλουθα:

- Οι μορφές απάτης και εγκλήματος που εμφανίζουν μεγαλύτερη συχνότητα είναι κυρίως οι οικονομικές απάτες και ακολουθούν οι απάτες και τα εγκλήματα μέσω των κοινωνικών δικτύων, όπως η προσβολή της προσωπικότητας και η κλοπή των προσωπικών δεδομένων που μπορεί να συσχετιστεί με τις οικονομικές απάτες. Στη συνέχεια μέσω των κοινωνικών δικτύων που προαναφέρθηκαν, μεγαλύτερη συχνότητα εμφάνισης παρουσιάζουν οι αυτοκτονίες που γίνονται μέσα από τα κοινωνικά δίκτυα είτε παρακινώντας κάποιον να αυτοκτονήσει είτε απλά ανακοινώνοντας ο χρήστης την δική του αυτοκτονία. Με όχι μικρότερο βαθμό συχνότητας ακολουθούν η διακίνηση πορνογραφικού υλικού και η σεξουαλική παρενόχληση ανηλίκων και μη, που διαπράττονται κυρίως μέσα από οργανωμένα κοινωνικά δίκτυα.
- Το νομοθετικό πλαίσιο που έγκειται του θέματος της Ηλεκτρονικής Εγκληματικότητας δεν θεωρείται επαρκές διότι παρουσιάζει κενά και ελλείψεις με αποτέλεσμα να δυσκολεύει την ικανοποιητική και πλήρη αντιμετώπιση της δίωξη του Ηλεκτρονικού Εγκλήματος.,

εξαιτίας της διχογνωμίας που υπάρχει σχετικά με την άρση του απορρήτου αλλά και στις διαφορές που εμφανίζει το κάθε νομοθετικό πλαίσιο μιας χώρας σε σχέση με το νομοθετικό πλαίσιο μιας άλλης χώρας, δυσκολεύοντας τις αρμόδιες αρχές της κάθε χώρας να χαρακτηρίσουν μια πράξη ηλεκτρονικής εγκληματικότητας ως παράνομη ή νόμιμη. Τέλος, η αδυναμία του νομοθετικού πλαισίου εμφανίζεται επίσης στα ελαστικά μέτρα που λαμβάνει το ίδιο το νομοθετικό για τη μη προφυλάκιση των ενόχων , για απάτες ή εγκλήματα άνω των δέκα ετών με αποτέλεσμα την αύξηση των δραστών.

- Η παράνομη εισβολή ενός hacker σε ένα σύστημα αρχείων γίνεται κυρίως με την αποστολή e-mail , όπου πατώντας log in ο χρήστης που έλαβε το e-mail, μεταφέρεται σε εικονικό site δίνοντας τη δυνατότητα στον δράστη να εισβάλλει στα προσωπικά αρχεία του θύματος και να τα αξιοποιήσει με όποιον τρόπο επιθυμεί ο ίδιος. Επίσης, ένας ακόμη πολύ συχνός τρόπος εισβολής των hackers σε υπολογιστές χρηστών – θυμάτων είναι με την βοήθεια ιών , για παράδειγμα Trojan horse.
- Όσον αφορά τις προτάσεις των ειδικών για την προστασία των χρηστών από το φαινόμενο της ηλεκτρονικής εγκληματικότητας υπήρξε ομοφωνία πως δεν μπορούν να προστατευτούν οι χρήστες ολοκληρωτικά αλλά εν μέρει με τη χρήση ειδικών προγραμμάτων προστασίας , όπως antivirus, αλλά και με την ενημέρωση και ευαισθητοποίηση της κοινότητας από ειδικούς σχετικά με τις ενέργειες που πρέπει να εφαρμόσει ο κάθε χρήστης για την προσωπική του προστασία. Επίσης θεωρήθηκε εξίσου σημαντικό το να προσληφθούν ειδικοί, κοινωνικοί λειτουργοί και ψυχολόγοι, στις αρμόδιες υπηρεσίες και οργανώσεις που ασχολούνται με το φαινόμενο της ηλεκτρονικής εγκληματικότητας καθώς επίσης και η τοποθέτηση ειδικών σε σχολεία για την πρόληψη κυρίως του φαινομένου. Τέλος, η λήψη κατασταλτικών μέτρων από τις αστυνομικές αρχές ,θεωρήθηκε εξίσου σημαντική ενέργεια.

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΕΣ ΕΡΕΥΝΕΣ

5.1 Συμπεράσματα

Λόγω της μειωμένης βιβλιογραφίας σε σχέση με το φαινόμενο του ηλεκτρονικού εγκλήματος , καθώς επίσης και την ελλιπή ύπαρξη βιβλίων , τόσο στην βιβλιοθήκη του Α.Τ.Ε.Ι Πατρών, αλλά και άλλων δημόσιων βιβλιοθηκών, παρεμποδίστηκε πολύ η συλλογή βιβλιογραφικής ανασκόπησης. Εξαιτίας των παραπάνω διαπιστώθηκε πως το αντίστοιχο θέμα δεν έχει διεξαχθεί στην Ελλάδα και κυρίως στον κλάδο των ανθρωπιστικών επιστημών, χαρακτηρίζοντάς την ως πρωτότυπη.

Η παρούσα πτυχιακή εργασία έχει ως θέμα: «Μορφές Ηλεκτρονικού Εγκλήματος και προτάσεις για την μείωση του φαινομένου: Οι απόψεις των ειδικών που ασχολούνται με το Ηλεκτρονικό Έγκλημα».

Το μεθοδολογικό πλαίσιο που χρησιμοποιήθηκε από τις ερευνήτριες στην συγκεκριμένη μελέτη ήταν η ποιοτική έρευνα με εργαλείο τους την ημι-δομημένη συνέντευξη. Από την ολοκλήρωση της βιβλιογραφικής ανασκόπησης και της έρευνας προκύπτουν τα ακόλουθα συμπεράσματα.

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές στην καθημερινότητα μας και γενικότερα στην ανθρώπινη επαφή. Η εκρηκτική διάδοση χρήσης του διαδικτύου από ανθρώπους ανεξαρτήτως ηλικίας, εκπαίδευσης και εθνικής ή γεωγραφικής προέλευσης, είναι ίσως το χαρακτηριστικό γνώρισμα της εποχής μας. Το διαδίκτυο προσφέρει στο άτομο την ταχύτατη και ταυτόχρονη επαφή με διαφορετικές κουλτούρες και διαφορετικούς πολιτισμούς. Προσφέρει επίσης τη δυνατότητα ενός αλλαγμένου βιώματος του χώρου και του χρόνου, την ελευθερία μεταμόρφωσης του υποκειμένου σε άπειρες ψηφιακές περσόνες, εικονικές αλλά πανταχού παρούσες.(Λάζος, 2001)

Ο μαγικός κόσμος του διαδικτύου είναι ένα «σίγουρο καταφύγιο» από τις εντάσεις και τις πιέσεις της καθημερινότητας. Δίνοντάς στο χρήστη πολλές

φορές την ευκαιρία μιας «δεύτερης ζωής» εικονικής, αλλά πολύ πιο ενδιαφέρουσας από την αληθινή. Επιπλέον το νέο ψηφιακό περιβάλλον διευκολύνει την εξ αποστάσεως σύναψη συναλλαγών εκ μέρους των πολιτών -καταναλωτών με οικονομία χρόνου και χρήματος. Μεταξύ αυτών περιλαμβάνονται συναλλαγές με το Δημόσιο, υποβολή φορολογικών δηλώσεων και ΦΠΑ, ηλεκτρονικές κρατήσεις και αγορές εισιτηρίων μεταφοράς και θεαμάτων, ηλεκτρονικές πληρωμές, τηλε-αγορές, διαχείριση μέσω διαδικτύου τραπεζικών λογαριασμών (web banking), τηλε-ιατρική, πρόσβαση σε χρηστικές υπηρεσίες πληροφοριών ή σε υπηρεσίες διασκέδασης και ψυχαγωγίας. Η πρόσβαση στον κυβερνοχώρο και η μετάβαση στην Κοινωνία της Πληροφορίας συνεπάγεται πολλαπλά οφέλη για κάθε πολίτη ατομικά και για την εθνική οικονομία συνολικά.(Βλαχόπουλος, 2007)

Παρόλο όμως τη ραγδαία εξέλιξη της τεχνολογίας, την ανάπτυξη της πληροφορικής και την ευρύτατη χρήση του Διαδικτύου, που αναμφίβολα έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα». (Λάζος ,2001)

Από την βιβλιογραφική ανασκόπηση προκύπτει ότι στο Ηλεκτρονικό Έγκλημα ανήκει η διαδικτυακή απάτη, η εξύβριση ή δυσφήμηση τρίτων μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, η εκβίαση μέσω παρανόμως κτηθέντων φωτογραφιών ή προσωπικών δεδομένων, η διασπορά μέσω δικτύων κακόβουλου λογισμικού υπό μορφή «ιών», η κατοχή και διακίνηση απαγορευμένου υλικού παιδικής πορνογραφίας και η υποκλοπή στοιχείων πιστωτικών καρτών με συνέπεια την αθέμιτη χρέωση του κατόχου τους. Στην ίδια κατηγορία παραβατικής συμπεριφοράς εντάσσεται και η δημιουργία ηλεκτρονικών «προφίλ» καταναλωτών μέσω ανάλυσης των επισκέψεων αυτών σε ιστοσελίδες με συνέπεια την προς αυτούς μαζική

αποστολή ανεπιθύμητης εμπορικής αλληλογραφίας, η προσβολή πνευματικών δικαιωμάτων ,η πειρατεία λογισμικού και ονομάτων χώρου, η μεταφορά κεφαλαίων μέσω υποκλοπής κωδικών από τον τραπεζικό λογαριασμό του ανύποπτου καταναλωτή στους λογαριασμούς των εισβολέων .Σε σοβαρές περιπτώσεις ηλεκτρονικού εγκλήματος εντάσσονται ακόμα τρομοκρατικές επιθέσεις με αθέμιτη διείσδυση τρίτων σε πληροφοριακά συστήματα κρατικών επιχειρήσεων και οργανισμών κοινής ωφελείας. Αυτές έχουν ως συνέπεια την υποκλοπή από τον τεχνοκρατικών ή στρατιωτικών απορρήτων, την παράλυση ζωτικών λειτουργιών στους τομείς της ενέργειας, των μεταφορών ή των επικοινωνιών, ή τη βιομηχανική κατασκοπεία. (Βλαχόπουλος, 2007)

Ύστερα από την διεξαγωγή της έρευνας τα κυριότερα ευρήματα που προέκυψαν είναι: Η μεγάλη συχνότητα εμφάνισης που επικρατεί στις οικονομικές απάτες και στη συνέχεια ακολουθούν οι απάτες και τα εγκλήματα μέσω των κοινωνικών δικτύων. Πράγματι η ραγδαία εξάπλωση των κοινωνικών δικτύων και η εύκολη αποδοχή και χρήση αυτών κυρίως από ανήλικους έχει οδηγήσει στην αύξηση του ηλεκτρονικού εγκλήματος. Πρωτοπόρος όλων των κοινωνικών δικτύων είναι το facebook όπου λόγω της διαδεδομένης χρήσης του και της ανωνυμίας που προσφέρει ενισχύει την τέλεση εγκληματικών πράξεων. Επιπλέον, η αδυναμία του νομοθετικού πλαισίου δυσκολεύει την ικανοποιητική και πλήρη αντιμετώπιση και δίωξη του Ηλεκτρονικού Εγκλήματος., εξαιτίας της διχογνωμίας που υπάρχει σχετικά με την άρση του απορρήτου αλλά και στις διαφορές που εμφανίζει το κάθε νομοθετικό πλαίσιο μιας χώρας σε σχέση με το νομοθετικό πλαίσιο μιας άλλης χώρας, δυσκολεύοντας τις αρμόδιες αρχές της κάθε χώρας να χαρακτηρίσουν μια πράξη ηλεκτρονικής εγκληματικότητας ως παράνομη ή νόμιμη. Τέλος η έλλειψη ειδικών, κοινωνικών λειτουργών κι ψυχολόγων από τις υπηρεσίες και τις οργανώσεις που ασχολούνται με την καταπολέμηση του ηλεκτρονικού εγκλήματος καθώς και η απουσία των ειδικών από τα σχολεία ήταν ένα θέμα που φάνηκε πως απασχολούσε τους ειδικούς καθώς το ανέφεραν συνεχώς κατά την διάρκεια των συνεντεύξεων τους.

Εν κατακλείδι είναι σκόπιμο να αναφερθεί ότι ύστερα από την ανάλυση των δεδομένων ανακαλύψαμε τον συσχετισμό των κοινωνικών δικτύων και

κυρίως του facebook, με την τέλεση εγκληματικών πράξεων κυρίως σε ανήλιους, όπως σεξουαλική παρενόχληση, προσβολή προσωπικότητας, σχολικός εκφοβισμός(cyberbullying) και κλοπή προσωπικών δεδομένων. Θα ήταν λοιπόν ενδιαφέρον να πραγματοποιηθεί στο μέλλον έρευνα που να εξετάσει αντίστοιχο θέμα με το παραπάνω ώστε να διαπιστωθεί η εγκυρότητά του.

5.2 Προτάσεις ερευνητριών για αντιμετώπιση του φαινομένου

→ Ενημέρωση και ευαισθητοποίηση της κοινότητας από ειδικούς σχετικά με τις ενέργειες που πρέπει να εφαρμόσει ο κάθε χρήστης για την προσωπική του προστασία.

→ Τοποθέτηση ειδικών, κοινωνικών λειτουργών και ψυχολόγων, στις αρμόδιες υπηρεσίες και οργανώσεις που ασχολούνται με το φαινόμενο της ηλεκτρονικής εγκληματικότητας καθώς επίσης και η τοποθέτηση ειδικών σε σχολεία για την πρόληψη κυρίως του φαινομένου μέσα από την δημιουργία role playing σχετικά με το ηλεκτρονικό έγκλημα που θα πραγματοποιούνται στα σχολεία από τους ειδικούς..

→ Τέλος η θεσμοθέτηση ενός παγκόσμιου νομοθετικού πλαισίου σχετικά με το ηλεκτρονικό έγκλημα έτσι ώστε να καλυφτούν τα κενά και οι ελλείψεις που προκύπτουν από την μη ύπαρξη ενός παγκόσμιου νομοθετικού πλαισίου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

1. Αναγνωστοπούλου, Τ.(2002). « Βασικές αρχές δεοντολογίας στην ψυχοθεραπεία». Θεσσαλονίκη: Ινστιτούτο Ψυχολογίας και Υγείας.
2. Αργυρόπουλος ,Α.(2001) «Ηλεκτρονική εγκληματικότητα» σελ.80, Αθήνα: Αντ .Ν.Σάκκουλας,
3. Βλαχόπουλος ,Κ,(2007) «Ηλεκτρονικό Έγκλημα», σελ. 63 Αθήνα: Νομική Βιβλιοθήκη
4. Ζαννή, Α.(2005) «Το διαδικτυακό έγκλημα» ,σελ.88,93,Αθήνα :Αντ.Ν. Σάκκουλας
5. Ιγγλεζάκης,Ι .(2006) «Εισαγωγή στο δίκαιο της πληροφορικής» ,σελ.78, Θεσσαλονίκη: Αντ. Ν. Σάκκουλα
6. Ιωσηφίδης Θ. & Μ.Σπυριδάκης (2006) « Ποιοτική Κοινωνική Έρευνα. Μεθοδολογικές προσεγγίσεις και ανάλυση δεδομένων». Αθήνα: Κριτική
7. Καρακώστας,Ι .(2001) «Δίκαιο και ίντερνετ» ,σελ.65 ,Αθήνα : Αντ. Ν. Σάκκουλα
8. (Κυριαζή, 1999). Κυριαζή, Ν.,(1999). Η κοινωνιολογική έρευνα. Αθήνα: Ελληνικά Γράμματα
9. Λάζος,Γ .(2001) «Πληροφορική και έγκλημα». σελ.76 ,55,35, 123,143,145, Αθήνα :Νομική Βιβλιοθήκη ,
10. Λέανδρος ,Ν(2005) «Το διαδίκτυο :Ανάπτυξη και αλλαγή» ,σελ 250,Αθήνα: Καστανιώτης
11. Μυλωνόπουλος,Χ.(2007) «Ποινικό Δίκαιο-Γενικό Μέρος Ι», Αθήνα: Π.Ν.Σάκκουλα
12. Τσουραμάνης ,Χ.(2005) « Εγκληματικότητα» Αθήνα: Κατσαρού Β.
13. Cohen & Manion , 1994)« Μεθοδολογία εκπαιδευτικής έρευνας». Αθήνα: Μεταίχμιο.
14. Furnell , S. (2006) « Κυβερνοέγκλημα » Αθήνα :Παπαζήση
15. Mason, S. (1996). «Η διεξαγωγή της ποιοτικής έρευνας». Αθήνα: Ελληνικά Γράμματα
16. Thio,A.(2008) «Παρεκκλίνουσα συμπεριφορά », σελ.583-568 ,Αθήνα :Ελλήν

ΑΡΘΡΑ ΣΕ ΠΕΡΙΟΔΙΚΑ

17. Κατερίνα Μάτσα,(2009). Εξάρτηση από το Διαδίκτυο: η πιο σύγχρονη μορφή τοξικομανίας. Τετράδια Ψυχιατρικής 12/2009 τ.108, σσ78-86

ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

18. Yount, Lisa.(2006) «Does the internet increase the risk of crime?»Detroit,Mitch:Greenhaven press
19. Jenkins ,Philip.(2001) «Beyond Tolerence: Child Pornography on the internet» New York :New York university press
20. Newton, Michael(2004) «The encyclopedia of high-tech crime and crime –fighting» New York: Facts on file

ΠΗΓΕΣ ΔΙΑΔΙΚΤΥΟΥ

21 . «Διαδίκτυο και Δίκαιο», http://www.lawnet.gr/pages/eofn/2/cybercrime.asp (ανάκτηση 17/01/2009)

22 . Βλαχόπουλος Κ,(2007) «Δικτυακός τόπος για το ηλεκτρονικό έγκλημα»http://www.e-crime.gr/nomothesia.htm (ανάκτηση 17/01/2010) , τελευταία ενημέρωση 10-05-2008

23 . Ομάδα Δράσης για την Ψηφιακή Ασφάλεια(2008). http://www.dart.gov.gr/?q=node/28

(ανάκτηση 20/12/2009)

24. Φαφούτη, Ξ.(2008) « Δίωξη ηλεκτρονικού εγκλήματος του ίντερνετ και οι μορφές του» http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm(ανάκτηση 10/01/2010, 13:28)

25. Woodruff, C., Gregory, S.(2005) “Profile of internet gamblers: Betting on the future” UNLV Gaming Research & Review Journal,9, 1-14

http://www.cababstractsplus.org/abstracts/Abstract.aspx?AcNo=200530780 1 (ανάκτηση 26/01/2010 17:12)

26 . Griffiths ,M., Parke,J.(2002)“The Social Impact of Internet Gambling” Social Science Computer Review ,20,312-320 http://www.eou.edu/~jdense/griffithsparke.pdf (ανάκτηση 15/02/2010 ,12:09)

27 . LAWNET SA, (2004) «Ηλεκτρονικό έγκλημα»

http://www.goonline.gr/ebusiness/specials/article.html?article_id=341

(ανάκτηση 25/02/2010 01:20)

28 . ΚΥΔ του Πανεπιστημίου Μακεδονίας «Ηλεκτρονικές απάτες στο διαδίκτυο »

http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf(ανάκτηση 25/02/2010)

29.Παπαβασιλείου,Σ.(2009) «Κλοπή ταυτότητας στο Διαδίκτυο» http://www.fititis.gr/fititis2/index.php?option=com_content&task=view&id=3392&Itemid=11 (ανάκτηση 29/02/2010 20:00)

30 .Vangie ,A.(2006) «Identity Theft»

,http://translate.google.gr/translate?hl=el&langpair=en%7Cel&u=http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp (ανάκτηση 29/02/2010 01:30)

31.¨Identity Theft And Your Social Security Number¨(2006),http://retirement.gov/multilanguage/Greek/10064-GR.pdf(ανάκτηση 20/03/2010 22:50)

32 . Webb,G.(2001)¨Sex and the internet¨Yahoo! internet Life ,7,88-98

,http://sax.sagepub.com/cgi/content/refs/19/4/449 (ανάκτηση 03/04/2010 21:00)

33 . Wysoscki, K.(1998)¨Let your fingers do the talking: Sex on an adult chat –line¨sexualities ,Vol.1,pp.425-452.

http://sexualities.sagepub.com/cgi/content/abstract/1/4/425(ανάκτηση10/04/2010 ,14:00)

ΠΑΡΑΡΤΗΜΑ

Α. ΟΔΗΓΟΣ ΣΥΝΕΝΤΕΥΞΗΣ

Οδηγός Συνέντευξης ανά κατηγορίες

- **ΠΡΩΤΗ ΚΑΤΗΓΟΡΙΑ: ΑΣΤΥΝΟΜΙΚΟΙ-ΝΟΜΙΚΟΣ**

1η φάση (γνωριμία)

2η φάση (εις βάθους συνέντευξη)

1. Τι θεωρείται παράνομο περιεχόμενο στο διαδίκτυο;
2. Ποιές είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;
3. Πώς φτάνουν τα θύματα σε εσάς και πως γίνεται η καταγγελία; μπορεί να τηρηθεί η ανωνυμία;
4. Πώς εξακριβώνεται μια υπόθεση; Ποιες ενέργειες γίνονται από την υπηρεσία σας μετά από την κατάθεση της καταγγελίας;
5. Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητα;
6. Ποιές οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

- **ΔΕΥΤΕΡΗ ΚΑΤΗΓΟΡΙΑ:ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ**

1η φάση (γνωριμία)

2η φάση (εις βάθους συνέντευξη)

1. Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;
2. Πώς μπορεί ένας hacker να εισβάλει στον υπολογιστή μας και τι μπορεί να κάνει σε αυτό ;

3. Πως μπορούμε να προστατευθούμε από το φαινόμενο του ηλεκτρονικού εγκλήματος; ποιες είναι οι προτάσεις σας;

- **ΤΡΙΤΗ ΚΑΤΗΓΟΡΙΑ:ΨΥΧΟΛΟΓΟΙ**

1η φάση (γνωριμία)

2η φάση (εις βάθους συνέντευξη)

1. Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;
2. Θα ήθελα να μου πείτε λίγα λόγια για τον ρόλο του ψυχολόγου στην αντιμετώπιση του φαινομένου και στην προστασία των θυμάτων;
3. Ποιές οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

- **ΤΕΤΑΡΤΗ ΚΑΤΗΓΟΡΙΑ:ΔΙΔΑΣΚΟΥΣΑ**

1η φάση (γνωριμία)

2η φάση (εις βάθους συνέντευξη)

1. Ποιές είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο και αν έχετε συναντήσει κάποια από αυτές μέσα από την δουλειά σας;
2. Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητα;
3. Τι θα συμβουλεύατε στους γονείς και τους εκπαιδευτικούς να κάνουν για να προλάβουν τα εγκλήματα μέσω διαδικτύου;
4. Ποιές οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

Β.ΑΥΤΟΥΣΙΕΣ ΣΥΝΕΝΤΕΥΞΕΙΣ ΕΙΔΙΚΩΝ

1η ΣΥΝΕΝΤΕΥΞΗ

ΤΟΠΟΘΕΣΙΑ:ΓΡΑΦΕΙΟ ΚΑΘΗΓΗΤΩΝ 1ΟΥ ΕΠΑΛ ΝΑΟΥΣΑΣ

ΕΙΔΙΚΟΤΗΤΑ: ΔΙΔΑΣΚΟΥΣΑ ΑΝΟΙΧΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΗΜΕΙΩΣΗ: Η συνέντευξη πραγματοποιήθηκε στο 1ο ΕΠΑΛ Νάουσας μετά τη λήξη του 2ου Πανελλήνιου εκπαιδευτικού συνεδρίου Ημαθίας με θέμα «Ψηφιακές και διαδικτυακές Εφαρμογές στην Εκπαίδευση»

ΚΟΙΝ.ΛΕΙΤ: Γνωρίζουμε ότι η ομιλία σας αφορούσε τον εκφοβισμό μέσω διαδικτύου αλλά θα θέλαμε να μας πείτε, εάν θέλετε, αν γνωρίζετε ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο και αν έχετε συναντήσει κάποια από αυτές μέσα από την δουλειά σας;

ΔΙΔΑΣΚΟΥΣΑ ΑΠΘ: Όλοι αντιλαμβανόμαστε πως το διαδίκτυο έχει εισβάλλει για τα καλά στην ζωή μας και πως εκτός από τα οφέλη που μας προσφέρει, καραδοκεί και πολλούς κινδύνους. Είμαι και εγώ μάνα και δεν θα σας κρύψω τον φόβο μου και την αγωνία μου για την επίτευξη μόνο της σωστής και ασφαλής χρήσης του διαδικτύου από τα παιδιά μου. Στο Πανεπιστήμιο διδάσκω Πληροφορική αλλά αναφερόμαστε και στην σωστή χρήση του διαδικτύου και στην προστασία των χρηστών. Θέλω να σας πω ότι έχω ασχοληθεί πολύ με το χώρο του διαδικτύου και έχω συνεργαστεί πολλές φορές με την Δίωξη Ηλεκτρονικού Εγκλήματος, με την safe Line, με την safe internet αλλά και με το Ιπποκράτειο Νοσοκομείο Θεσσαλονίκης και συγκεκριμένα με το τμήμα εθισμού στο Διαδίκτυο για την συλλογή πληροφοριών, την καταγραφή εργασιών αλλά και την διεξαγωγή ερευνών σχετικά με το διαδίκτυο. Οι συνηθέστερες μορφές απάτης είναι η οικονομικές και η παρενόχληση μέσω διαδικτύου, όπως ο σχολικός εκφοβισμός, η δυσφήμιση ενός ατόμου με ανάρτηση φωτογραφιών ή ενοχλητικών μηνυμάτων καθώς και η σεξουαλική παρενόχληση μέσω διαδικτύου. Φυσικά η πορνογραφία κι οι υπόλοιπες μορφές απάτης δεν έχουν μικρά ποσοστά, ίσα ίσα πλησιάζουν πολύ τις επικρατούσες μορφές απάτης που προανέφερα. Προσωπικά έχω ασχοληθεί περισσότερο με τον

εκφοβισμό μέσω διαδικτύου και πιο συγκεκριμένα με τον σχολικό εκφοβισμό και την παρενόχληση στον κυβερνοχώρο. Θεωρώ ότι όλα ξεκινούν από το σχολείο και εκεί πρέπει να στρέψουμε την προσοχή μας. Φυσικά αυτό δεν σημαίνει πως το σχολείο μόνο του μπορεί να φέρει θετικά αποτελέσματα για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Απαραίτητη προϋπόθεση για την επίτευξη του συγκεκριμένου στόχου είναι η συνεργασία των γονέων και των εκπαιδευτικών. Γι αυτό και εμείς διοργανώνουμε ημερίδες και σεμινάρια σε σχολεία για την ενημέρωση των παιδιών, των εκπαιδευτικών και των γονέων για το διαδίκτυο και τους κινδύνους που αυτό κρύβει. Ένα τέτοιο σεμινάριο πραγματοποιήθηκε και σήμερα στην περιοχή σας.

ΚΟΙΝ.ΛΕΙΤ: Τι θα συμβουλεύατε στους γονείς και τους εκπαιδευτικούς να κάνουν για να προλάβουν τα εγκλήματα μέσω διαδικτύου;

ΔΙΔΑΣΚΟΥΣΑ ΑΠΘ: Αρχικά όπως ακούσατε και στην ομιλία μου ανέφερα κάποιες συμβουλές τόσο για τα παιδιά, να μην δημοσιεύουν προσωπικά τους στοιχεία και φωτογραφίες με προσωπικές τους στιγμές στο διαδίκτυο γιατί θα πρέπει να ξέρουν πως ότι ανεβαίνει στο διαδίκτυο ακόμη και αν το σβήσουμε μετά αυτό συνεχίζει να υπάρχει στο server και μπορεί κάποιος να το ξαναβρεί ακόμη και μετά από χρόνια δημιουργώντας προβλήματα στο άτομο που απεικονίζεται στις φωτογραφίες ή στο άτομο για το οποίο έχουν γίνει κάποια αρνητικά σχόλια, τόσο στη δουλεία του ή ακόμη και στην οικογένεια που πιθανόν να έχει δημιουργήσει. Επίσης οι συμβουλές που έδωσα σε γονείς και εκπαιδευτικούς αφορούσαν αρχικά την ενημέρωση των παιδιών για τον κυβερνοχώρο, εξηγώντας τους πως το διαδίκτυο είναι παντού και πουθενά, πως δεν πηγαίνουμε εμείς σε αυτό αλλά κάνουμε log in και έρχεται αυτό σε εμάς και γενικότερα να ενημερώσουν τα παιδιά πως το προφίλ του χρήστη που μιλούν μπορεί να μην είναι έτσι όπως παρουσιάζεται αλλά να είναι εικονικό και να εξηγήσουν τους λόγους που κάποιος μπαίνει στην διαδικασία να φτιάξει ένα ψεύτικο προφίλ. Τέλος ανέφερα κάποια σημάδια που εμφανίζουν τα παιδιά θύματα αλλά και τα παιδιά δράστες του διαδικτυακού εγκλήματος. Σε αυτά πρέπει να δίνουν περισσότερη προσοχή οι γονείς και οι εκπαιδευτικοί και

να πλησιάζουν τα παιδιά για να μάθουν τι συμβαίνει. Δεν είναι τυχαίο ότι μέσα από έρευνες έχει βρεθεί ότι το 60% των παιδιών δεν μιλούν στους γονείς τους εάν πέσουν θύματα.

ΚΟΙΝ.ΛΕΙΤ: Ποιες οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

ΔΙΔΑΣΚΟΥΣΑ ΑΠΘ: Θεωρώ πολύ σημαντικό το κομμάτι της ενημέρωσης της κοινότητας για το συγκεκριμένο θέμα. Επίσης η τοποθέτηση κοινωνικών λειτουργών και ψυχολόγων στα σχολεία είναι κάτι που πρέπει να γίνει άμεσα διότι οι ειδικοί σίγουρα θα εντοπίσουν τέτοιες περιπτώσεις και θα προβούν σε ενέργειες για να τις σταματήσουν πριν να είναι αργά. Με την τοποθέτηση των ειδικών στα σχολεία θα δημιουργηθούν βιωματικά εργαστήρια όπου θα γίνονται role playing όπου τα παιδιά θα διαδραματίζουν το ρόλο και του θύτη και του θύματος και μέσα από αυτό ο ειδικός όχι μόνο θα αντιλαμβάνεται προβληματικές συμπεριφορές αλλά θα είναι και ένας τρόπος να συμβουλέψει τα παιδιά για το πώς θα πρέπει να χειριστούν διάφορες περιπτώσεις που σχετίζονται με το διαδίκτυο.

ΚΟΙΝ.ΛΕΙΤ: Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητας;

ΔΙΔΑΣΚΟΥΣΑ ΑΠΘ: Η αλήθεια είναι πως δεν είναι επαρκές το νομοθετικό πλαίσιο διότι κάτι που μπορεί να είναι παράνομο σε μια χώρα σε κάποια άλλη μπορεί να μην θεωρείται παράνομο. Γι αυτό στις 15 Μαΐου ο κ. Παπαντωνίου που είναι στη Δίωξη Ηλεκτρονικού Εγκλήματος θα πάρει μέρος σε Συνέδριο στην Ευρώπη όπου θα συζητήσουν για την ύπαρξη ενός Ενιαίου Παγκόσμιου νομοθετικού πλαισίου για την αντιμετώπιση της ηλεκτρονικής εγκληματικότητας. Δεν εύκολο να εντοπίσεις έναν εγκληματία στο διαδίκτυο λόγο της ανωνυμίας και της μεγάλης δικτύωσης που υπάρχει. Επίσης όπως ανέφερα στην ομιλία μου το Ελληνικό νομοθετικό πλαίσιο ορίζει ότι για εγκλήματα διαδικτύου που διαπράττονται από παιδιά μέχρι 11 ετών, δεν τιμωρούνται τα παιδιά αλλά οι γονείς τους. Παρόλα αυτά για παιδιά πάνω από 11 ετών τιμωρούνται τα παιδιά όχι με τόσο αυστηρές ποινές όπως αρμόζει με τη βλάβη που προκάλεσαν στο θύμα τους διότι δεν θέλουμε να στιγματίσουμε τα παιδιά θύτες. Τι γίνεται όμως

με τον στιγματισμό των παιδιών- θύματα; Είναι δύσκολο να αποφασίσει κανείς τι είναι δίκαιο και τι άδικο σε τέτοιες περιπτώσεις.

2η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΝΟΜΙΚΟΣ –ΥΠΕΥΘΥΝΗ ΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ SAFELINE

ΚΟΙΝ.ΛΕΙΤ: Τι θεωρείται παράνομο περιεχόμενο στο διαδίκτυο;

ΝΟΜΙΚΟΣ:Η κάθε χώρα με την εσωτερική της νομοθεσία ορίζει τι είναι παράνομο ή όχι στον φυσικό κόσμο. Ακολούθως, και ο κόσμος του Διαδικτύου ως μέσο επικοινωνίας και ανταλλαγής απόψεων μεταξύ συμμετεχόντων, που υπόκεινται στις αντίστοιχες εθνικές νομοθεσίες, δεν λειτουργεί σε νομικό κενό. Αυτό που θεωρείται παράνομο έξω από το Διαδίκτυο πρέπει να θεωρείται παράνομο και μέσα στο Διαδίκτυο.

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε ;

ΝΟΜΙΚΟΣ: Τα αδικήματα που διαπράττονται στο Διαδίκτυο είναι πολλά και θίγουν σημαντικά δικαιώματα των ανθρώπων. Ενδεικτικά, τα πιο ουσιώδη είναι η διακίνηση της παιδικής πορνογραφίας που είναι και το σημαντικότερο όλων, η προτροπή σε αυτοκτονία, η παραβίαση προσωπικών δεδομένων, η οικονομική εξαπάτηση μέσω αγορών που πραγματοποιήθηκαν με αναξιόπιστες ιστοσελίδες του Διαδικτύου, η παραβίαση του απορρήτου των επικοινωνιών, η εξύβριση και η συκοφαντική δυσφήμηση.

ΚΟΙΝ.ΛΕΙΤ: Πως φτάνουν τα θύματα σε εσάς; κ πως γίνεται η καταγγελία; μπορεί ο καταγγέλλων να κρατήσει την ανωνυμία του;

ΝΟΜΙΚΟΣ: Τα θύματα μπορούν να κάνουν την καταγγελία τους σε εμάς με πολλούς τρόπους με e-mail, συμπληρώνοντας την ειδική ηλεκτρονική φόρμα καταγγελίας ,τηλεφωνικά ,με sms και ταχυδρομικά .Δική μας αρμοδιότητα είναι να εξακριβώσουμε αν το περιεχόμενο είναι παράνομο και έπειτα το προωθούμε στην μονάδα Δίωξης για ποινική δίωξη των

υπευθύνων και απομάκρυνση του παράνομου περιεχόμενου από το Διαδίκτυο. Υπάρχει απόλυτη εχεμύθεια και διατήρηση της ανωνυμίας

ΚΟΙΝ.ΛΕΙΤ: Ποιες ενέργειες γίνονται από την safeline μετά από την κατάθεση της καταγγελίας;

ΝΟΜΙΚΟΣ: Επεξεργαζόμαστε την καταγγελία, επαληθεύουμε αν το περιεχόμενο είναι παράνομο .Έπειτα επιχειρούμε να βρούμε την πηγή του περιεχομένου ώστε να βρεθεί η χώρα προέλευσης με τεχνικές μεθόδους. Τέλος προωθούμε τις καταγγελίες στην δίωξη ανεξάρτητα την χώρα προελεύσεως και ενημερώνουμε τον καταγγέλλων για την εξέλιξη της καταγγελίας του.

ΚΟΙΝ.ΛΕΙΤ: Πιστεύετε πως σε περιπτώσεις καταγγελίας, το ελληνικό νομοθετικό σύστημα είναι επαρκές;

ΝΟΜΙΚΟΣ: Το Ελληνικό νομοθετικό πλαίσιο όσον αφορά τα εγκλήματα στο Διαδίκτυο συνεχώς και εμπλουτίζεται ή τροποποιείται με τέτοιο τρόπο ώστε να μπορέσει να καλύψει τα νέα δεδομένα του Διαδικτύου. Αυτό ωστόσο που είναι πολύ σημαντικό όσον αφορά τα εγκλήματα στο Διαδίκτυο είναι ότι αυτά λαμβάνουν χώρα σε πολλά διαφορετικά μέρη του κόσμου πράγμα που σημαίνει ότι πρέπει να ακολουθηθεί μια κοινή πορεία ως προς το νομικό πλαίσιο παγκοσμίως. Κάτι που είναι παράνομο σε μια χώρα του κόσμου δεν είναι παράνομο σε μια άλλη χώρα και έτσι γεννάται το μεγαλύτερο πρόβλημα όσον αφορά την αντιμετώπιση του Διαδικτυακού εγκλήματος. Στην Ελλάδα ακόμα δεν έχουμε ένα ενιαίο νομοθέτημα που να αφορά τα διαδικτυακά εγκλήματα και έτσι πρέπει να ανατρέχουμε σε πολλά ξεχωριστά. Πολύ συχνά για να καλυφθούν τα κενά της ελληνικής νομοθεσίας οι διωκτικές αρχές εφαρμόζουν αναλογικά τις διατάξεις που ποινικοποιούν αξιόποινες πράξεις στον φυσικό κόσμο που ζούμε.

ΚΟΙΝ.ΛΕΙΤ: Ποιές είναι οι προτάσεις σας για την καταπολέμηση του φαινομένου και την προστασία των χρηστών; Θεωρείτε πως οι νέοι ξέρουν να προστατευτούν και να διαφυλάξουν τα προσωπικά τους δεδομένα;

ΝΟΜΙΚΟΣ: Οι νέοι πολλές φορές λόγω του ενθουσιασμού που τους διακατέχει δεν έχουν την αίσθηση του κινδύνου. Παρά τις ενημερώσεις που πραγματοποιούνται και τις προειδοποιήσεις που ακούμε καθημερινά σχετικά με την προστασία των προσωπικών τους δεδομένων, παρόλα αυτά οι έφηβοι αναρτούν πάρα πολλά από τα προσωπικά τους δεδομένα στο Διαδίκτυο όπως είναι κυρίως ονοματεπώνυμο, φωτογραφίες, βίντεο κα. Αυτό που πρέπει να κατανοήσουν οι νέοι σήμερα είναι πως όποιο προσωπικό στοιχείο αναρτήσουν στο Διαδίκτυο αυτό πια δεν ξανακατεβαίνει από κει και είναι πιθανό να χρησιμοποιηθεί με τέτοιο τρόπο που εν τέλει να βλάψει την προσωπικότητά του. Συνιστούμε στους νέους χρήστες να είναι πολύ φειδωλοί όταν αναρτούν τα στοιχεία τους στο διαδίκτυο. Πέρα από τους όρους προστασίας που παρέχουν τα διάφορα συστήματα κοινωνικής δικτύωσης, είναι απαραίτητη και η αυτοπροστασία του χρήστη μέσα σε αυτά. Συστήματα κοινωνικής δικτύωσης όπως είναι το Facebook, το Myspace, το Hi5 κ.α. μας δίνουν τη δυνατότητα να εκθέτουμε προσωπικά μας δεδομένα σε πολύ μεγάλο αριθμό χρηστών οι οποίοι δεν ξέρουμε πάντα πώς θα «εκμεταλλευτούν» όλες αυτές τις πληροφορίες. Πρέπει επομένως να είμαστε επιφυλακτικοί και προσεκτικοί με όσους επιδιώκουν κάποια «φιλία» μέσω αυτών των συστημάτων. Να μην δεχόμαστε φιλίες από άγνωστα άτομα και στη συνέχεια να προσέχουμε τι προσωπικά δεδομένα ανεβάζουμε.

3η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ: ΤΜΗΜΑΤΑΡΧΗΣ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΤΟΠΟΘΕΣΙΑ: Γ.Α.Δ.Α –ΤΜΗΜΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΚΟΙΝ.ΛΕΙΤ: Τι θεωρείται παράνομο περιεχόμενο στο διαδίκτυο;

ΑΣΤΥΝΟΜΙΚΟΣ: Παράνομο είναι το περιεχόμενο το οποίο τιμωρείται από την ελληνική νομοθεσία. Το έγκλημα από απλό κ παραδοσιακό έχει γίνει και ηλεκτρονικό .Όλες οι μορφές εγκληματικότητας έχουν περάσει στο διαδίκτυο .Για να καταλάβετε οι παράνομες πράξεις που τιμωρούνται από

τον ποινικό κώδικα στην καθημερινότητα μας αναλογικά τιμωρούνται και στο διαδίκτυο. Παραδείγματος χάρη διαπράχθηκε ανθρωποκτονία μέσω υπολογιστή όπου κάποιος εισέβαλε στα αρχεία μιας κλινικής και μέσω υπολογιστή άλλαξε τα χάπια ενός ασθενή και τον οδήγησε στον θάνατο .

ΚΟΙΝ.ΛΕΙΤ: Τιμωρούνται οι ανθρωποκτονίες που εκτελούνται μέσω υπολογιστή;

ΑΣΤΥΝΟΜΙΚΟΣ: Ναι ,τιμωρούνται πάντα και μην σας πω με πιο αυστηρό τρόπο ,δεν υπάρχει περίπτωση μια υπόθεση να μην εξιχνιαστεί

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;

ΑΣΤΥΝΟΜΙΚΟΣ: Από τις πιο συνηθέστερες απάτες είναι οι νιγηριανές επιστολές οι οποίες στέλνονται σε ανυποψίαστους παραλήπτες όπου έχουν έδρα το Λονδίνο, το Άμστερνταμ ,την Μαδρίτη. Είναι πολύ πειστικές στέλνουν e-mail όπου σου γνωστοποιούν ότι κέρδισες το λόττο η πως είσαι ο κληρονόμος μιας μεγάλης περιουσίας μιας πάμπλουτης γιαγιάς που πέθανε από το Λονδίνο και όλα αυτά αρκεί να τους καταθέσεις κάποιο ποσό ανάλογα με την περίπτωση ή δίνοντας τον αριθμό της πιστωτικής σου κάρτας ή τον τραπεζικό σου λογαριασμό. Οι συγκεκριμένες επιστολές έχουν καταστρέψει πολύ κόσμο .Μια άλλη μορφή απάτης είναι αυτές που γίνονται μέσω των κοινωνικών δικτύων όπου σου λένε τον τρόπο και την ημερομηνία που θα πεθάνεις η το επίπεδο του iq σου δίνοντας τον αριθμό του τηλεφώνου σου ,αυτό έχει σαν συνέπεια να σε χρεώνουν 15 ευρώ κάθε μήνα .Αυτή είναι μια νέα μορφή καταιγίδας μηνυμάτων ώστε να γραφούν πολλούς συνδρομητές για να πάρουν όσα πιο πολλά χρήματα μπορούν .Αυτές οι εταιρείες τηλεπικοινωνιών έχουν κερδίσει αρκετά εκατομμύρια .Επίσης μια άλλη μορφή απάτης είναι οι ευκαιριακές ιστοσελίδες όπου κάνουν προσφορές π.χ ταξίδι στην Βραζιλία μόνο με 450Ε πλήρες γεύμα και πληρωμένο το ξενοδοχείο αρκεί να στείλουν πρώτα χρήματα ώστε να κλείσουν τα εισιτήρια τους. Επίσης στήνουν και ψεύτικες παραγωγές στην τηλεόραση όπου διαφημίζουν το συγκεκριμένο ταξιδιωτικό γραφείο που έχει την τάδε προσφορά ,ο πολίτης πείθεται και τρέχει να προλάβει την

προσφορά δίνει τα χρήματα και έπειτα αυτοί εξαφανίζονται καθώς το ταξιδιωτικό γραφείο δεν υπάρχει και οι ίδιοι έχουν εξαφανιστεί .

ΚΟΙΝ.ΛΕΙΤ: Μπορούν να εξιχνιαστούν τέτοιες υποθέσεις;

ΑΣΤΥΝΟΜΙΚΟΣ: Βεβαίως και μπορούν αλλά τα χρήματα δεν υπάρχουν και έτσι δεν τα παίρνουν πίσω οι άνθρωποι. Επίσης η νομοθεσία για τέτοιες περιπτώσεις είναι πολύ ελαστική καθώς δεν προφυλακίζεσαι για αδικήματα 10 χρόνων ,με αυτό τον τρόπο προάγει απατεώνες .Επίσης από τις σημαντικότερες μορφές εγκλήματος και όχι απάτης είναι το κο bullying όπου μέσα από τα κοινωνικά δίκτυα facebook hi5 όπου ο καθένας βγάζει τα απωθημένα του μπορεί ο καθένας να σε εκδικηθεί δημιουργώντας ένα ψεύτικο προφίλ, διασύροντας σε όλο το διαδίκτυο. Αυτή είναι η νέα μάστιγα .Τέλος μια άλλη μορφή εγκλήματος με τεράστιες διαστάσεις είναι παιδική πορνογραφία και η παιδεραστία .Στην Ελλάδα δεν γίνεται παραγωγή ταινιών παρά μόνο διακίνηση ,εδώ ο νόμος είναι πολύ αυστηρός ύστερα από μια εκστρατεία που έκανα ο ίδιος ώστε να τιμωρούνται από δέκα χρόνια και πάνω όποιος κάνει διακίνηση πορνογραφικού υλικού .Θεωρείται το ίδιο συνένοχος με εκείνον που κάνει τη πράξη αυτός που πληρώνει για να κατεβάσει την ταινία ή για να την δει online τη στιγμή που βιάζουν ένα μωρό, ένα σκυλί ή κάποιος άντρας .Αυτός λοιπόν που πληρώνει για να δει τον βιασμό διαπράττει μεγαλύτερο αδίκημα. Όσον αφορά τώρα την παιδεραστία έχει πάρει τεράστιες διαστάσεις καθώς οι παιδεραστές δημιουργούν ψεύτικα προφίλ και πλησιάζουν ανήλικα, έτσι κ εμείς παρακολουθούμε και συμμετέχουμε σε online συζητήσεις δημιουργώντας επίσης ένα ψεύτικο προφίλ και τους παγιδεύουμε . Ένας κύριος όγκος της δουλειάς μας είναι οι ηλεκτρονικοί παιδόφιλοι. Από το 2001, έχουμε αντιμετωπίσει 47 υποθέσεις παιδικής πορνογραφίας με 99 κατηγορουμένους & 88 συλλήψεις. Μάλιστα, για όλες αυτές τις υποθέσεις έχουμε συνολικά 17 προφυλακίσεις. Οι συλληφθέντες μπορεί να είναι από ιδιωτικοί υπάλληλοι μέχρι καταστηματάρχες, Ιατροί & Καθηγητές Πανεπιστημίου.

ΚΟΙΝ.ΛΕΙΤ: Πως φτάνουν τα θύματα σε εσάς και πως γίνεται η καταγγελία; μπορεί να τηρηθεί η ανωνυμία;

ΑΣΤΥΝΟΜΙΚΟΣ: Οι καταγγελίες γίνονται είτε τηλεφωνικά είτε με προσέλευση στην υπηρεσία μας και τηρείται η ανωνυμία πάντοτε .

ΚΟΙΝ.ΛΕΙΤ: Πως εξακριβώνεται μια υπόθεση; Ποιες ενέργειες γίνονται από την υπηρεσία σας μετά από την κατάθεση της καταγγελίας;

ΑΣΤΥΝΟΜΙΚΟΣ: Υποβάλλεται στην υπηρεσία μας η μήνυση. Εμείς κάνουμε έρευνα και εντοπίζουμε τα στοιχεία που αναφέρει ο μηνυτής. Βρίσκουμε τα ηλεκτρονικά ίχνη, τα στοιχειοθετούμε. Ενημερώνουμε τον προϊστάμενο της Εισαγγελίας Αθηνών. Κι εδώ πρέπει να πω ότι ο προϊστάμενος της Εισαγγελίας, είναι δίπλα μας καθημερινά. Δεν υπάρχει ημέρα που να μην τον ενοχλήσω δύο και τρεις φορές για θέματα που φτάνουν στην υπηρεσία μας. Είμαστε ίσως η υπηρεσία που τον έχει ζαλίσει, αλλά εκείνος με χαρά και μεράκι στέκεται δίπλα μας. Έτσι δεν φοβόμαστε τίποτα. Άλλωστε δεν κάνουμε τίποτα χωρίς προηγουμένως να ενημερώσουμε τον Εισαγγελέα. Για να καταλάβετε για να συνδεθείς στο διαδίκτυο έχεις κάνει σύνδεση με μια εταιρεία η οποία σου δίνει ένα ηλεκτρονικό ίχνος μοναδικό στον κόσμο για κάθε άνθρωπο ,αυτό το ηλεκτρονικό ίχνος ονομάζεται ip address .Δεν υπάρχει άλλος άνθρωπος που να έχει το ίδιο, είναι μοναδικό αναγνωριστικό σαν να έχουμε ένα δαχτυλικό αποτύπωμα ,έτσι είμαστε σίγουροι για το ποιος το έκανε .Μόλις εξακριβώσουμε την υπόθεση την πάμε στον εισαγγελέα ο οποίος δίνει παραγγελία για να μας δοθεί από την εταιρεία τα στοιχεία του κατόχου που έχει το συγκεκριμένο ίχνος .Έπειτα μέσω του εισαγγελέα μας δίνεται η άδεια για περαιτέρω έρευνα ,αναφέροντας ότι επιθυμούμε την ποινική δίωξη του τάδε για τους παραπάνω λόγους. Μπορούν να γίνουν δύο ειδών έρευνες ,η πρώτη είναι μέσω της εξακρίβωσης του ηλεκτρονικού ίχνους και η δεύτερη μέσω μήνυσης ευθείας μορφής αν γνωρίζουμε τον δράστη .Π.χ: Είχες μια σχέση και χώρισες και ο σύντροφος σου για να σε εκδικηθεί ανεβάζει ένα βίντεο σου στο facebook που έχετε τραβήξει σε προσωπικές σας στιγμές, σε αυτή την περίπτωση γνωρίζουμε τον δράστη οπότε γίνεται κατευθείαν μήνυση στο πρόσωπο του. Κάθε υπόθεση εκδικάζετε γιατί υπάρχει το ηλεκτρονικό αποτύπωμα. Τέλος μέσα στις ενέργειες μας συμπεριλαμβάνεται και η συνεργασία μας με ψυχολόγους και

κοιν.λειτουργούς από το Χαμόγελο του παιδιού και από Μ.Κ.Ο. Όπου ο ρόλος τους είναι η σκιαγράφηση της προσωπικότητας των δραστών, η επεξεργασία μηνυμάτων και η προσέγγιση του θύματος παρέχοντας ψυχολογική υποστήριξή καθώς το θύμα ιδιαίτερα αν είναι ανήλικο δεν βλέπει τον αστυνομικό.

ΚΟΙΝ.ΛΕΙΤ :Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητα;

ΑΣΤΥΝΟΜΙΚΟΣ: Το νομοθετικό πλαίσιο αυτή την στιγμή στην Ελλάδα κατά ένα ποσοστό είναι επαρκές καθώς εφαρμόζει το ποινικό δίκαιο. Εκεί που έχουμε πρόβλημα είναι στην άρση του απορρήτου .Ο εισαγγελέας λέει πως γίνεται άρση απορρήτου σε όλες τις υποθέσεις ενώ η Α.Δ.Α.Ε συμφώνα με το προεδρικό διάταγμα 47 του 2005 όλο το διαδίκτυο είναι απόρρητο, επιτρέπει την άρση απορρήτου σε συγκεκριμένες υποθέσεις όπως ναρκωτικά , ανθρωποκτονίες ,εκβιασμούς και οργανωμένο έγκλημα κατά της εθνικής ασφάλειας. Το ισχύον νομοθετικό πλαίσιο δεν προσφέρει επαρκή προστασία από τη διακίνηση παιδικής πορνογραφίας και τα περιστατικά εκβιασμού μέσω Διαδικτύου, Παραδείγματος χάρη σε περιπτώσεις συκοφαντίας δεν γίνεται άρση απορρήτου ενώ ο εισαγγελέας κάνει άρση. Υπάρχει μια διχογνωμία ,που πιστεύουμε ότι θα λυθεί σύντομα. Με λίγα λόγια οι μισοί εφαρμόζουν αυτά που λέει ο εισαγγελέας και οι άλλοι την Α..Δ.Α.Ε αλλά σε περιπτώσεις εμβρασμού γίνεται πάντα άρση .

ΚΟΙΝ.ΛΕΙΤ: Ποιες οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

ΑΣΤΥΝΟΜΙΚΟΣ: Οι προτάσεις μου είναι οι εξής ,καταρχήν να ισορροπήσει ο νόμος ,να νομοθετήσει το κράτος ώστε να μην υπάρχουν κενά και διχογνωμία σχετικά με την άρση του απορρήτου . Θα είχα δεύτερη άλλα η πρόταση μου θα πραγματοποιηθεί σε ένα μήνα όπου θα γίνουμε διεύθυνση .Στην νέα μας διεύθυνση θα υλοποιηθεί η πρόταση μου ώστε να δημιουργηθεί οργανωμένη ομάδα ειδικών ψυχολόγων ,κοινωνικών λειτουργών και προγραμματιστών που θα ενημερώνει τα σχολεία ,τις νομαρχίες και τους δήμους για το ίντερνετ δίνοντας συμβουλές για ασφαλή πλοήγηση. Είναι ανησυχητική η χρήση του διαδικτύου από εφήβους καθώς

αγγίζει τα όρια του εθισμού, χωρίς ωστόσο να υπάρχει η κατάλληλη μέριμνα από την Πολιτεία, ούτε επαρκής ενημέρωση των οικογενειών για την αποτελεσματικότερη προστασία τους. Αυτός ακριβώς θα είναι ο ρόλος τους η πρόληψη. Θα ήθελα να συμπληρώσω πως το διαδίκτυο είναι ότι καλύτερο υπάρχει αυτή τη στιγμή. Χωρίς αυτό δεν μπορεί να λειτουργήσει τίποτα. Εκείνο που επιδιώκουμε είναι να βοηθήσουμε τους ανθρώπους να έχουν ασφαλή πλοήγηση, να προστατέψουμε τον πολίτη από τους κινδύνους που πιθανόν διατρέχει. Συμβουλή μου λοιπόν είναι οι ίδιοι οι πολίτες να θωρακίζουν τα προσωπικά τους δεδομένα και να μην εκθέτουν την προσωπική τους ζωή στο ίντερνετ .

4η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ

ΤΟΠΟΘΕΣΙΑ:Γ.Α.Δ.Α ΤΜΗΜΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Οι συνηθέστερες μορφές απάτης και εγκλήματος αφορούν την παιδική πορνογραφία, αλλά έχουμε μεγάλο όγκο καταγγελιών για συκοφαντικές δυσφημήσεις, εξύβριση και οικονομικές απάτες .Η μεγάλη μάστιγα όμως είναι τα κοινωνικά δίκτυα όπου μέσα από αυτά έχει δημιουργηθεί μια νέα μορφή τρομοκρατίας το cyber bowling όπου ο καθένας μπορεί να εκβιάσει και να συκοφαντήσει τον καθένα δημιουργώντας ψεύτικα προφίλ .

ΚΟΙΝ.ΛΕΙΤ: Πώς μπορεί ένας hacker να εισβάλει στον υπολογιστή μας και τι μπορεί να κάνει σε αυτό ;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Υπάρχει ένα μότο για τους hacker τίποτα δεν κλειδώνει .Αν πέσεις στο μάτι κάποιου hacker δεν γλιτώνεις. Μπορώ να σου μιλώ μέχρι αύριο για τους τρόπους που μπορεί να εισβάλει ένας hacker

.Υπάρχουν ωστόσο δύο βασικοί τρόποι :Πρώτον να εισβάλλει μέσω του ιού Trojan horse στέλνοντας σου μέσω msn μια φωτογραφία την ώρα που συνομιλείς η όποια περιέχει ένα πρόγραμμα όπου βλέποντας εσύ την φωτογραφία ο hacker έχει πρόσβαση στον υπολογιστή σου .Δεύτερον ένας άλλος τρόπος είναι μέσω e-mail όπου στέλνουν επισυναπτόμενα αρχεία τα οποία όταν ανοιχτούν ανοίγει παράλληλα και ένα πρόγραμμα με το οποίο ο hacker μπορεί να κάνει υποχείριο του τον υπολογιστή σου .Με λίγα λόγια μπορεί να σου αλλάξει τους κωδικούς σου να κλέψει οποιοδήποτε αρχείο έχεις στον υπολογιστή σου, θα μάθει όλη την ιστορία σου και τέλος μπορεί να στον κλειδώσει τελείως ώστε να μην μπορείς να ξαναμπείς .

ΚΟΙΝ.ΛΕΙΤ: Πως μπορούμε να προστατευθούμε από το διαδίκτυο; ποιες είναι οι προτάσεις σας;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Χωρίς να θέλω να σας τρομοκρατήσω ο υπολογιστής σας είναι ασφαλής μόνο όταν είναι κλειστός και εκτός πρίζας. Τα antivarious που πουλιούνται στην αγορά προσφέρουν απλά ένα Α ‘ Επίπεδο προστασίας και σίγουρα πρέπει να τα χρησιμοποιούμε αλλά δεν σημαίνει ότι είμαστε απόλυτα ασφαλής εδώ 15 χρόνοι hacker έχουν εισβάλει στα αρχεία της NASA και του πεντάγωνου φανταστείτε πόσο εύκολα εισβάλλουν στους δικούς μας υπολογιστές .Πρόταση μου είναι να θωρακίζουμε τον υπολογιστή μας να μην έχουμε προσωπικό μας υλικό αποθηκευμένο ,να μην ανοίγουμε e-mail από ξένους και να ενημερωνόμαστε από ειδικούς για οτιδήποτε μας απασχολεί .

5η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΑΣΤΥΝΟΜΟΣ Β ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΤΟΠΟΘΕΣΙΑ: ΑΣΤΥΝΟΜΙΚΟ ΜΕΓΑΡΟ –ΤΜΗΜΑ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΚΟΙΝ.ΛΕΙΤ: Τι θεωρείται παράνομο περιεχόμενο στο διαδίκτυο;

ΑΣΤΥΝΟΜΙΚΟΣ: Παράνομο στο διαδίκτυο θεωρείται οποιαδήποτε πράξη τιμωρείται από τον ποινικό κώδικα στην καθημερινότητα μας, τιμωρείται εξίσου και στο διαδίκτυο.

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;

ΑΣΤΥΝΟΜΙΚΟΣ: Υπάρχουν τέσσερις μορφές απάτης: οι αγοροπωλησίες μέσω διαδικτύου όπου ζητούν από τους χρήστες οι οποίοι θέλουν να αποκτήσουν κάποιο προϊόν να στείλουν μια προκαταβολή χωρίς ποτέ να λάβουν το προϊόν που παρήγγειλα, επίσης οι απάτες με πιστωτικές, οι απάτες γνωστές ως νιγηριανές όπου σου στέλνουν για παράδειγμα ένα e-mail και σου λένε ότι κέρδισες το λόττο και πρέπει να δώσεις κάποια στοιχεία σου ή να καταθέσεις κάποιο ποσό για να λάβεις το μεγάλο ποσό που κέρδισες και τέλος είναι οι απάτες με τις τράπεζες όπου σου στέλνουν ένα e-mail και σου λένε ότι υπάρχει κάποιο πρόβλημα με τα στοιχεία του λογαριασμού σου στην τάδε τράπεζα και ότι πρέπει να τα εισάγεις για να ενημερωθεί η τράπεζα. Αυτές είναι οι γνωστές οικονομικές απάτες. Από εκεί και έπειτα άλλα εγκλήματα στο διαδίκτυο με μεγάλη συχνότητα εμφάνισης είναι η προσβολή της προσωπικότητας μέσα από κοινωνικά δίκτυα και πιο συγκεκριμένα από το γνωστό σε όλους μας facebook.

ΚΟΙΝ.ΛΕΙΤ: Πως φτάνουν τα θύματα σε εσάς και πως γίνεται η καταγγελία; μπορεί να τηρηθεί η ανωνυμία;

ΑΣΤΥΝΟΜΙΚΟΣ: Οι καταγγελίες γίνονται τις περισσότερες φορές από τα ίδια τα θύματα τα οποία έρχονται σε εμάς για να καταθέσουν μήνυση σε

κάποιο συγκεκριμένο πρόσωπο. Βέβαια υπάρχουν περιπτώσεις όπως η πορνογραφία ή οι αγγελίες για εκδιδόμενες γυναίκες όπου δεν προϋποθέτουν μήνυση για να ξεκινήσουμε να διεξάγουμε έρευνα. Το αν μπορεί να τηρηθεί η όχι η ανωνυμία αυτό είναι σχετικό διότι ακόμη και αν στην αρχή υπάρχει ανωνυμία όταν η υπόθεση φτάσει στα δικαστήρια θα γίνει άρση απόρρητου.

ΚΟΙΝ.ΛΕΙΤ: Πως εξακριβώνεται μια υπόθεση; Ποιες ενέργειες γίνονται από την υπηρεσία σας μετά από την κατάθεση της καταγγελίας;

ΑΣΤΥΝΟΜΙΚΟΣ: Μετά από την μήνυση που υποβάλλεται στην υπηρεσία μας γίνεται έρευνα και εντοπίζουμε τα στοιχεία που αναφέρει ο μηνυτής. Βρίσκουμε τα ηλεκτρονικά ίχνη, τα στοιχειοθετούμε. Στην συνέχεια η υπόθεση πηγαίνει στον Εισαγγελέα . Από εκεί μας δίνεται η άδεια για να μπούμε στα αρχεία της εταιρίας και να βρούμε το ίχνος, αυτό συμβαίνει στις περιπτώσεις όπου δεν γνωρίζουμε το δράστη, δεν έχει υπάρξει δηλαδή επώνυμη καταγγελία. Στην συνέχεια ακολουθείται ότι προβλέπει ο ποινικός κώδικας σε τέτοιες περιπτώσεις .

ΚΟΙΝ.ΛΕΙΤ :Θεωρείται επαρκές το νομοθετικό πλαίσιο που έγκειται του θέματος της ηλεκτρονικής εγκληματικότητα;

ΑΣΤΥΝΟΜΙΚΟΣ: Θεωρώ ότι υπάρχουν κάποιες ελλείψεις στο νομοθετικό πλαίσιο όχι μόνο για τα εγκλήματα και τις απάτες του διαδικτύου αλλά και για τις παραδοσιακές απάτες και τα παραδοσιακά εγκλήματα. Βέβαια το Δεκέμβριο του 2008 . Επίσης ένα άλλο πρόβλημα που αντιμετωπίζουμε είναι ότι το νομοθετικό πλαίσιο σε παγκόσμιο επίπεδο διότι κάτι που θεωρείται παράνομο σε μια χώρα σε κάποια άλλη χώρα μπορεί να μην θεωρείται παράνομο. Επομένως τι κάνουμε σε τέτοιες περιπτώσεις; Συνήθως ο χρήστης που διέπραξε μια παράνομη πράξη δικάζεται σύμφωνα με το νομοθετικό πλαίσιο της χώρας από την οποία διεξήγε η συγκεκριμένη παράνομη πράξη. Για παράδειγμα στην Ελλάδα το στοίχημα είναι παράνομο ενώ στην Αγγλία μπορεί και να μην θεωρείται παράνομο. Εσύ είσαι σπίτι σου στην Ελλάδα και παίζεις παράνομο στοίχημα σε σελίδα της Αγγλίας; Είναι παράνομο αυτό ή όχι; Είναι γιατί η πράξη διαπράχθηκε στην

Ελλάδα όπου ο ποινικός μας κώδικας νομοθετεί ότι το στοίχημα είναι παράνομο.

ΚΟΙΝ.ΛΕΙΤ: Ποιες οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

ΑΣΤΥΝΟΜΙΚΟΣ: Τι να σας πω; Δεν υπάρχει τρόπος να προστατευτείς. Το μόνο που μπορούμε να κάνουμε είναι να προστατεύσουμε εμείς οι ίδιοι τον εαυτό μας με το να προσέχουμε σε τι σελίδες μπαίνουμε και να είμαστε πιο υποψιασμένοι με τα διάφορα e-mail που θα φτάνουν σε εμάς από αγνώστους και όχι μόνο.

6η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την υπηρεσία από όπου εργάζεστε;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Η μεγαλύτερη και πιο διαδεδομένη μορφή απάτης στο διαδίκτυο σήμερα θεωρώ ότι είναι τα κοινωνικά δίκτυα και πιο συγκεκριμένα το facebook. Μέσα από αυτό μπορούν να σου κλέψουν προσωπικά σου στοιχεία, να δυσφημίσουν ή να προσβάλλουν κάποιον, να δημιουργήσουν εικονικό προφίλ για να πλησιάσουν ανήλικα και πολλά άλλα. Αυτό επιτυγχάνεται με πολύ εύκολο τρόπο. Όταν ασχολείσαι με το διαδίκτυο και είσαι ένας μέσος χρήστης, όχι απλός χρήστης, τότε μπορείς να χρησιμοποιήσεις προγράμματα τα οποία είναι δωρεάν και με την βοήθεια αυτών των προγραμμάτων να υποκλέβεις την ip διεύθυνση κάποιου. Η ip διεύθυνση είναι η ηλεκτρονική διεύθυνση που εκπέμπει κάθε μόντεμ-ρούτερ και αυτή είναι διαφορετική και μοναδική για τον κάθε χρήστη. Ο μέσος χρήστης που θέλει να βρει το ip σου το κάνει με πολύ εύκολο τρόπο, γιατί μέσω του facebook το εκπέμπεις συνέχεια. Βρίσκοντας λοιπόν κάποιος το ip σου μετά μπορεί να βρει το στίγμα που βρίσκεσαι, το τηλέφωνο σου και όλα αυτά με την βοήθεια προγραμμάτων. Να σημειωθεί

ότι εάν έχεις ασύρματο δίκτυο είναι λίγο πιο δύσκολο να σε βρει κάποιος διότι είναι σαν να ψάχνει κινητό τηλέφωνο, δεν είναι όμως ακατόρθωτο απλά θα χρειαστεί ένα συνδυασμό προγραμμάτων αντί για ένα απλό πρόγραμμα. Άλλες πολύ διαδεδομένες μορφές απάτης είναι οι οικονομικές απάτες και η διακίνηση πορνογραφικού υλικού.

ΚΟΙΝ.ΛΕΙΤ: Πώς μπορεί ένας hacker να εισβάλει στον υπολογιστή μας και τι μπορεί να κάνει σε αυτό ;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Πολύ εύκολα! Απλά στέλνοντας σου ένα e-mail που συνήθως σου ζητά να κάνεις log in για κάποιο λόγο, σε εικονικό site, και έτσι ενεργοποιείται ιός και όποτε ανοίγεις τον υπολογιστή σου, αυτό φαίνεται στον «ενδιαφερόμενο» και είναι σαν να του ανοίγεις την πόρτα για να έχει ελεύθερη πρόσβαση στον υπολογιστή σου και στα προσωπικά σου δεδομένα. Με αυτόν τον τρόπο μπορεί να υποκλέψει τα αρχεία σου ή απλά αν είναι ένας περίεργος hacker θα θέλει να έχει πρόσβαση στο e-mail σου και σε φωτογραφίες σου ή άλλοι hackers εισβάλλουν στον υπολογιστή σου μόνο και μόνο για να σου «κοτσάρουν» έναν ιό και να σου κάψουν τα βασικά σου αρχεία με αποτέλεσμα να μην δουλεύει ο υπολογιστή σου και να θέλει οπωσδήποτε format για να επανέλθει χάνοντας όμως, αν όχι όλα , μεγάλο όγκο των αποθηκευμένων σου αρχείων.

ΚΟΙΝ.ΛΕΙΤ: Πως μπορούμε να προστατευθούμε από το φαινόμενο του ηλεκτρονικού εγκλήματος; ποιες είναι οι προτάσεις σας;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Ο μοναδικός τρόπος για να προστατευτεί κάποιος είναι να μην έχει internet. Διαφορετικά μπορεί να προστατευτεί εν μέρει από χρησιμοποιώντας antivirus, antitrojan, antispyware και με το τοίχος προστασίας(βασικό). Υπάρχουν διάφορα προγράμματα αλλά και με αυτά κινδυνεύεις, είσαι καλυμμένος σε ποσοστό 90% αλλά ένας έμπειρος χρήστης μπορεί να εισβάλλει στο υπόλοιπο 10% που μένεις ακάλυπτος.

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι προτάσεις σας για την καταπολέμηση του φαινομένου;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Βασικά πρέπει να είμαστε πιο προσεκτικοί και να μπαίνουμε μόνο σε έγκυρες σελίδες. Σε σελίδες οι οποίες είναι κλειδωμένες

και υπάρχει η προστασία από αυτόν που έχει φτιάξει τη σελίδα. Να είναι πιστοποιημένη η σελίδα. Επίσης για να είμαστε ασφαλείς ότι δεν θα χάσουμε τίποτα από τα δεδομένα μας, θα πρέπει να τα κρατάμε αποθηκευμένα σε εξωτερικά αποθηκευτικά μέσα(εξωτερικός σκληρός δίσκος κ.α) και όταν είμαστε συνδεδεμένοι στο internet να μην έχουμε συνδεδεμένο τον εξωτερικό σκληρό δίσκο, για παράδειγμα, στον υπολογιστή μας. Επιπλέον ένας άλλος τρόπος να προστατέψουμε τα δεδομένα μας είναι να κρατάμε back up αρχεία. Να τα zipπάρουμε και να κρυπτογραφούμε τα αρχεία μας, βάζοντας τους και κωδικό αποzipπαρίσματος. Έτσι και να μας τα κλέψει κάποιος δύσκολα θα καταφέρει να τα ανοίξει. Εντελώς πληροφοριακά η ηλεκτρονική κρυπτογράφηση ξεκίνησε την εποχή του Β' Παγκοσμίου Πολέμου από τους Άγγλους και έχει μείνει γνωστό ως «αίνιγμα». Παρόλα αυτά και τα συγκεκριμένα αποκωδικοποιήθηκαν. Είναι με το πόσο θέλει να ασχοληθεί ο άλλος. Αν σε βάλει στο μάτι και ασχοληθεί έχει μεγάλες πιθανότητες να το καταφέρει. Για να λέμε και τα πράγματα με το όνομά τους, ένας hacker δεν ξεκινάει να στήσει ένα πρόγραμμα ιού από την αρχή. Η βάση των προγραμμάτων αυτών γίνεται από τις εταιρείες (Microsoft, Linux κ.α), μετά τα παίρνουν οι hackers και τα τροποποιούν σύμφωνα με αυτό που θέλουν να επιτύχουν, είτε να σου καταστρέψουν τον υπολογιστή, είτε να σου κάνουν τον υπολογιστή σου πιο αργό και πολλά άλλα. Και όλα αυτά γίνονται για να πουλάνε οι εταιρείες τα προστατευτικά προγράμματα που προανέφερα όπως antivirus κ.α Καταλαβαίνεις τι γίνεται!

ΚΟΙΝ.ΛΕΙΤ: Αν ήσουν hacker τι θα μπορούσες να κάνεις με έναν υπολογιστή;

ΠΡΟΓΡΑΜΜΑΤΙΣΤΗΣ: Εξαρτάται σε ποια κατηγορία hacker θα επέλεγα να ανήκω. Υπάρχουν διάφοροι τύποι hacker. Είναι αυτοί που σαν στόχο τους έχουν να μολύνουν το διαδίκτυο με ιούς, αυτοί που ασχολούνται με το σπάσιμο και το ξεκλείδωμα προγραμμάτων, αυτοί που σαν σκοπό τους έχουν να σου υποκλέψουν τον αριθμό της πιστωτικής σου κάρτας, τον αριθμό της ταυτότητάς σου κλπ, επίσης είναι αυτού που είναι απλά περίεργοι και θέλουν να μπουν στο e-mail σου ή στο facebook σου και τέλος είναι και οι super hackers οι οποίοι θέλουν να εισβάλλουν στο

Παγκόσμιο Διαδίκτυο. Δεν ξέρω αν θυμάσαι τον «ιό του 2000»; Τότε λέγανε ότι θα δημιουργηθεί από τους hackers ένας ιός ο οποίος θα μολύνει τον Παγκόσμιο server και θα σβήσει τα πάντα. Τελικά δεν έγινε τίποτα γιατί αν γινόταν κάτι τέτοιο θα έπρεπε όλα να ξανά ξεκινήσουν από το μηδέν.

7η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΨΥΧΟΛΟΓΟΣ

ΤΟΠΟΘΕΣΙΑ:ΓΡΑΦΕΙΑ Μ.Κ.Ο ¨ΑΛΛΗΛΕΓΓΥΗΣ¨

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει κατά την συνεργασία σας με το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Αττικής;

ΨΥΧΟΛΟΓΟΣ: Το διαδικτυακό έγκλημα έχει πάρει τεράστιες διαστάσεις σε παγκόσμιο επίπεδο όπως αντιληφθήκατε και εσείς μέσα από την ερευνά σας διαπράττονται πολλές απάτες η πιο συνήθης είναι η οικονομική εξαπάτηση .Μια από τις απειλητικές μορφές διαδικτυακού εγκλήματος δεδομένου της πρόσβασης των παιδιών στο διαδίκτυο αφορά την παιδική ηλεκτρονική πορνογραφία, την προτροπή σε αυτοκτονία και την σεξουαλική παρενόχληση ανηλίκων ,όπου ενήλικες προσεγγίζουν ανήλικους με ψεύτικο προφίλ παρουσιάζοντας τον εαυτό τους ως συνομήλικους. Εγώ προσωπικά και συνάδελφοι έχουμε συνεργαστεί με την Δίωξη κυρίως σε περιπτώσεις σεξουαλικής παρενόχλησης ανηλίκων κ σε περιπτώσεις αυτοκτονιών .

ΚΟΙΝ.ΛΕΙΤ: Θα ήθελα να μου πείτε λίγα λόγια για τον ρόλο του ψυχολόγου στην αντιμετώπιση του φαινομένου και στην προστασία των θυμάτων;

ΨΥΧΟΛΟΓΟΣ: Θα σου μιλήσω αρχικά γενικά για τον ρόλο μας. Ο ρόλος του ψυχολόγου είναι να βοηθά τα άτομα να διαπραγματεύονται αποτελεσματικά τα συναισθήματα τους και αλλά προσωπικά τους προβλήματα ,ενδιαφέρεται κυρίως για τις κρυμμένες δυνάμεις του ατόμου ,για το υποστηρικτικό περιβάλλον και για τους τρόπους επικοινωνίας και συνδιαλλαγής του με αυτά που τον περιβάλλουν. Συγκεκριμένα έχουμε

κλιθεί να αποτρέψουμε και να βοηθήσουμε άτομα που απειλούν πως θα αφαιρέσουν την ίδια τους την ζωή κάνοντας μια ακραία επιλογή ώστε να ξεφύγουν από καταστάσεις που τους προκαλούν αφόρητο πόνο .Υπάρχει σαφώς σημαντική αύξηση αυτοκτονιών μέσω διαδικτύου αφού συνομήλικοι παρακινούν τον φίλο τους να αυτοκτονήσει ή οργανώνουν ομαδικές αυτοκτονίες. Σε περιπτώσεις όπου έχουμε να κάνουμε με ανήλικα παιδιά ,το παιδί βλέπει μόνο τον ψυχολόγο ή τον κοιν.λειτουργό ο οποίος τον προσεγγίζει και του παρέχει ψυχολογική υποστήριξη.

ΚΟΙΝ.ΛΕΙΤ: Για ποιο λόγο πιστεύετε αυξήθηκε το ποσοστό αυτοκτονιών μέσω του διαδικτύου;

ΨΥΧΟΛΟΓΟΣ: Οι άνθρωποι πραγματοποιούν πιο εύκολα κάτι που στην πραγματική ζωή δεν θα τολμούσαν να κάνουν .Αυτή η απελευθέρωση των κρυφών πτυχών οδηγεί σε αυτοκαταστροφικές ενέργειες και αυτό είναι γεγονός. Πλέον πολλοί χρήστες εγκλωβίζονται σε αυτή την ψευδαίσθηση του κυβερνοχώρου και παρατούν την προσωπική τους ζωή και σε ακραίες περιπτώσεις την τερματίζουν.

ΚΟΙΝ.ΛΕΙΤ: Θα μπορούσατε να μου αναφέρετε κάποιο περιστατικό όπου κλιθήκατε για να βοηθήσετε;

ΨΥΧΟΛΟΓΟΣ: Υπάρχουν πολλά περιστατικά αυτοχείρων όπου σε online σύνδεση απειλούν ότι θα αυτοκτονήσουν ή αποχαιρετούν τους φίλους τους υπονοώντας ότι θα φύγουν από την ζωή. Οι ειδικοί του τμήματος Δίωξης εντόπισαν τέτοιες συνομιλίες σε chat rooms μεταξύ χρηστών και κινητοποιήθηκαν για τον εντοπισμό τους .Συγκεκριμένα ένα νεαρό ζευγάρι ενηλίκων ανακοίνωνε ότι θα αυτοκτονήσει επειδή οι οικογένειες τους δεν αποδέχονταν τον έρωτα τους καθώς και δύο νεαροί 15 κ 13 χρονών αποχαιρετούσαν τους φίλους τους λέγοντας πως είναι μάταιη ζωή τους .Κλιθήκαμε λοιπόν αμέσως από το τμήμα, ψυχολόγοι και κοινωνικοί λειτουργοί από τα γραφεία της Μ.Κ.Ο και του χαμόγελου του παιδιού ώστε να διερευνήσουμε επιστημονικά τα μηνύματα των χρηστών και να προσφέρουμε άμεσα τις υπηρεσίες μας στους ίδιους και στις οικογένειες τους. Ευτυχώς επιτύχαμε τον στόχο μας κ δράσαμε άμεσα και αποτρέψαμε

το ζευγάρι κ τα ανήλικα παιδιά .Κάθε περίπτωση είναι ξεχωριστή και προσπαθούμε να βοηθήσουμε όσο μπορούμε .

ΚΟΙΝ.ΛΕΙΤ: Ποιες οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

ΨΥΧΟΛΟΓΟΣ: Έχω να καταθέσω κάποιες προτάσεις χωρίς να θεωρώ τον εαυτό μου ειδικό στο διαδίκτυο. Θα πρέπει να παρθούν προληπτικά μέτρα ενημερώνοντας αρχικά τους πολίτες για τους τρόπους που θα μπορούσαν να προφυλαχθούν από το διαδίκτυο αλλά και για τις μορφές διαδικτυακού εγκλήματος .Θα πρέπει να δημιουργηθούν διαδικτυακοί τόποι αποτροπής αυτοκτονιών όπου ειδικοί θα συμβουλεύουν μέσω online συνομιλία .Πέρα από τα προληπτικά μέτρα ,θα πρέπει να παρθούν και κατασταλτικά μέτρα όπου πρωταγωνιστικό ρόλο καλούνται να αναλάβουν οι αστυνομικές αρχές ,να διατεθούν από το κράτος τα απαραίτητα μέσα και να αναπτυχθεί το θεωρητικό υπόβαθρο των αστυνομικών για τον εντοπισμό και την σύλληψη των εγκληματιών. Τέλος καλό θα ήταν να ευαισθητοποιηθούν ομάδες ειδικών επαγγελματιών που μπορούν να παίξουν ενεργό ρόλο στην αναγνώριση αυτοκαταστροφικών ατόμων όπως οι εκπαιδευτικοί που έχουν άμεση καθημερινή επαφή με μαθητές.

8η ΣΥΝΕΝΤΕΥΞΗ

ΕΙΔΙΚΟΤΗΤΑ:ΨΥΧΟΛΟΓΟΣ

ΤΟΠΟΘΕΣΙΑ: ΙΑΤΡΕΙΑ ΑΣΤΥΝΟΜΙΚΟΥ ΜΕΓΑΡΟΥ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΚΟΙΝ.ΛΕΙΤ: Ποιες είναι οι συνηθέστερες μορφές απάτης στο διαδίκτυο που γνωρίζετε και έχετε συναντήσει μέσα από την Υπηρεσία από όπου εργάζεστε;

ΨΥΧΟΛΟΓΟΣ: Η εξάπλωση του διαδικτυακού εγκλήματος τα τελευταία χρόνια είναι πολύ μεγάλη με αποτέλεσμα καθημερινά να φτάνουν στην Δίωξη Ηλεκτρονικού Εγκλήματος πολλές περιπτώσεις που να σχετίζονται με το ηλεκτρονικό έγκλημα. Συνήθως η πιο συχνή μορφή απάτης που συναντούμε είναι η οικονομική απάτη. Χωρίς αυτό να σημαίνει πως τα ποσοστά εμφάνισης των άλλων μορφών απάτης στο διαδίκτυο απέχουν με

μεγάλη διαφορά από την οικονομική απάτη. Για παράδειγμα συναντούμε και πολλές περιπτώσεις σεξουαλικής παρενόχλησης μέσω διαδικτύου, όπου ενήλικες δημιουργούν ψεύτικα προφίλ στα διάφορα Chat rooms(facebook, msn κτλ.)προσπαθώντας να προσεγγίσουν τους ανήλικους χρήστες είτε για να προβούν σε σεξουαλική παρενόχληση είτε στο να τους αποσπάσουν φωτογραφικό υλικό ή κάποιο βιντεάκι που πιθανόν να έχουν , έτσι οδηγούμαστε μετά και στην διακίνηση πορνογραφικού υλικού αλλά και πολλές περιπτώσεις, ιδιαίτερα τελευταία, που σχετίζονται με την αυτοκτονία. Θα λέγαμε πως αποτελεί «μόδα» ή και «παιχνίδι» η προτροπή κάποιου ατόμου στην αυτοκτονία ή η ανακοίνωση ότι κάποιος σκοπεύει να προβεί σε τέτοιου είδους ενέργεια.

ΚΟΙΝ.ΛΕΙΤ: Θα ήθελα να μου πείτε λίγα λόγια για τον ρόλο του ψυχολόγου στην αντιμετώπιση του φαινομένου και στην προστασία των θυμάτων;

ΨΥΧΟΛΟΓΟΣ: Αρχικά να σου ξεκαθαρίσω πως δεν υπάρχει ψυχολόγος στο τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος, ο οποίος να ασχολείται αποκλειστικά με περιπτώσεις διαδικτυακού εγκλήματος. Άλλωστε το ίδιο το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος είναι ένα νεοσύστατο σχετικά τμήμα ακόμη. Ευελπιστούμε στο μέλλον να υπάρξει αποκλειστικά θέση ψυχολόγου ή κοινωνικού λειτουργού στο συγκεκριμένο τμήμα. Προς το παρόν όμως, εμείς οι ψυχολόγοι της αστυνομίας πλαισιώνουμε και το συγκεκριμένο τμήμα μέσα σε όλες τις υπόλοιπες δραστηριότητες που αναλαμβάνουμε. Όσον αφορά την εμπλοκή μας με το συγκεκριμένο τμήμα, ασχολούμαστε κυρίως με την αποτροπή ενός ατόμου στο να προβεί σε αυτοκτονία, σκιαγραφούμε πολλές φορές το προφίλ ενός παιδόφιλου για να μπορέσουν να μπουν σε ομάδες παιδόφιλων οι αστυνομικοί με σκοπό να έχουν επικοινωνία μαζί τους, έτσι ώστε να τους εμπιστευτούν και να φτάσουμε στον εντοπισμό τους. Αυτές κυρίως είναι οι περιπτώσεις όπου παρεμβαίνουμε εμείς, η αυτοκτονία και η σκιαγράφηση του προφίλ του δράστη. Βέβαια σε περιπτώσεις σεξουαλικής κακοποίησης, κυρίως ανηλίκων, ή και σε περιπτώσεις αυτοκτονιών που υπάρχουν ανήλικοι, ο ψυχολόγος προσεγγίσει το θύμα και ξεκινούν μια συνεργασία ώστε να παραχθεί στο θύμα ψυχολογική υποστήριξη.

ΚΟΙΝ.ΛΕΙΤ: Για ποιο λόγο πιστεύετε ότι έχουν αυξηθεί τα ποσοστά διαδικτυακών εγκλημάτων;

ΨΥΧΟΛΟΓΟΣ: Κοίτα, καλώς η κακώς περίπου το 80% του πλανήτη μας σήμερα χρησιμοποιεί έναν ή και περισσότερους ηλεκτρονικούς υπολογιστές. Έτσι βλέπουμε πόσα άτομα έχουν πρόσβαση στο διαδίκτυο και με την βοήθεια της ανωνυμίας που τους προσφέρει το διαδίκτυο ή ακόμη και της δημιουργίας ενός ψεύτικου προφίλ που στην πραγματική τους ζωή δεν θα είχαν ποτέ, φτάνουν σε σημείο να προβούν ευκολότερα σε εγκληματικές πράξεις από ότι θα έκαναν στην πραγματική τους ζωή. Θεωρώ πως όλα αυτά τα εγκλήματα που υπάρχουν στο διαδίκτυο προϋπήρχαν και πριν την χρήση υπολογιστών, απλά τώρα είναι μεγαλύτερη η δικτύωση που αποκτούν οι δράστες και πιο αυξημένη η απειλή προσέγγισης που έχουν τα θύματα από τους δράστες.

ΚΟΙΝ.ΛΕΙΤ: Ποιες οι προτάσεις σας για την καταπολέμηση του φαινομένου και για την προστασία των θυμάτων;

ΨΥΧΟΛΟΓΟΣ: Τώρα μου βάζεις δύσκολα! Σίγουρα θα πρέπει να προσληφτούν περισσότεροι ψυχολόγοι και κοινωνικοί λειτουργοί στην αστυνομία, γιατί εμείς εδώ είμαστε τρία άτομα και προσπαθούμε να καλύψουμε όλες τις περιπτώσεις της αστυνομίας στην περιοχή της Θεσσαλονίκης αλλά και στην ευρύτερη περιοχή της Βόρειας Ελλάδας πράγμα το οποίο είναι αδύνατον και πολλές φορές ζητούμε την βοήθεια και συνεργασία συναδέλφων από άλλες υπηρεσίες. Βασικά αυτό, να γίνουν περισσότερες προσλήψεις ψυχολόγων και κοινωνικών λειτουργών. Επίσης καλό θα ήταν να ευαισθητοποιήσουμε και να ενημερώσουμε την κοινότητα για το διαδικτυακό έγκλημα και τις μορφές τους αλλά και τον τρόπο προστασίας τους με διάφορες εκδηλώσεις και ομιλίες, έτσι ώστε τα εν δυνάμει θύματα να μην φτάσουν να γίνουν θύματα επιτήδειων δραστών. Ιδιαίτερα όσον αφορά τους ανήλικους θα πρέπει να γίνουν ομιλίες σε σχολεία για να ενημερωθούν, τόσο τα παιδιά όσο και οι γονείς και οι εκπαιδευτικοί για το πώς μπορούν να προστατευτούν από τα εγκλήματα του διαδικτύου. Επίσης θα πρέπει να στελεχωθούν με περισσότερα άτομα οι γραμμές εντοπισμού και αποτροπής διαδικτυακών εγκλημάτων και να

δημιουργηθούν και νέες γραμμές αν κρίνεται απαραίτητο. Τέλος καλό θα ήταν τέτοιου είδους συμπεριφορές, είτε ως δράστης είτε ως θύμα, να προλαμβάνονται στο σχολείο με την ύπαρξη ενός ψυχολόγου ή κοινωνικού λειτουργού, ο οποίος θα μπορεί να εντοπίσει μια τέτοια συμπεριφορά

Γ. ΑΝΟΙΧΤΗ ΓΡΑΜΜΗ ΚΑΤΑΓΓΕΛΙΩΝ ΓΙΑ ΠΑΡΑΝΟΜΟ ΠΕΡΙΕΧΟΜΕΝΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ(SafeLine)

Το Διαδίκτυο έχει κατακτήσει διεθνώς την πρώτη θέση στον τομέα της ενημέρωσης, της ψυχαγωγίας αλλά και της επικοινωνίας. Η πληθώρα των θεμάτων και των δραστηριοτήτων που μπορεί κανείς να συναντήσει στον Κυβερνοχώρο είναι τόσο μεγάλη που προσελκύει χρήστες διαφόρων ηλικιών και ενδιαφερόντων. Στα πλαίσια αυτής της ποικιλομορφίας των πληροφοριών που προσφέρει το Διαδίκτυο, αναπόφευκτα έχουν παρουσιαστεί και περιπτώσεις διαφόρων επιτηδείων οι οποίοι εκμεταλλευόμενοι τις δυνατότητες του Κυβερνοχώρου προβαίνουν σε εγκληματικές δραστηριότητες. Δεν είναι λίγες οι φορές που χρήστες του Διαδικτύου έχουν έρθει αντιμέτωποι με περιεχόμενο ανάρμοστο και επιβλαβές που συχνά χαρακτηρίζεται από την Ελληνική Νομοθεσία και ως παράνομο. Η ασφαλής πλοήγηση στο Διαδίκτυο είναι δικαίωμα τόσο των ενηλίκων όσο και των ανηλίκων χρηστών το οποίο πρέπει να διαφυλαχθεί με κάθε δυνατό τρόπο από τη διεθνή κοινότητα. Σε αυτήν την προσπάθεια συντελεί και η SafeLine, από τις 14 Απριλίου του 2003, ημέρα αρχής της λειτουργίας της. (www.safeline.gr)

Η Ανοικτή Γραμμή Safe Line δέχεται καταγγελίες για δικτυακούς τόπους (websites) και υπηρεσίες νέων (news groups) που περιέχουν παράνομο περιεχόμενο και οι οποίες αντιμετωπίζονται με την προώθησή τους στις αστυνομικές και δικαστικές αρχές. Για την αντιμετώπιση του βλαβερού περιεχομένου οι χρήστες θα πρέπει να χρησιμοποιούν τεχνολογικές λύσεις (συστήματα φιλτραρίσματος και βαθμολόγησης περιεχομένου). Το ενδιαφέρον της Safe Line επικεντρώνεται κυρίως σε θέματα προστασίας

των παιδιών (π.χ. παιδική πορνογραφία**)** και της ανθρώπινης αξιοπρέπειας (π.χ. ρατσισμός και βία). (www.safeline.gr)

Πιο συγκεκριμένα πρωταρχικός ρόλος της SafeLine είναι να παρέχει ένα σημείο επικοινωνίας για τους χρήστες που επιθυμούν την ποινική δίωξη και την αφαίρεση από το Διαδίκτυο παράνομου περιεχομένου. Η Ανοιχτή Γραμμή SafeLine δέχεται καταγγελίες για περιεχόμενο που συναντάτε στο Διαδίκτυο και χαρακτηρίζεται παράνομο. Τα μέλη της SafeLine στη συνέχεια θα εξετάσουν την καταγγελία και θα κάνουν τις σωστές ενέργειες για την αναφορά της καταγγελίας στις αρχές για περαιτέρω επεξεργασία. Ο χρήστης που κατέθεσε μια καταγγελία έχει το δικαίωμα να πληροφορηθεί για το αποτέλεσμα της μόλις αυτό είναι επιτρεπτό. Αν κάποιος χρήστης το επιθυμεί μπορεί να κρατήσει την ανωνυμία του. Τα στοιχεία των χρηστών που καταθέτουν καταγγελίες είναι άκρως εμπιστευτικά. (www.safeline.gr)

Η SafeLine έχει σαν στόχο της να αποτελέσει σημείο αναφοράς για χρήστες που επιθυμούν να προστατέψουν τους εαυτούς τους καθώς και τις οικογένειες τους από παράνομο περιεχόμενο που υπάρχει στο Διαδίκτυο. Γι' αυτό τον σκοπό, όπως προαναφέρθηκε παραπάνω, η ιστοσελίδα της SafeLine προσφέρει μια συλλογή από συμβουλές για γονείς και παιδιά καθώς και μια λίστα από συνήθεις ερωτήσεις με σκοπό να πληροφορήσει με απλό τρόπο τον χρήστη για διαδικαστικά, νομικά καθώς και τεχνολογικά θέματα που σχετίζονται με την ασφάλεια στο Διαδίκτυο. Τεχνολογικά θέματα περιλαμβάνουν την ύπαρξη φίλτρων λογισμικού που φράζουν σελίδες του Διαδικτύου με επιβλαβές περιεχόμενο. Μια συλλογή από συνδέσμους μπορούν να χρησιμεύσουν σαν αρχή της περιπλάνησης σας για θέματα ασφάλειας του Διαδικτύου. (www.safeline.gr)

ΜΕ ΠΟΙΟΥΣ ΤΡΟΠΟΥΣ ΓΙΝΕΤΑΙ Η ΚΑΤΑΓΓΕΛΙΑ

Για την υποβολή καταγγελίας που αφορά ιστοσελίδες ή υπηρεσίες νέων (newsgroups) με παράνομο περιεχόμενο η καταγγελία γίνεται με έναν από τους παρακάτω τρόπους:

- **Μέσω Διαδικτύου**, συμπληρώνοντας την ηλεκτρονική φόρμα υποβολής καταγγελίας: http://www.safeline.gr/report/.

- **Μέσω e-mail**, στην ηλεκτρονική διεύθυνση report@safeline.gr
- **Ταχυδρομικά**, στέλνοντας την καταγγελία σας με επιστολή, στη διεύθυνση: SafeNet, Στουρνάρη 63, 10432 Αθήνα.
- **Τηλεφωνικά**, καλώντας στο τηλέφωνο **2811391615** τις εργάσιμες ημέρες από τις 9:00 έως τις 16:00.

Σε περίπτωση που απλώς κάποιος θέλει να εκθέσει μια απορία ή να ζητήσει οποιαδήποτε συμβουλή ή πληροφορία από τους ειδικούς της συγκεκριμένης γραμμής χωρίς αυτό να αποτελεί καταγγελία, μπορεί να στείλει ηλεκτρονικό μήνυμα στο contact@safeline.gr. (www.safeline.gr)

Οι παραπάνω τρόποι καταγγελίας είναι πάρα πολύ απλοί και εξυπηρετούν τις δυνατότητες κάθε χρήστη-καταγγέλλοντα. Αυτό όμως που είναι αξιοσημείωτο για την διαδικασία υποβολής καταγγελιών είναι η **ανωνυμία** την οποία μπορεί να διατηρήσει ο καταγγέλλον. Αυτό σημαίνει πως ο χρήστης-καταγγέλλον εφόσον δεν επιθυμεί να φανεί η ταυτότητά του μπορεί να αποκρύψει τα προσωπικά του στοιχεία. Η διεύθυνση IP του υπολογιστή που χρησιμοποιείται για την καταγγελία δεν καταγράφεται από το σύστημα της **SafeLine** και αν κάποιος χρήστης θελήσει να δώσει τα στοιχεία του, αυτά είναι απολύτως απόρρητα και χρησιμοποιούνται αποκλειστικά για την ενημέρωσή του σχετικά με την εξέλιξη της καταγγελίας του. Η διασφάλιση της ανωνυμίας του καταγγέλλοντα έχει ως σκοπό να αποβάλει κάθε πιθανό δισταγμό του για την υποβολή καταγγελίας. (www.safeline.gr)

ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΤΑΓΓΕΛΙΑΣ

Τα βήματα που ακολουθεί η SafeLine, για την επεξεργασία των καταγγελιών που λαμβάνει, είναι τα εξής:

→ **Επαλήθευση:** Πρώτα γίνεται από την SafeLine μια τυπική επαλήθευση του περιεχόμενου της καταγγελίας. Για παράδειγμα, αν πρόκειται για δικτυακό τόπο (website), η SafeLine επαληθεύει ότι διεύθυνση (URL) που καταγγέλθηκε υπάρχει και το περιεχόμενό της είναι πιθανόν παράνομο.

→ **Ανεύρεση πηγής περιεχομένου:** Έπειτα επιχειρείται να βρεθεί η χώρα προέλευσης του περιεχομένου χρησιμοποιώντας τεχνικές μεθόδους.

→ **Ειδοποίηση Ελληνικής Αστυνομίας:** Η SafeLine προωθεί όλες ανεξαιρέτως τις καταγγελίες, ανεξάρτητα από την χώρα προέλευσης, στην Ελληνική Αστυνομία.

→ **Ειδοποίηση ξένου hotline:** Σε περίπτωση που το περιεχόμενο βρίσκεται στο εξωτερικό, η καταγγελία προωθείται σε αντίστοιχη ανοικτή γραμμή (hotline) της χώρας προέλευσης (εάν υπάρχει).

→ **Ενημέρωση:** Εάν ο καταγγέλλον χρήστης έχει δώσει προσωπικά του στοιχεία, τότε η SafeLine τον ενημερώνει για τις ενέργειες που έκανε με βάση την καταγγελία του. (www.safeline.gr)

Θα πρέπει να σημειωθεί πως η Ανοιχτή Γραμμή καταγγελιών για παράνομο περιεχόμενο στο Διαδίκτυο διοργανώνει πολύ συχνά Συνέδρια και Ημερίδες για την ενημέρωση της κοινότητας για την προστασία τους από Εγκλήματα του Διαδικτύου. Επιπλέον, αξιόλογη θεωρείται η προσπάθεια ενημέρωσης που γίνεται σε διάφορα σχολεία όσον αφορά τους κινδύνους του Διαδικτύου.

ΟΙ ΣΥΝΕΡΓΑΤΕΣ ΤΗΣ SAFELINE

- ΙΤΕ - Ίδρυμα Τεχνολογίας και Έρευνας, Ινστιτούτο Πληροφορικής
- SAFENET - Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Διαδικτύου

- Η χρηματοδότηση της λειτουργίας γίνεται από τους παραπάνω οργανισμούς και από το πρόγραμμα της **Ευρωπαϊκής Ένωσης** "Safer Internet Plus". Επίσης, η SafeLine συνεργάζεται με τον Ελληνικό Κόμβο Ασφαλούς Διαδικτύου.

ΙΔΡΥΤΙΚΑ ΜΕΛΗ ΤΗΣ SAFELINE

Η SafeLine ιδρύθηκε το 2003 από τους ακόλουθους οργανισμούς:

- SAFENET - Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Διαδικτύου
- FORTHnet - Ελληνική Εταιρία Τηλεπικοινωνιών και Τηλεματικών Εφαρμογών
- ITE - Ίδρυμα Τεχνολογίας και Έρευνας, Ινστιτούτο Πληροφορικής
- IME - Ίδρυμα Μείζονος Ελληνισμού

Οι παραπάνω οργανισμοί συμμετείχαν και στη συγχρηματοδότηση της λειτουργίας της SafeLine (μαζί με το "Safer Internet Action Plan") μέχρι και το 2008. Από τις 1/1/2009 η SafeLine λειτουργεί με την τωρινή της σύνθεση.