ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ **Α**ΝΘΡΩΠΙΣΤΙΚΩΝ & **Κ**ΟΙΝΩΝΙΚΩΝ **Ε**ΠΙΣΤΗΜΩΝ & **Δ**ΙΚΑΙΟΥ

ΕΓΚΛΗΜΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΚΩΝΣΤΑΝΤΙΝΑΣ Π. ΛΙΑΝΟΥ

Επιβλέπων : Άρης Κουτούγκος
Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΑΝΘΡΩΠΙΣΤΙΚΩΝ & ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΚΑΙΟΥ

ΕΓΚΛΗΜΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΚΩΝΣΤΑΝΤΙΝΑΣ ΛΙΑΝΟΥ

Επιβλέπων : Άρης Κουτούγκος
Καθηγητής Ε.Μ.Π.

Υπεύθυνη: Αλίκη ΧΑΤΖΟΠΟΥΛΟΥ ΤΖΙΚΑ
Ομότιμη Καθηγήτρια ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την … Φεβρουαρίου 2013.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Άρης Κουτούγκος	Παναγιώτης Μιχαηλίδης	Κωνσταντίνος Δέρβος
Καθηγητής Ε.Μ.Π.	Επικ. Καθηγήτης Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2013

(Υπογραφή)

.....

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά, θα ήθελα να ευχαριστήσω θερμά την ομότιμη καθηγήτρια κ. Αλίκη ΧΑΤΖΟΠΟΥΛΟΥ-ΤΖΙΚΑ που μου ανέθεσε αυτήν την διπλωματική εργασία, καθώς και για την συνεργασία της και τις πολύτιμες συμβουλές καθ' όλη τη διάρκειά της.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Κωνσταντίνο Δέρβο για την συνεργασία του .

Ευχαριστώ, τέλος, από τα βάθη της καρδιάς μου την οικογένειά μου για τη διαρκή τους υποστήριξη όλα αυτά τα χρόνια, και φυσικά τους φίλους μου για τη συμπαράσταση και βοήθεια, που εξακολουθούν να μου δείχνουν, και που τα κάνει όλα δυνατά!

ΠΕΡΙΛΗΨΗ

Είναι γεγονός αναμφισβήτητο ότι οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο αποτελούν πλέον ένα από τα πιο σπουδαία επιτεύγματα της τεχνολογίας. Έχουν φέρει τη δική τους επανάσταση στη ανθρωπινή καθημερινότητα, στην επιστήμη, στην εκπαίδευση. Οι άπειρες δυνατότητες που προσφέρουν είναι ο λόγος για τη συνεχή προσπάθεια του ανθρώπου να ανακαλύψει, να εξελίξει, και να εκμεταλλευτεί περαιτέρω δυνατότητες. Ο ηλεκτρονικός υπολογιστής και το διαδίκτυο είναι κάτι πολύ περισσότερο από ένα βοήθημα για τον άνθρωπο αφού σε πολλές περιπτώσεις εκεί εκθέτονται στοιχεία προσωπικών δεδομένων ενός πολίτη ή στοιχεία που οδηγούν πολύ εύκολα στον εντοπισμό πληροφοριών αυτού.

Ελλοχεύει λοιπόν ο κίνδυνος κάθε είδους απατής από επίσης καλούς γνώστες της τεχνολογίας που θέτουν αυτή ως μέσο πραγματοποίησης παράνομων πράξεων και έτσι η τεχνολογία με αυτό το χειρισμό αποτελεί «όπλο» στραμμένο στον πολίτη - χρηστή. Οι δυνατότητες δίωξης από τις αρμόδιες αρχές δεν αποτελούν εμπόδιο αυτής της μορφής εγκλήματος αφού, οι εν λόγο δυνατότητες είναι περιορισμένες λόγω έλλειψης εμπειρίας κ επαρκούς εκπαίδευσης στο τομέα αυτό ενώ το σχετικό νομοθετικό πλαίσιο είναι ασαφές.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Ηλεκτρονικό έγκλημα, χάκερ, διαδίκτυο, έγκλημα, εθισμός, πρόληψη , ασφάλεια.

ABSTRACT

It is an undeniable fact that computers and the Internet have become one of the most important achievements of technology. They have brought their own revolution in human daily life, in science, in education. The infinite potential is the reason for the continuous effort of man to discover, evolve, and exploit further opportunities. The computer and the Internet is much more than a tool for the man because in many cases there are exhibited items of personal data of a citizen or elements that drive very easy to identify this information.

There could therefore be a risk of any type of fraud is also very knowledgeable of the technology to put this as a tool to carry out illegal acts, so the technology is handling this "weapon" turned the citizen. The potential prosecution by the relevant authorities do not prevent this type of crime because, they reason, options are limited due to lack of experience and adequate training in this area, and the legal framework is unclear.

KEYWORDS

Cybercrime, hacker, internet , crime, addiction, prevention, safety.

ΕΙΣΑΓΩΓΗ

Αντικείμενο της παρούσας εργασίας αποτελεί η μελέτη του σύγχρονου και ταχύτατα αυξανόμενου φαινομένου του ηλεκτρονικού εγκλήματος και οι μορφές με τις οποίες αυτό παρουσιάζεται και επηρεάζει πολλές πτυχές του σύγχρονου χρήστη ηλεκτρονικού υπολογιστή και του διαδικτύου.

Σκοπός μας αποτελεί η εξαγωγή συμπερασμάτων σχετικά με τον τρόπο που ο χρήστης κάθε ηλικίας δύναται να προστατευτεί από την σύγχρονη αυτή μορφή εγκληματικότητας καθώς και η μελέτη μερικών μεθόδων μέσω των οποίων οι διωκτικές αρχές δύναται να αντιμετωπίσουν τον δράστη τέτοιων εγκλημάτων.

Η έρευνα μας βασίστηκε τόσο σε βιβλιογραφικές αναφορές ηλεκτρονικής και έντυπης φύσεως όσο και σε πραγματικά στοιχεία που καταφέραμε να συλλέξουμε από την ΕΛ. ΑΣ και το νοσοκομείο Παίδων «Παν& Αγλ. Κυριακού». Οι προεκτάσεις που δώσαμε και τα στοιχεία που παραθέτουμε είναι σαφώς πολύ περιορισμένα σε σχέση με το πραγματικό φαινόμενο.

Στο **πρώτο** κεφάλαιο ορίζονται οι έννοιες του εγκλήματος και του διαδικτύου ξεχωριστά στην αρχή και στη συνέχεια ως δύο έννοιες που συναποτελούν το λεγόμενο ηλεκτρονικό έγκλημα. Στη συνέχεια του ίδιου κεφαλαίου, παρουσιάζονται τα βασικά είδη του ηλεκτρονικού εγκλήματος, η ιστορική εξέλιξη καθώς και τα κυριότερα χαρακτηριστικά του γνωρίσματα.

Στο **δεύτερο** κεφάλαιο, αναλύονται διεξοδικά οι μορφές του ηλεκτρονικού εγκλήματος, αφού πρώτα έχει γίνει η κατηγοριοποίηση των επιμέρους εγκλημάτων .

Στο **τρίτο** κεφάλαιο γίνεται αναφορά σε νομοθετικά ζητήματα γύρω από τη διαδικτυακή εγκληματικότητα.

Στο **τέταρτο** κεφάλαιο αναφέρονται γενικά χαρακτηριστικά τα οποία με μεγάλη πιθανότητα συναντιόνται στην προσωπικότητα του cybercriminal[1] καθώς και τα χαρακτηριστικά που πρέπει να συγκεντρώνει ένας καλός ερευνητής , ο οποίος χειρίζεται την διελεύκανση μιας υπόθεσης που αφορά την τέλεση ηλεκτρονικού εγκλήματος.

Στο **πέμπτο** κεφάλαιο αναφέρονται οι βασικότερες έννοιες που αφορούν την ασφάλεια, την πρόληψη καθώς και κάποιες από τις πλέον διαδομένες τακτικές προς αποφυγή της θυματοποίησης του πολίτη με την χρήση ηλεκτρονικού υπολογιστή.

Στο **έκτο** κεφάλαιο αναφέρονται μια συνοπτική ιστορική αναδρομή στο φαινόμενο του εθισμού, τα κλινικά κριτήρια που τον οριοθετούν καθώς και τα αίτια και οι ηλικιακές ομάδες οι οποίες εμφανίζουν συχνότερα εθισμό. Κατόπιν παρουσιάζεται έρευνα με τίτλο «ΧΡΗΣΗ ΚΑΙ ΚΑΤΑΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ (INTERNET): ΣΥΣΧΕΤΙΣΕΙΣ ΜΕ ΨΥΧΟΚΟΙΝΩΝΙΚΟΥΣ ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΧΡΗΣΤΕΣ –ΑΠΟΤΕΛΕΣΜΑΤΑ»που διεξήγαγε η Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.),/Πανεπιστήμιο Αθηνών και τα αποτελέσματα της.

Στο **έβδομο** κεφάλαιο αναφέρεται ο ρόλος της ΕΛ.ΑΣ καθώς και κάποιες τεχνικές εντοπισμού του διαδικτυακού δράστη.

Την εργασία συμπληρώνουν δύο παραρτήματα.

Το **πρώτο** περιλαμβάνει νομοθεσία γύρω από τα ηλεκτρονικά εγκλήματα, ισχύουσα στην Ελλάδα (άρθρα Ποινικού Κώδικα, Νόμοι, Προεδρικά Διατάγματα) αλλά και στην Ευρώπη (Οδηγίες). Στο **δεύτερο** παράρτημα παραθέτονται κάποια άρθρα από τις ηλεκτρονικές εκδόσεις καθημερινών εφημερίδων της Ελλάδας, που δείχνουν ξεκάθαρα σε πόσο μεγάλο βαθμό έχει εισχωρήσει η ηλεκτρονική εγκληματικότητα στην ζωή μας.

[1] Με τον όρο αυτό χαρακτηρίζεται ο δράστης τέλεσης ενός ηλεκτρονικού-διαδικτυακού εγκλήματος.

ΚΕΦΑΛΑΙΟ 1^{Ο}
ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Σε αυτό το κεφάλαιο θα αναλυθεί το εγκληματικό φαινόμενο στη συμβατική του μορφή. Στη συνέχεια θα αναφερθούμε στην έννοια του διαδικτύου και πως η είσοδος του στην καθημερινότητα μας έχει φέρει τεράστιες αλλαγές. Τέλος αναφορά γίνεται στη νέα μορφή παραβατικής συμπεριφοράς που καλείται «ηλεκτρονικό» ή αλλιώς «ψηφιακό» έγκλημα. Παρατίθενται ιστορικά στοιχεία καθώς και τα κυριότερα χαρακτηριστικά του.

1.1 Τι είναι έγκλημα.

Το έγκλημα έχει φύση σύνθετη, γιατί σε αυτήν συναντώνται και την συγκαθορίζουν από την μία μεριά η κοινωνική, βιολογική και ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει στο πλαίσιο ορισμένης κοινωνίας την κοινωνική συμπεριφορά του. Έτσι το έγκλημα είναι αξεχώριστα τόσο ως οντολογικό όσο και ως αξιολογικό φαινόμενο. Δεν είναι ούτε μόνο το ένα ούτε μόνο το άλλο. Η σύνθετη φύση του εγκλήματος μπορεί να αποδοθεί από τον χαρακτηρισμό του ως ορισμένου, αρνητικά αξιολογούμενου, φαινομένου της πραγματικότητας.[2]

Το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας και συμπεριφέρεται ως ένας οργανισμός που συνεχώς μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης καθώς και το νομικό πλαίσιο που το διέπει. Με διαφορετική μάσκα αλλά και περιεχόμενο πολλές φορές, ανάλογα με τις κοινωνικοπολιτικές και ηθικές τάσεις κάθε εποχής και τόπου το έγκλημα παραμένει παρόν, κινούμενο πάντα σε τρείς βασικούς άξονες, τα απαραίτητα συστατικά στοιχεία του, αυτά που το ορίζουν. **Ποια είναι όμως αυτά τα στοιχεία;**

Δογματικό ορισμό του εγκλήματος μας δίνει ο ίδιος ο Ποινικός Κώδικας μας στην διάταξη του άρθρου 14. Έτσι σύμφωνα με το άρθρο 14 Π.Κ. «έγκλημα

[2]Γ.Α. Μαγκάκης «Ποινικό Δίκαιο», έκδοση γ΄ βελτιωμένη, εκδόσεις Παπαζήση, 1984

είναι πράξη άδικος και καταλογιστή εις τον πράξαντα, τιμωρούμενη υπό του νόμου».

Το ουσιαστικότερο περιεχόμενο του εγκλήματος συνίσταται στο ότι :είναι η πράξη εκείνη που θίγει τις αξίες της κοινωνική ζωής στις γενικότερης αποδοχής πλευρές της, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά απόλυτα αναγκαία.[3]

Το εγκληματικό φαινόμενο αποτελεί ιστορικό, κοινωνικό φαινόμενο καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Αυτό που έχει ιδιαίτερη σημασία να επισημάνουμε είναι η διαχρονικότητα του στο πέρασμα των αιώνων. Καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό, αν και σε κάθε έγκλημα (προσβολή), υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση), απεναντίας. Αντίθετα αυτό που παρατηρείται είναι μια αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς.[4]

Σε κάθε κοινωνία υπάρχουν κανόνες οι οποίοι θεσπίστηκαν τυπικά ή άτυπα (έθιμα) προκειμένου να προστατευτούν κοινωνικά αγαθά και άνθρωποι οι οποίοι παραβαίνουν τους κανόνες αυτούς. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων (ποινών) στους παραβάτες, οι οποίες αποτελούν τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση, καθώς και το είδος της ποινής, βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό.

Τα βασικά στοιχεία του εγκληματικού φαινομένου, κανόνας, έγκλημα, κύρωση (ποινή), συναποτελούν έναν αδιάσπαστο κύκλο. Εδώ είναι ξεκάθαρη η αλληλεξάρτηση των στοιχείων. Αν δεν υπήρχε έγκλημα δεν θα υφίστατο η κύρωση. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή την παράβασή του. Ο κανόνας δημιουργήθηκε για να οργανώσει και να προστατέψει τα κοινωνικά αγαθά (υλικά και άυλα) από κάθε προσβολή τους μέσα στα πλαίσια της κοινωνικής συμβίωσης. Στη συνέχεια, και αφού επέλθει η προσβολή του έννομου αγαθού (αυτό που προστατεύεται από τον κανόνα-νόμο), έρχεται η κύρωση (ποινή). Είναι με λίγα λόγια η κύρωση (ποινή) συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η

[3] Γ.Α. Μαγκάκης «Ποινικό Δίκαιο», έκδοση γ΄ βελτιωμένη, εκδόσεις Παπαζήση, 1984
[4] Γ.Α. Μαγκάκης «Ποινικό Δίκαιο», έκδοση γ΄ βελτιωμένη, εκδόσεις Παπαζήση, 1984

συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Θα λέγαμε ότι η ποινή αποτελεί την εκτόνωση της κοινωνικής αντίδρασης στο έγκλημα. Μπορεί δε, να παρουσιαστεί με πολλούς διαφορετικούς τρόπους, όσο αφορά τη ιδεολογική της προσέγγιση, όπως ως αποκατάσταση της διαταραχθείσας από το έγκλημα κοινωνικής τάξης ή ως το μέσο για την ηθική βελτίωση του παραβάτη.

1.2.1 Τι είναι το διαδίκτυο.

Το διαδίκτυο αποτελεί μία από τις βάσεις της σημερινής κοινωνίας. Έχει αλλάξει τον τρόπο με τον οποίο ο κόσμος επικοινωνεί, δουλεύει, μαθαίνει και το σπουδαιότερο ζει. Το διαδίκτυο (ιντερνέτ) μπορεί να περιγραφεί ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, το οποίο διασυνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων.[5]

Αποτελεί την κύρια μηχανή με την οποία άτομα επικοινωνούν μεταξύ τους ταχύτερα πλέον από ποτέ. Στα σπουδαιότερα πλεονεκτήματα του έχουν περιληφθεί, η ταχύτητα και η άνεση. Τα πάντα μπορούν να πραγματοποιηθούν με το πάτημα ενός κουμπιού του πληκτρολογίου ή με ένα κλικ του ποντικιού. Στο διαδίκτυο ο τόπος χάνει την σημασία του. Η σωστή χρήση του διαδικτύου μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών του προσφέροντας τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης Το διαδίκτυο και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές (Η/Υ), έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητας μας, είτε ως μέσα ψυχαγωγίας- ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων.

Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Στις μέρες μας, γίνεται σε μεγάλο βαθμό και η χρήση εφαρμογών κοινωνικής δικτύωσης (facebook, twitter, chat rooms).

[5] Ζάννη Αναστασία «Διαδικτυκό Έγκλημα» σελ. 23

1.2.2. Ποια η λειτουργία του διαδικτύου.

Το διαδίκτυο[6] είναι παγκοσμίως το μεγαλύτερο σύστημα υπολογιστών, το οποίο λόγω της ανοικτής δομής και της απεριόριστης εξάπλωσής του συνδέει εκατοντάδες εκατομμύρια χρήστες σε όλο τον κόσμο. Βασικό χαρακτηριστικό του είναι το γεγονός ότι δεν υπάρχει ένα συντονιστικό κέντρο[7] και τούτο σημαίνει ότι σε περίπτωση που καταστραφεί κάποιο τμήμα του, τότε οι πληροφορίες ακολουθούν άλλη δίοδο που παρακάμπτει το κατεστραμμένο τμήμα, ώστε να επιτυγχάνεται η συνεχής ροή δεδομένων εντός του συστήματος, δίνοντας έτσι την εντύπωση ενός ενιαίου πλέγματος.

Ειδικότερα, όλοι οι συνδεδεμένοι με το διαδίκτυο ηλεκτρονικοί υπολογιστές συνεργάζονται για να μεταφέρουν πληροφορίες προς διάφορες κατευθύνσεις σε όλο τον κόσμο. Με την αποστολή μιας τέτοιας ηλεκτρονικής πληροφορίας αυτή χωρίζεται από το TCP (Transmission Control Protocol) και το IP (Internet Protocol)[8] σε μικρότερα κομμάτια που ονομάζονται πακέτα (packets) και το καθένα αποκτά τη δική του ταυτότητα το κάθε μικρότερο κομμάτι της πληροφορίας (πακέτο) ακολουθεί διαφορετικό δρόμο, για να φτάσει στον προορισμό του. Όταν η ηλεκτρονική πληροφορία φτάσει στον προορισμό της, τότε όλα τα διασπασμένα κομμάτια (πακέτα) της πληροφορίας ενώνονται ξανά και υπεύθυνο για την ασφαλή και ορθή επανένωση αυτή είναι το TCP (Transmission Control Protocol) και το IP (Internet Protocol). Την κυκλοφορία μέσω του διαδικτύου διευθύνει ένας ειδικός υπολογιστής που ονομάζεται Router. Ένα πακέτο μπορεί να περάσει από πολλούς Routers ως τον προορισμό του.

Για να αποκτήσει κάποιος πρόσβαση στο διαδίκτυο, ώστε να γίνει δέκτης του πλήθους των υπηρεσιών που προσφέρει, πρέπει να επιλέξει έναν από του εξής τρόπους σύνδεσης με το διαδίκτυο:

1. **Διαρκής σύνδεση** με το διαδίκτυο υφίσταται όταν ο ηλεκτρονικός υπολογιστής είναι μόνιμα και άμεσα συνδεδεμένος με ένα δίκτυο, το οποίο είναι ακολούθως συνδεδεμένο με το διαδίκτυο. Μ' αυτόν τρόπο ο χρήστης έχει στη διάθεσή του διαρκώς όλες τις υπηρεσίες που προσφέρει το διαδίκτυο.

---

[6] Ονομάζεται εκτός από internet και net (δίκτυο) ή information superhighway (λεωφόρος των πληροφοριών) ή cyberspace (κυβερνοχώρος)

[7] Κιούπης Δ., «Ποινικό Δίκαιο και Internet», σελ. 22 και Καράκωστας Ι., «Δίκαιο και internet», σελ. 3

[8] Υπενθυμίζεται ότι το TCP (Πρωτόκολλο ελέγχου μεταβίβασης) και το IP (Πρωτόκολλο του διαδικτύου) είναι η κοινή γλώσσα των συνδεδεμένων με το διαδίκτυο υπολογιστών

Όμως λόγω του αυξημένου κόστους αυτού του τρόπου σύνδεσης αυτός είναι απαγορευτικός για τους απλούς χρήστες και προτιμάται από μεγάλες επιχειρήσεις και ιδρύματα.

2. **Προσωρινή άμεση σύνδεση** με το διαδίκτυο επιτυγχάνεται με τη χρήση ενός υπολογιστή, μιας συσκευής modem[9] και μιας τηλεφωνικής γραμμής και μέσω κλήσεως ενός συνδέσμου εισόδου που οδηγεί ευθέως στο διαδίκτυο. Κλασσικό παράδειγμα αυτού του είδους σύνδεσης είναι οι πανεπιστημιακοί σύνδεσμοι. Έτσι κάποιος φοιτητής καλώντας τον αριθμό τηλεφώνου του συνδέσμου εισόδου του πανεπιστημίου από τον προσωπικό του υπολογιστή και δίδοντας το όνομα συμμετοχής του και τον προσωπικό κωδικό εισόδου του στο δίκτυο συνδέεται άμεσα με το διαδίκτυο.

3. Ο συνηθέστερος τρόπος σύνδεσης με το διαδίκτυο είναι **η προσωρινή έμμεση σύνδεση**, που προϋποθέτει έναν υπολογιστή, μια συσκευή modem, μια τηλεφωνική γραμμή και την πληρωμή συνδρομής σε ένα φορέα παροχής πρόσβασης (Internet Service Provider)[10.] Πρακτικά, ο χρήστης καλεί τον αριθμό του παροχέα και μόλις επιτευχθεί η σύνδεση του είναι επιτρεπτή η «είσοδος» στο διαδίκτυο, όπου μπορεί να κάνει χρήση των διαφόρων λειτουργιών και υπηρεσιών του.

1.3. Ποια η έννοια του ηλεκτρονικού-διαδικτυακού εγκλήματος.

Το ιντερνέτ και οι Η/Υ παρέχουν στους χρήστες αφενός μεν ασύλληπτες δυνατότητες και αφετέρου όμως εισαγάγουν νέες μορφές παραβατικής συμπεριφοράς. Επιπρόσθετα «γεννώνται» αξιόποινες πράξεις που υφίστανται μόνο με τη χρήση Η/Υ και του ιντερνέτ, όπως η διασπορά κακόβουλου λογισμικού σε Η/Υ και η παραβίαση ηλεκτρονικών αρχείων. Έτσι, παραδοσιακές εγκληματικές πράξεις όπως εξύβριση ή δυσφήμιση, μέσω μιας ιστοσελίδας (web site) ή ηλεκτρονικού ταχυδρομείου, διαπράττονται πλέον ταχύτερα, με το διαδίκτυο να αποτελεί το κύριο μέσο τέλεσης τους. Το καθεστώς της ανωνυμίας των δραστών, η δυσκολία των διωκτικών αρχών στην διαλεύκανση της ηλεκτρονικής εγκληματικότητας με αποτέλεσμα την

[9] Δηλαδή ενός κωδικοποιητή που μετατρέπει τις πληροφορίες ενός ηλεκτρονικού υπολογιστή σε τέτοια μορφή που μπορεί να μεταδοθεί μέσω τηλεφωνικών γραμμών και αντίστροφα

[10] Οι φορείς παροχής πρόσβασης διακρίνονται σε : α) παροχείς πρόσβασης, που ανοίγουν στους πελάτες δίοδο στο διαδίκτυο μέσω δικής τους πρόσβασης σ' αυτό και β) παροχείς περιεχομένου, που προσφέρουν πρόσβαση στο διαδίκτυο και παράλληλα δυνατότητα πρόσβασης σε δικό τους περιεχόμενο και άλλες πρόσθετες υπηρεσίες

ελαχιστοποίηση της τιμωρίας του δράστη είναι εκείνα τα στοιχεία που τους ωθούν στην τέλεση αξιόποινων πράξεων μέσω Διαδικτύου Στις μέρες μας, παρά την εξέλιξη και ανάπτυξη των διωκτικών μηχανισμών, η διαλεύκανση της ηλεκτρονικής εγκληματικότητας παραμένει μία δύσκολη υπόθεση.

Είναι όμως το ηλεκτρονικό έγκλημα διαδικτυακό;

Είναι πλέον αναγκαίο να γίνεται διάκριση μεταξύ του λεγόμενου ηλεκτρονικού εγκλήματος και του διαδικτυακού (cyber crime) το οποίο παρουσιάζει ποιοτικά σημαντικές διαφοροποιήσεις από το πρώτο λόγω των ιδιαίτερων χαρακτηριστικών του διαδικτύου, που συνοψίζονται στη δυνατότητα ανταλλαγής δεδομένων και προγραμμάτων μεταξύ όλων των συνδεδεμένων υπολογιστών.

Επίσης πρέπει να σημειωθεί η δυσκολία στη διατύπωση ενός ενιαίου ορισμού που να περιλαμβάνει όλες τις εκφάνσεις του διαδικτυακού εγκλήματος, κάτι που παρατηρείται και αναφορικά με τον εννοιολογικό προσδιορισμό εν γένει της ηλεκτρονικής εγκληματικότητας. Τούτο συμβαίνει διότι οι παραβάσεις στο διαδικτύου παρουσιάζουν ποικιλομορφία ως προς τις μορφές εκδήλωσης τους και κατατείνουν στην προσβολή διαφόρων κάθε φορά έννομων αγαθών.

Συμφωνά με ορισμό που δόθηκε από τους **Forester and Morrison (1994),** είναι «Μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Ένας άλλος ορισμός, από τους πλέον διαδεδομένους, είναι αυτός που δόθηκε από τον Οργανισμό **Οικονομικής Συνεργασίας και Ανάπτυξης**, αρκετά χρόνια πριν (1986). Έτσι λοιπόν, «Ηλεκτρονικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων».

Απαραίτητο στοιχείο για την τέλεση ηλεκτρονικού εγκλήματος, θεωρείται η ύπαρξη συσκευής ηλεκτρονικής επεξεργασίας δεδομένων όπως είναι ο ηλεκτρονικός υπολογιστής, το κινητό τηλέφωνο κλπ. Σύμφωνα με τον **Shinder** (2002), ο ρόλος που διαδραματίζει ο Η/Υ στα πλαίσια του ηλεκτρονικού εγκλήματος είναι κυρίαρχος καθώς:

• Μπορεί να αποτελεί το στόχο κάποιας επίθεσης, στη συγκεκριμένη περίπτωση ο Η/Υ είναι το «θύμα» της επίθεσης.

• Δύναται να αποτελεί μέσο για τη διάπραξη κάποιας επίθεσης. Εδώ είναι το εργαλείο που χρησιμοποιείται από το δράστη για την πραγματοποίηση εγκληματικού σκοπού.

• Τέλος, υπάρχει και η περίπτωση που ο Η/Υ αποτελεί βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Μέχρι στιγμής έχουμε προσδιορίσει τον όρο «ηλεκτρονικό έγκλημα», ο οποίος διαφοροποιείται από τον όρο του διαδικτυακού εγκλήματος . Η παραπάνω παρατήρηση δεν παραβλέπει σε καμία περίπτωση τη σχέση που τις συνδέει, η οποία είναι σχέση γένους προς είδος. Το ηλεκτρονικό έγκλημα είναι έννοια γένους που περιλαμβάνει εννοιολογικά και το διαδικτυακό έγκλημα χωρίς όμως να ταυτίζεται με αυτό. Το διαδικτυακό έγκλημα είναι δηλαδή μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος

Κατά τον ορισμό του **Donn Parker** «το διαδικτυακό έγκλημα λοιπόν ή αλλιώς κυβερνοέγκλημα (cyber-crime), είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, αυτό για την τέλεση του οποίου ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο. Σχετίζεται με την οιονδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο».

Αν λοιπόν θέλουμε να κατηγοριοποιήσουμε τις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων, σύμφωνα με τον **Αργυρόπουλο (2001),** θα διακρίνουμε τα παρακάτω ηλεκτρονικά εγκλήματα:

• Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.

• Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.

• Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσουμε τη διασπορά κακόβουλου λογισμικού.

Σύμφωνα με τον **Neil Barrett (1997)** τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο (2) κατηγορίες :

α) σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ , η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών

β) σε εκείνα που υποστηρίζονται από Η/Υ και οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά

Σύμφωνα με τον **Donald Pipkin (2003)** τα ηλεκτρονικά εγκλήματα διακρίνονται σε τέσσερις (4) κατηγορίες :

α) στην πρώτη κατηγορία ανήκουν τα παραδοσιακά εγκλήματα τα οποία τελούνται με χρήση Η/Υ και ως τέτοια αναφέρει την απάτη, την κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και την κλοπή της ηλεκτρονικής ταυτότητας.

β) στην δεύτερη κατηγορία υπάγονται τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια ο συγγραφέας θεωρεί την επίθεση της άρνησης παροχής υπηρεσίων , την άρνηση πρόσβασης σε πληροφόριες και τη διασπορά καταστρεπτικών ιών.

γ) στην τρίτη κατηγορία τοποθετεί τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί

δ) στην τέταρτη κατηγορία ανήκουν τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

Μια άλλη οπτική είναι η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων που προτάθηκε από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα που από την ίδρυση του στις αρχές της δεκαετία του 1980, διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του εγκλήματος μέσω Η/Υ σε δημόσιο και ιδιωτικό τομέα. Οι κατηγορίες είναι [11]

[11] Steven Furnell, «Κυβερνοέγκλημα, καταστρέφοντας την κοινωνία της πληροφορίας», μετάφραση Φωτεινή Μηλιώνη, εκδόσεις Παπαζήση, Αθήνα 2006, σελ.26,28

1. **απάτη**: Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή /συμπίεση/ ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς)
2. **κλοπή:** των δεδομένων, του λογισμικού
3. **χρήση** λογισμικού χωρίς άδεια: χρήση παράνομων αντιγράφων λογισμικού
4. **ιδιωτική εργασία**: μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκοδιμή κέρδους ή για ίδιον όφελος
5. **χάκινγκ:** :ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας
6. **σαμποτάζ:** η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό
7. **εισαγωγή:** πορνογραφικού υλικού
8. **ιοι:** διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής.

1.4 Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα.

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.

Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών , οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται.

1.5. Τα κυριότερα χαρακτηριστικά γνωρίσματα των εγκλημάτων στον κυβερνοχώρο.

Με την εμφάνιση όμως του φαινομένου της συνεχούς δικτύωσης των ηλεκτρονικών υπολογιστών τα νομικά ζητήματα έγιναν ακόμα πιο πολύπλοκα και η ανάγκη της νομικής αντιμετώπισης των συνεχώς νεοεμφανιζόμενων εγκληματικών συμπεριφορών πιο επιτακτικών. Ο εντοπισμός των χαρακτηριστικών της νέας γενιάς εγκληματικότητας φωτίζει την ανάγκη της θέσπισης των νέων κανόνων ποινικού δικαίου αναδεικνύοντας ταυτόχρονα την επικινδυνότητα και τις προεκτάσεις του νέου αυτού ποινικού φαινομένου. Συνοψίζουμε τα βασικότερα χαρακτηριστικά του :

1. Το διαδικτυακό έγκλημα διαπράττεται σε χρόνο ελάχιστων δευτερολέπτων. Η αμεσότητα αυτή έχει αποτέλεσμα τέτοια ταχύτητα τέλεσης που πολλές φορές δεν γίνεται αντιληπτό ούτε το ίδιο το θύμα. Ο δράστης, κάνοντας χρήση του Η/Υ που είναι συνδεδεμένος στο διαδίκτυο, επιτίθεται και μπορεί να εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του πλανήτη. Επομένως γίνεται εύκολα αντιληπτό, ότι δεν απαιτείται η φυσική παρουσία του δράστη στον τόπο τέλεσης του εγκλήματος, καθώς με το πάτημα ορισμένων πλήκτρων του υπολογιστή του δύναται να τελέσει το έγκλημα ακόμα και από το σπίτι ή το γραφείο του.

2. Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα. Βλάβες, φθορές καθώς και αλλοιώσεις που προκαλούνται σε ενσώματα αντικείμενα όπως σκληρούς δίσκους, μνήμες κλπ, είναι απλά δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά τα δεδομένα.

3. Η εισβολή σε ένα υπολογιστικό σύστημα διευκολύνεται από το ίδιο το διαδίκτυο και αυτό γιατί διατίθεται σε αυτό ελεύθερα εφαρμογές λογισμικού με τις οποίες οι χάκερς μπορούν να εισβάλλουν εύκολα σε δίκτυα και υπολογιστικά συστήματα και να πραγματοποιήσουν πλήθος ηλεκτρονικών επιθέσεων.

4. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (του κράτους στο οποίο γίνεται αντιληπτή η διάπραξη του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Αυτός ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος οδηγεί σε πολλές περιπτώσεις σε διαφορετική

αξιολόγηση του περιεχομένου, αφού αυτό μπορεί να είναι νόμιμο στο κράτος που βρίσκεται ο δράστης ή που υπάρχουν αποθηκευμένα τα δεδομένα και να είναι παράνομο στο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους.

5. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής τεχνολογίας και διαδικτύου καθώς και συνεχή εκπαίδευση όσων είναι αρμόδιοι για τη δίωξή του (αστυνομικές και δικαστικές αρχές).

6. Το ηλεκτρονικό έγκλημα έχει εισάγει νέους περιορισμούς: α) πολλές φορές είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου ηλεκτρονικού υπολογιστή ο εγκληματίας μμπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου και β) ο ακριβής χρόνος τέλεσης του εγκλήματος και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημιά που προκλήθηκαν πολύ αργότερα από το χρόνο που πραγματοποιηθήκαν.

7. Τα στατιστικά στοιχεία που υπάρχουν τόσο στον διεθνή όσο και στον ελληνικό χώρο δεν είναι επαρκή. Τα εγκλήματα στον κυβερνοχώρο που καταγγέλλονται είναι σχετικά λίγα και αυτό γιατί το θύμα ακόμα και όταν αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, δεν καταφεύγει στις αρμόδιες διωκτικές αρχές. Ένας από τους πιο σπουδαίους λόγους για τον δισταγμό αναφοράς του εγκλήματος, είναι ο φόβος της εταιρίας που δέχτηκε την επίθεση ότι η αποκάλυψη του γεγονότος θα επέφερε αρνητικές συνέπειες κυρίως όσο αφορά το κύρος, την αξιοπιστία και την εικόνα προς τους πελάτες της.

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Σε αυτό κεφάλαιο προχωρούμε σε μια εκτενέστερη ανάλυση των διαφόρων μορφών του ηλεκτρονικού εγκλήματος, τις οποίες έχουμε εντάξει σε δύο κατηγορίες. Στην πρώτη εντάσσονται τα λεγόμενα «γνήσια» ηλεκτρονικά εγκλήματα, των οποίων η εμφάνιση συμπίπτει με αυτήν των Η/Υ και του διαδικτύου και στη δεύτερη τα παραδοσιακά ή αλλιώς συμβατικά εγκλήματα που προϋπαρχαν των Η/Υ και του διαδικτύου όμως τα τελευταία συνέβαλαν σε μεγάλο βαθμό στους διαφορετικούς, ευκολότερους τρόπους εκτέλεσης τους.

2.1. Γνήσια Ηλεκτρονικά Εγκλήματα.

Τα κυριότερα και πιο διαδεδομένα εγκλήματα που περιλαμβάνονται σε αυτήν την κατηγορία είναι :

• Κακόβουλες εισβολές σε δίκτυα (hacking, cracking)
• Ανεπιθύμητη αλληλογραφία (spamming)
• Ηλεκτρονικό «Ψάρεμα» (phising - pharming)
• Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)
• Πειρατεία ονομάτων χώρου (domain names piracy)
• Απάτη με τη Νιγηριανή Επιστολή (Nigerian scam)
• Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

2.1.1. Κακόβουλες εισβολές σε δίκτυα.

α. Hacking .

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας

καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Η έννοια του hacking είναι ευρεία. Μπορεί να αφορά από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και εγκληματικές. Η εισβολή στο δίκτυο ακόμα και αν δεν είναι κακόβουλη, θα λέγαμε ότι ενέχει κακόβουλο χαρακτήρα. Αυτό γιατί ο επιτιθέμενος ή αλλιώς hacker, εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του, εντοπίζει πιθανά αδύνατα σημεία του και έτσι μπορεί στη συνέχεια αν θέλει να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Η δράση των hackers δεν είναι πάντα καταστροφική και συνδεδεμένη με εγκληματικές πράξεις βανδαλισμού, αλλά μια πτυχή των παραβιάσεων σχετίζεται με την ανάγκη επίδειξης των τεχνικών δυνατοτήτων τους. [12]

Όπως σε μια πραγματική μάχη, έτσι και στο ιντερνέτ το βασικότερο πράγμα πριν από μια επίθεση είναι η συλλογή πληροφοριών για τον αντίπαλο.

Συνοπτικά ως χάκερ (hacker) μπορεί να ορισθεί το άτομο εκείνο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών Γενικά υπάρχουν τρεις (3) κατηγορίες hacker:

1. White hat-hackers: Στόχος τους είναι να καταπολεμούν το ηλεκτρονικό έγκλημα και τους black hat – hackers . Οι grey hats τους ταυτίζουν με τους ειδικούς ασφαλείας και διαχειριστές συστημάτων. Οι ηλικία τους κυμαίνεται από 25 έως και 40 έτη, Μερικές φορές οι grey hats μετατρέπονται σε white hats όταν μεγαλώσουν.

2 Black hat- hackers: Είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν , σπάνε κωδικούς

[12] www.go-online.gr/e-business/specials/article/html?article_id_370, πρόσβαση στις 12/10/2012

από ιστοσελίδες και τις καταστρέφουν. Το κίνητρο τους είναι χρηματικό τις περισσοτέρες φορές και όχι ιδεολογικό.

3. Grey hat-Hackers Εδώ μπαίνουμε στην γκρίζα ζώνη του ιντερνετ. Σε αυτή την κατηγορία ανήκουν χάκερ που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφαλείας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους. Αυτοί οι χάκερ είναι επί το πλείστο μικρής ηλικίας, ξεκινούν σε ηλικία 15 χρονών και φτάνουν στο αποκορύφωμα των γνώσεων τους ως φοιτητές. Οι ίδιοι δεν θεωρούν τον εαυτό τους εγκληματία ακόμα και αν παραβιάζουν νόμους γιατί δεν καταστρέφουν ούτε δημιουργούν ζημία στα συστήματα που εισβάλουν. Θεωρούν τον εαυτό τους ερευνητές της τεχνολογίας και σε κάποιες περιπτώσεις ενημέρωνουν ακόμα και το κοινό ή τους διαχειριστές συστημάτων για τυχόν προβλήματα ασφάλειας.[13]

β) Cracking.

Το Cracking αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. **Βασικός σκοπός** είναι η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς .[14]

2.1.2. Ανεπιθύμητη αλληλογραφία (spamming).[15]

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει. Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη»

[13] www.it.security.gr/ hacker.html πρόσβαση στις 12/10/2012
[14] www.it.security.gr/ cracking.html πρόσβαση στις 12/10/2012
[15] . www.sch.gr/ sch_portlets/static/manualabout spam/index.php?listavoid πρόσβαση την 12/10/2012

καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας .[16]

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming :

• **Απρόκλητο**: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.

• **Εμπορικό:** Το spamming αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.

• **Μαζικό**: Το spamming συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

Για να προστατευτεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, και αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Κρίνεται σκόπιμο κάθε χρήστης να εγκαταστήσει στον Η/Υ ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων όπως επίσης να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει.

Για να προστατευτεί ο χρήστης :

-Μην δημοσεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου.

-Μη δίνεται την διεύθυνση ηλεκτρονικού ταχυδρομείου σε οργανισμούς που δεν εμπιστεύεστε.

-Μην απαντάται στα spam.

-Αναφέρατε κάθε μήνυμα spam που δέχεστε.

-Διαδώστε τη γνώση σας και την εμπειρία σας σχετικά με τα spam.

2.1.3. Ηλεκτρονικό «Ψάρεμα» (phising - pharming).

α) Phishing [17]

[16] Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθάνα 2001, σελ.169.

[17] www. computer.howstuffworks.com/ phishing.html πρόσβαση την 12/10/2012 και Χρ,. Τσουραμάνης «Ψηφιακή Εγκληματικότητα , εκδόσεις Βας. Ν. Κατσαρού, Αθήνα 2005, σελ 23-24

Στην περίπτωση αυτή ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η.Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το email αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα

Vishing

Vishing είναι η προσαρμογή του ηλεκτρονικού ψαρέματος (phishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το VoIP (Voice over IP tools). Ο χρήστης λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία.

β) Pharming [18]

Pharming είναι η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται

[18] www.pharming-fishing.gr πρόσβαση την 12/10/2012

στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν. Κατόπιν τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα.

2.1.4. Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) καθώς και οι δούρειοι ίπποι (Trojan horses).

α) Ιοί (Viruses) [19]

Ο ιός [20] είναι ένα πρόγραμμα Η/Υ που έχει σχεδιαστεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δε έχει την δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από ένα σύστημα σε άλλο , με σκοπό να εκτελέσει την αποστολή του η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων , την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων. Ουσιαστικά είναι ένας βλαβερός εκτελέσιμος κώδικας , ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Έχουν παρασιτική συμπεριφορά, καθώς επιζούν με το να «μμολύνουν» άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη συμπεριφορά (ο τρόπος που ζουν και πολλαπλασιάζονται) των οργανικών ιών. Σήμερα ο συνηθέστερος τρόπος μμετάδοσης των ιών είναι η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

[19] www. it security.gr πρόσβαση 12/10/2012
[20] Γρ. Λάζος «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη 2001

Ξεκίνησαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. ή εταιριών προϊόντων υψηλής τεχνολογίας όπως XEROX, BELL κλπ.

Σύμφωνα με τον **Kyas** (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό[21]:

1. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).

2. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).

3. Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).

4. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων Anti-Virus (Polymorphous Viruses).

5. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).

6. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).

7. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

β) Δούρειοι ίπποι (Trojan Horses).

Ένας **δούρειος ίππος** αποτελείται από δύο (2) μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον

[21] Χρ. ΤΣΟΥΡΑΜΑΝΗΣ, Ψηφιακή Εγκληματικότητα, εκδόσεις Β.Ν.Κατσαρού Αθήνα 2005, σελ. 20-21

υπολογιστή του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall).[22]
Είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. 'Ετσι ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού , αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου.

Στις περισσότερες των περιπτώσεων, ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης[23].

γ) Σκουλήκια (worms).

Τα σκουλήκια είναι και αυτά προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για τον λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλαδη έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους από τους ιούς αναφέρεται ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους. [24]

δ) Άλλα είδη κακόβουλου λογισμικού.

δ.1. Dialers[25] .

Οι dialers είναι μια υποκατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες

[22] Γρ. Λάζος «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη 2001, σελ
[23] www.itsecurity.gr προσβαση 12/10/2012
[24] Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθάνα 2001, σελ.116
[25] www.itsecurity.gr προσβαση 12/10/2012

(κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, στοιχεία λογαριασμών κλπ) για τον χρήστη, χωρίς τη γνώση και έγκρισή του. Σκοπός των δημιουργών προγραμμάτων spyware είναι η προσκόμιση πολλών χρημάτων εύκολα και γρήγορα. Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (dial up networking) ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου.

δ.2 . Λογική βόμβα. [26]

Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή τροποποιούν κάποιον υπάρχοντα κώδικα. Ονομάζονται έτσι λόγω του γεγονότος ότι είναι προγραμματισμένες να «εκραγούν» ηλεκτρονικά κάτω από ορισμένες προϋποθέσεις. Η λογική βόμβα προστίθεται στο πρόγραμμα από χρήστη ο οποίος έχει πρόσβαση στο σύστημα και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους γιατί κατασκευάζονται ευκολότερα και έχουν δυνατότητα να προκαλέσουν σοβαρές ζημιές ακόμα και καταστροφές σε σωσμένα αρχεία αλλά και σε ολόκληρο το λογισμικό ενός ηλεκτρονικού υπολογιστή.

δ.3. Rootkits. [27]

Τα rootkits είναι ένα σύνολο εργαλείων και υπηρεσιών που ο χάκερ μπορεί να χρησιμοποιήσει για να διατηρήσει την πρόσβαση του στο σύστημα που έχει χακάρει από τη στιγμή που θα εισβάλει σε αυτό. Τα εργαλεία του rootkit θα του επιτρέψουν να αναζητήσει ονόματα χρηστών και κωδικούς πρόσβασης, να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να αποκρύψει τις δράσεις του με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος.

[26] www.netsecurity.about.com προσβαση 12/10/2012
[27] www.netsecurity.about.com/cs./grnrralsecurity/gdef_rootlit.htm προσβαση 12/10/2012

Μια και με το rootkit αποκτά πρόσβαση, μπορεί να κάνει σχεδόν ότι θέλει, έχοντας δικαιώματα διαχειριστή, παραδείγματος χάριν, να ελέγξει την κίνηση, την πληκτρολόγηση, να επιτίθεται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσει κερκόπορτες συστήματος για την εξυπηρέτηση των εισβολέων.

δ. 4. Ransomware. [28]

Είναι μια κατηγορία κακόβουλου λογισμικού, το οποίο από απόσταση κρυπτογραφεί δεδομένα του χρηστή και για να τα αποκρυπτογραφήσει απαιτεί «λύτρα».

δ.5. Bots – zombies. [29]

Μία «bot» είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο πάνω στον «πληγέντα» υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί με bot γενικά αναφέροντα ως ζόμπι. Υπάρχουν κυριολεκτικά χιλιάδες υπολογιστές στο Ιντερνετ που έχουν μολυνθεί με κάποιο είδος bot και δεν το συνειδοτοποιούν ακόμα. Συχνά ο ιδιοκτήτης δεν γνωρίζει ότι έχει εξαπολύσει έναν ιό ή εγκαταστήσει έναν δούρειο ίππο ο οποίος ενεργοποιεί τον υπολογιστή να λειτουργήσει σαν ένα Zombie. Ο εισβολέας μπορεί να χρησιμοποιήσει το μολυσμένο υπολογιστή για να επιτεθεί ή να στείλει spam σε άλλους υπολογιστές χωρίς να το ξέρουν οι ιδιοκτήτες τους.

δ.6. Scareware. [30]

Το scareware είναι προγράμματα εξαπάτησης. Γνωστά και ως fraudware, τα οποία τις περισσότερες φορές εμφανίζονται με τη μορφή pop-up παραθύρων, με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. προειδοποιώντας τους ότι ο υπολογιστής τους έχει μολυνθεί με κακόβουλο λογισμικό) και να τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου

[28] www.netsecurity.about.com/cs./grnrralsecurity/ ransomware.htm προσβαση 12/10/2012
[29] www. netsecurity.about.com /frequency asked questions/gt/pr_bot.htm προσβαση την 12/10/2012
[30] www. threatpost.com.enus/slideshow/sevenstepsto recovering from Scareware.htm πρόσβαση την 12-10-2012

λογισμικού που υποτίθεται πως θα τους προστατέψει από επιθέσεις και απειλές.

δ.7.Βακτήρια (bacteria). [31]

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα πολυπρογραμματιζόμενο σύστημα ή πιθανόν να δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

2.1.5. Πειρατεία ονομάτων χώρου (domain names piracy).[32]

α) Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο διαδίκτυο αποτελεί το «domain name» (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το «domain name» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα «domain names» και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο). Το δεύτερο μέρος (second level domain – SLD) ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε

[31] www. e-crime.gr πρόσβαση την 12-10-2012

[32] www.greeklaw.voidpress.com/2010/01/07/κυβερνοσβετερισμός πρόσβαση την 12/10/2012 και www.en.wikipedia.org/wiki/Domain_name.gr πρόσβαση την 12/10/2012

ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατ' εξοχήν όνομα, την κατ' εξοχήν διαδικτυακή διεύθυνση. Το τρίτο μέρος αποτελεί το επονομαζόμενο top level domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέσης) ή τη γεωγραφική προέλευση, όπως «.com» για όσους ασκούν εμπορική δραστηριότητα, «.edu» για εκπαιδευτικούς οργανισμούς, «.org» για οργανισμούς, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς, «.int» για διεθνείς οργανισμούς, «.gr» για τη χώρα αρχειακής καταχωρίσεως του «domain name» του χρήστη, εν προκειμένω για την Ελλάδα (βλ. Ι. Καράκωστα, Δίκαιο & Internet, 2003, σελ. 27).

Το «domain name» δεν μπορεί κατ' αρχήν να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει, ωστόσο, να αποδίδεται σ' αυτό λειτουργία τόσο διακριτικού τίτλου όσο και σήματος, κατά έμμεσο τρόπο, όταν αυτό χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο, διότι, έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσεως οποιασδήποτε ονομασίας, όσο γνωστή και φημισμένη και αν είναι, από τον πρώτο τυχόντα, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση που καθιερώθηκε στις συναλλαγές με την επίμαχη ονομασία. Για τη διαφύλαξη έτσι των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο «domain name» μια οιονεί λειτουργία διακριτικού τίτλου και σήματος. Τούτο ενισχύεται και από το ότι οι κάτοχοι «domain names» στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους κατέστησαν γνωστούς στον υλικό κόσμο, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, δεδομένων μάλιστα των περιορισμένων ορίων παροχής «domain names» για κάθε χρήση αλλά και της επιβαλλόμενης συντομίας γι' αυτού του είδους την επικοινωνία.

β) Έννομη Προστασία: Δεδομένων των ανωτέρω, θα πρέπει να απολαμβάνει προστασίας αντίστοιχης με εκείνη των διακριτικών γνωρισμάτων (εφαρμοζομένων αναλόγως των σχετικών διατάξεων), αλλά και ένα διακριτικό γνώρισμα θα πρέπει να προστατεύεται (εφόσον βεβαίως πληρούνται προϋποθέσεις προστασίας του) από τη χρήση ενός ονόματος διαδικτύου,

παρά το γεγονός ότι προηγήθηκε χρονικά η καταχώριση αυτού στο διαδίκτυο, λαμβανομένων όμως υπόψη, υπό τα εκάστοτε κρίσιμα πραγματικά περιστατικά, των ιδιαιτεροτήτων του διαδικτύου, και συγκεκριμένα της παγκοσμιότητας του διαδικτύου ως μέσου ενημέρωσης, της μοναδικότητας των ηλεκτρονικών διευθύνσεων, της πεπερασμένης δυνατότητας συνδυασμών διευθύνσεων, του ιδιόρρυθμου συστήματος καταχωρίσεως των ονομασιών, κατά το οποίο η εξυπηρέτηση των αιτήσεων γίνεται κατά τη σειρά άφιξής τους χωρίς διενέργεια προληπτικού ελέγχου, αρκεί να μην έχει χορηγηθεί το συγκεκριμένο όνομα σε άλλον αιτούντα (First Come First Served) (βλ. Άνθιμο, Εισαγωγή στην προβληματική του domain name, ΔΕΕ 1999,815 επ., ιδίου, Η διασφάλιση των διακριτικών γνωρισμάτων στο Διαδίκτυο, Ο κίνδυνος από τα domain names, ΕπισκΕΔ 2000,588, Μαρίνο, παρατηρήσεις υπό ΜΠρΣυρ 637/1999 ΕΕμπΔ 2000,146 επ., Ιγγλεζάκη, παρατηρήσεις υπό ΜΠρΑθ 9485/2000 ΕπισκΕΔ 2000,1109 επ.).

Η καταχώριση γνωστού ξένου διακριτικού γνωρίσματος ως «domain name» ενδέχεται να συνιστά και αθέμιτο παρεμποδιστικό ανταγωνισμό (άρθρο 1 Ν 146/1914), ενώ δεν αποκλείεται ότι μπορεί να συντρέχουν και οι προϋποθέσεις εφαρμογής του άρθρου 13 Ν 146/1914 , όταν το διακριτικό γνώρισμα χρησιμοποιείται στο διαδίκτυο.

Δημοσιεύθηκε η ΕφΠειρ 608/2009, που έκρινε μη νόμιμη την κατοχύρωση και χρήση του domain name “chattours.gr” από εταιρία που δραστηριοποιείται στον τομέα των υπηρεσιών τουρισμού, λόγω της προσβολής δικαιώματος της εταιρίας CHAT-TOURS ΕΠΕ, η οποία είχε προηγουμένως κατοχυρώσει το domain name “chatours.gr” (με ένα ‘t’), επεδίκασε δε συναφώς αποζημίωση.

2.1.6. Απάτη με τη Νιγηριανή Επιστολή. [33]

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως

[33] Τσουραμάνης Χρ., «Ψηφιακή Εγκληματικότητα», εκδόσεις Β. Ν. Κατσαρού, Αθήνα 2005, σελ. 22,23

κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

2.1.7 Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστή ιστοσελίδας(web server) ή ενος διακομιστή ρχείων(file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες

σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιότητατων δεδομένων και τη γενικότερη λειτουργία του συστήματος. Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

• Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο.

• Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.

• Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

2.2. Παραδοσιακά (συμβατικά) εγκλήματα που τελούνται και χωρίς τη χρήση Η/Υ ή και του Διαδικτύου

Στην κατηγορία αυτή εντάσσονται εγκλήματα που προϋπήρχαν της πληροφορικής τεχνολογίας δηλαδή εγκλήματα του κοινού Ποινικού Κώδικα τα οποία τελούνται και χωρίς τη χρήση Η/Υ και Διαδικτύου. Η τεχνολογία έχει δώσει δυνατότητες για νέους και πιο πρόσφορους τρόπους τέλεσης τους.

Τα κυριότερα εγκλήματα αυτής της κατηγορίας είναι τα εξής:

• Ξέπλυμα χρήματος .

• Πειρατεία Λογισμικού.

• Παιδική Πορνογραφία .

• Διαδικτυακή Τρομοκρατία .

2.2.1 Ξέπλυμα χρήματος

Ο όρος «ξέπλυμα χρήματος» χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μία σειρά διαδικασιών οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα).[34]

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια[35]:

1. **Τοποθέτηση** : Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο γενικότερο οικονομικό σύστημα, σε παραδοσιακό ή μη χρηματοοικονομικό οργανισμό, όπως τράπεζα με

[34] Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2001, σελ. 132

[35] Γ.Χλούπη, Νομιμοποίηση εσόδων από παράνομες δραστηριότητες: περιγραφή του φαινομένου και τρόποι αντιμετώπισης, Ποιν.Δικ. 2000/369 επ

κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις.

2. **Στρωματοποίηση**: Ο δράστης επιχειρεί σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι να μεταμφιέσει τις αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεγκτικά όργανα του φορέα στον οποίο επενδύθηκαν τελικά.

3. **Ενσωμάτωση** : Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας όπως για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ, έτσι ώστε τα εν λόγω κεφάλαια να επιστρέφουν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια.

Έτσι λοιπόν, βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεται με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή προσφέρει, με σύγχρονους τρόπους και μεθόδους πάντα όμως με τον ίδιο επιδιωκόμενο σκοπό.

Το βασικό πλεονέκτημα του ξεπλύματος χρήματος μέσω ιντερνέτ είναι ότι δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων μερών με άμεσο επακόλουθο, οι δράστες να νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους να νομιμοποιούν έσοδα παράνομων δραστηριοτήτων.

2.2.2.Πειρατεία λογισμικού

Ο όρος **πειρατεία λογισμικού** αναφέρεται στην αναπαραγωγή ή/και διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους[36].

α Μορφές πειρατείας λογισμικού

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:

1. Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της αδείας χρήσης: Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης

[36] Βλαχόπουλος Κωνσταντίνος, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2007, σελ. 61

εφόσον απαιτείται ξεχωριστή άδεια για κάθε υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα.
εκδηλώνεται δε ως εξής:
α. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.
β. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρεία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών υπολογιστών (η άδεια χρήσης παραδίδεται μαζί με το λογισμικό καθώς ορίζεται πως αφορούν σε ένα και μοναδικό εμπόρευμα).
γ. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών .
δ. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους. Συχνά οι πωλητές υπολογιστών προκειμένου να κάνουν την αγορά ενός υπολογιστή πιο ελκυστική προσφέρουν προγράμματα χωρίς τις άδειες. Έτσι χρειάζεται μεγάλη προσοχή και έλεγχος των αδειών κατά την αγορά υπολογιστή που διαθέτει προεγκατεστημένα προγράμματα. Το λογισμικό αυτό δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για προγράμματα.

2) Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος: Η παράνομη αναπαραγωγή και πώληση λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης πλαστών προϊόντων. Η όλο και περισσότερο εξελιγμένη τεχνολογία που χρησιμοποιούν οι πλαστογράφοι, καθιστούν ακόμα και τους πιο απαιτητικούς καταναλωτές συχνά ανήμπορους να διακρίνουν το νόμιμο λογισμικό από το πλαστό. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν.

2.2.3. Παιδική πορνογραφία .

Τι είναι όμως παιδική πορνογραφία; Σύμφωνα με το «Προαιρετικό Πρωτόκολλο της Σύμβασης για τα δικαιώματα του Παιδιού για την εμπορία

παιδιών, την παιδική πορνεία και την παιδική πορνογραφία» και συγκεκριμένα στο άρθρο 2, «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».

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Οι εγκληματίες διακίνησης πορνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα εκμεταλλευόμενοι την παιδική αθωότητα.[37]

Με τη χρήση του διαδικτύου:

• Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του.

• Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος.

• Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων.

• Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη «επιχειρηματική» δραστηριότητα. Αποτελεί προϊόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά.

Οι επιπτώσεις εις βάρος των ανηλίκων, μπορούν να ειδωθούν από πολλές οπτικές γωνίες. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων,

[37] A textbook of cybercrimes and penalties, σελ 8-16

αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε «μέσα» ικανοποίησης των σεξουαλικών τους ορέξεων. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους, που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική τους ωρίμανση. Ο ανήλικος από την πλευρά του, είναι ικανότατος χρήστης των υπολογιστών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου του χαρακτήρα του, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε δια μέσου του ιστού.

2.2.3.α. Τρόποι εγκληματικής δράσης.

Με βάση το άρθρο 348Α του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι:

1. Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη, μοντάζ, επεξεργασία εικόνων κλπ).
2. Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού.
3. Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη).
4. Μεταφορά πορνογραφικού υλικού.
5. Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση)[38].

Έχουμε λοιπόν δύο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο: από τη μία τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

2.2.4. Διαδικτυακή τρομοκρατία [39]

[38] Ε.Συμεωνίδου-Καστανίδου, «Εγκλήματα κατά προσωπικών αγαθών», Νομική Βιβλιοθήκη, 2006, σελ. 249, 250

[39] www.fbi.gov πρόσβαση 12/10/2012

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες».

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρόντας την ανωνυμία του. Με τη χρήση λοιπόν του Διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.

Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή του καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία.

ΚΕΦΑΛΑΙΟ 3^0

ΝΟΜΟΘΕΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Τόσο στην Ελλάδα όσο και σε άλλες χώρες, οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες. Ο νομοθέτης είναι αναγκασμένος να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθεί με τον τρόπο διάπραξης των σχετικών αξιόποινων πράξεων. Η ψηφιακή εγκληματικότητα αποτελεί δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά.

Οι διώξεις των ψηφιακών εγκλημάτων εφόσον και οι καταγγελίες είναι περιορισμένες. κινούνται σε χαμηλά επίπεδα. Θα πρέπει να παρατηρήσουμε πως οι επιχειρήσεις – κυρίως - αποφεύγουν να καταγγείλουν παραβάσεις, γιατί φοβούνται επανάληψη των αδικημάτων και πλήγμα στη φήμη τους. Επίσης, θέλουν να αποφεύγουν τα υψηλά δικαστικά έξοδα. Οι αστυνομικές και οι δικαστικές αρχές αντιμετωπίζουν δυσκολίες στον εντοπισμό και την περαιτέρω δίωξη, γεγονός που σχετίζεται, κυρίως, με το χαμηλό επίπεδο πληροφορικής κατάρτισης των στελεχών τους.

Ο διεθνής χαρακτήρας των συγκεκριμένων εγκλημάτων δίνει τη δυνατότητα στους δράστες να έχουν γρήγορη πρόσβαση και προσβολή των δεδομένων στα συστήματα Η/Υ παγκοσμίως. Τα ψηφιακά εγκλήματα διακρίνονται και για: το μεγάλο όγκο των δεδομένων τους, τον μη οπτικό χαρακτήρα των αποδείξεων, τη δυνατότητα «μεταμφίεσης» τους καθώς και την ταχεία εξαφάνιση των αποδεικτικών στοιχείων από τη μεριά των εγκληματιών.

Επίσης απαιτείται συνήθως αρκετός χρόνος, για να διευκρινιστούν οι υποθέσεις, που είναι συνήθως πολύπλοκες και απαιτούν συνεργασία και με άλλες υπηρεσίες. Πολλές φορές οι δικαστές υποβαθμίζουν τη σημασία των ψηφιακών εγκλημάτων, με τη δικαιολογία ότι το σύστημα της ποινικής

δικαιοσύνης δεν θα πρέπει να επιβαρυνθεί με τέτοιου είδους εγκληματίες, εφόσον η ποινή που τους επιβάλλεται, δεν είναι ικανή να τους αποτρέψει από την επανάληψη της πράξης.

Επιπλέον, υπάρχει το πρόβλημα της δικαιοδοσίας, αφού ο καθένας όπου και αν βρίσκεται μπορεί να έχει πρόσβαση σε οποιαδήποτε πληροφορία θελήσει. Είναι δύσκολο να ορισθεί ο τόπος τέλεσης του αδικήματος και η αρμοδιότητα του δικαστηρίου που θα πρέπει να εκδικάσει την υπόθεση.

Με δεδομένη όμως, την αύξηση των μορφών των ψηφιακών εγκλημάτων η ειδική και εξειδικευμένη νομοθετική αντιμετώπισή τους θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν όλα τα κράτη του κόσμου έχουν θεσπίσει νομοθετικές διατάξεις, σχετικές με τα ψηφιακά εγκλήματα. Ωστόσο, το νομοθετικό πλαίσιο που να αφορά ειδικότερα το ζήτημα είναι σε αρκετές περιπτώσεις εξαιρετικά ελλιπές και συνήθως καλύπτεται από γενικότερες διατάξεις.

Τα τελευταία χρόνια έχουν πραγματοποιηθεί Συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως, με σκοπό τη συζήτηση και τη λήψη αποφάσεων, σχετικά με το ζήτημα αυτό.

Συγκεκριμένα, πραγματοποιήθηκε Συνέδριο για το Ηλεκτρονικό Έγκλημα στη Βουδαπέστη και υπογράφτηκε συνθήκη, στις 23/11/2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Τη Συνθήκη υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές των ψηφιακών εγκλημάτων και είναι γνωστή ως “Convention on Cyber Crime 2001”.

Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα: Με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα 370Β, 370Γ και 386Α.

3.1 Το πρόβλημα της δικαιοδοσίας στο διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο διαδίκτυο είναι πολύπλοκο εξαιτίας της παγκοσμιότητας του. **Δικαιοδοσία**: είναι η αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά

συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά.

Η ανεύρεση της αρμοδιότητας του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες:

1. **Η θεωρία του τόπου του αποτελέσματος**. Τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

2. Η **θεωρία του τόπου ενέργειας**. Ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου έχει τελεστεί η ενέργεια που έτεινε στο άδικο αποτέλεσμα. Εφόσον η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος ενέργειας είναι αυτός όπου ολοκληρώθηκε η ενέργεια.

3. **Η μικτή θεωρία**. Τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

4. **Η θεωρία του βαρύνοντος τόπου**. Σύμφωνα με την αυτήν την θεωρία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Όμως υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας καθώς 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**.

3.2 Νομική προσέγγιση του Διαδικτύου.

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου (Ζάννη,2005).

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

• Είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του.

• Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.

• Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της.

• Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

• **Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα**:

• Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις.

• Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.

• Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας.

• Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.

Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες (Καρακώστας, 2003). Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δύο Οδηγίες την 90/38794 και την 90/388,95 κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιονδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

Η προσαρμογή της ελληνικής νομοθεσίας προς τις παραπάνω οδηγίες της Ευρωπαϊκής Κοινότητας, προήλθε, κατ' αρχήν, με τον Ν. 2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Ν. 2246/94 και στη συνέχεια με τον Ν. 2867/2000, που ως σήμερα είναι σε ισχύ. Με τον νόμο αυτό, ιδρύθηκε ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους. (Βλαχόπουλος, 2007)

3.3 Ελληνική Νομοθεσία.

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί έναν συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών.

Στο Σύνταγμα της Ελλάδος, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας». Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

Στον Ποινικό Κώδικα, η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α,370Β και 370Γ. Τα άρθρα 370 και 370Α αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας, αντίστοιχα. Η ανάλογη εφαρμογή των διατάξεων αυτών στο χώρο του Διαδικτύου, έχει προκαλέσει έντονο προβληματισμό στους νομικούς κύκλους, ιδιαίτερα όσον αφορά το άρθρο 370Α, το οποίο κατά πολλούς, θεωρείται ότι δεν μπορεί να τύχει εφαρμογής στο Διαδίκτυο, αν και η σύνδεση γίνεται μέσω μισθωμένης τηλεφωνικής γραμμής (Καράκωστας, 2001). Το άρθρο 370Β, παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα. Η πιο ουσιαστική διάταξη, όσον αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς άδεια πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ. Το απόρρητο στην περίπτωση αυτή προστατεύεται υπό μία ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται το δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την

πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον υπολογιστή του.

Τα παραπάνω άρθρα του Ποινικού Κώδικα δεν είναι αρκετά για να καλύψουν τις ανάγκες δίωξης της ηλεκτρονικής εγκληματικότητας, η οποία παράλληλα πάντα με τις τεχνολογικές εξελίξεις εμφανίζεται με νέες μορφές. Άλλωστε στα συγκεκριμένα άρθρα δεν έχει προβλεφθεί η ύπαρξη του διαδικτύου το οποίο πλέον δίνει νέες διαστάσεις στο ζήτημα. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν με βάση την ισχύουσα στην Ελλάδα νομοθεσία. Αυτό το κενό βέβαια αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, εφόσον ο εικονικός κόσμος του διαδικτύου θεωρηθεί απλά ως ένα ακόμα μέσο για τη διάπραξη εγκλημάτων.

Ακόμα, διατάξεις που σχετίζονται με το ηλεκτρονικό έγκλημα περιλαμβάνονται στο Π.Δ. 131/2003 που αναφέρεται στην ανεπιθύμητη αλληλογραφία (spamming) και στην ευθύνη των παρόχων υπηρεσιών διαδικτύου για πράξεις των χρηστών που είναι συνδρομητές τους. Το συγκεκριμένο Π.Δ. θεσπίστηκε σε εφαρμογή της κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο. Επίσης ο Ν.2867/2000 για την «οργάνωση και λειτουργία του τομέα των Τηλεπικοινωνιών», οι Ν.2774/1999 και Ν.2472/1997 «περί προσωπικών δεδομένων» και ο Ν.2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» σχετίζονται με κάποιες πτυχές του ηλεκτρονικού εγκλήματος..

3.4 Η Σύμβαση για τον κυβερνοχώρο

Η Διεθνής Σύμβαση για τον κυβερνοχώρο, με αντικείμενο την καταπολέμηση της εγκληματικής δραστηριότητας στους κόλπους του διαδικτύου, καταρτίστηκε στις 23/11/2001 στη Βουδαπέστη. Ήδη οι εργασίες για τη δημιουργία αυτής της σύμβασης ξεκίνησαν τον Απρίλιο του 1997, με τη σύσταση μιας επιτροπής ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με αρχικό χρονοδιάγραμμα περάτωσης τα τέλη του 1999. Λόγω όμως των ιδιαίτερων προβλημάτων που προέκυψαν (ταχύτατη εξέλιξη της τεχνολογίας),οι εργασίες της σύμβασης παρατάθηκαν έως το τέλος του 2000 και τελικά ολοκληρώθηκε ακόμα πιο μετά (Νοέμβριος 2001).

Η Σύμβαση έως σήμερα έχει υπογραφεί από τα περισσότερα μέλη του Ευρωπαικού Συμβουλίου, καθώς και από τις Η.Π.Α., τον Καναδά, την Ιαπωνία και τη Νότια Αφρική.

Ο βασικότερος σκοπός της «Σύμβασης για το Έγκλημα στον κυβερνοχώρο» είναι η εναρμόνιση των εθνικών νομοθεσιών των κρατών-μελών που έχουν υπογράψει, στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Επίσης, με τη σύμβαση παρέχεται το νομοθετικό πλαίσιο του δικονομικού δικαίου που είναι απαραίτητο για τη διερεύνηση και τη δίωξη των εγκλημάτων του κυβερνοχώρου. Με τη σύμβαση αυτή θέτονται οι βάσεις για μια αποτελεσματική συνεργασία για το ηλεκτρονικό έγκλημα.

ΚΕΦΑΛΑΙΟ 4^{0}

ΔΡΑΣΤΗΣ ΤΕΛΕΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΕΡΕΥΝΗΤΗΣ ΑΥΤΟΥ

Στο τέταρτο κεφάλαιο θα προσπαθήσουμε να σκιαγραφήσουμε το προφίλ του cybercriminal[40] επιλέγοντας κάποια γενικά χαρακτηριστικά, τα οποία με μεγάλη πιθανότητα συναντιόνται στην προσωπικότητα του, καθώς και τα χαρακτηριστικά που πρέπει να συγκεντρώνει ένας καλός ερευνητής , ο οποίος χειρίζεται την διελεύκανση μιας υπόθεσης που αφορά την τέλεση ηλεκτρονικού εγκλήματος.

4.1. Τα χαρακτηριστικά ενός cybercriminal[41].

Στην μεγάλη πλειοψηφία τους οι εγκληματίες αυτής κατηγορίας συγκεντρώνουν κάποια από τα ακόλουθα χαρακτηριστικά:

Ένα ελάχιστο επίπεδο γνώσης σε τεχνολογικά θέματα: Το χαρακτηριστικό αυτό βασίζεται στην κοινή λογική. Οι άνθρωποι γενικά χρησιμοποιούν εργαλεία με τα οποία αισθάνονται άνετα, πολύ περισσότερο όταν το εγχείρημα τους εμπεριέχει μια δόση κινδύνου, όπως είναι η τέλεση εγκλήματος. Ο τυπικός «κυβερνοεγκληματίας» δεν είναι «κομπιουτεροφοβικός» ή κάποιος που συνδέθηκε στο Ιντερνετ για πρώτη φορά.

Δυσαρέσκεια ως προς τον Νόμο ή θεωρούν τον εαυτό τους πάνω από τον νόμο : Πολλοί διαπράττοντας μία πράξη ενάντια στον νόμο, θεωρούν ότι ο νόμος είναι κακός και όχι αυτοί που τον παραβαίνουν. Με αυτό τον τρόπο δείχνουν την δυσαρέσκεια τους.

Χώρος μιας φανταστικής ζωής: Πολύ χρησιμοποιούν τον κυβερνοχώρο σαν μία διέξοδο από την καθημερινότητα τους. Με τον τρόπο αυτό και το πέπλο τις ανωνυμίας υποδύονται διαφορετικές προσωπικότητες καλύπτοντας τις ατέλειες τους και ικανοποιώντας τις φαντασιώσεις τους.

[40] Με τον όρο αυτό χαρακτηρίζεται ο δράστης τέλεσης ενός ηλεκτρονικού-διαδικτυακού εγκλήματος.
[41] Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 111-112

Ρίσκο / επιζητούν τον έλεγχο μιας κατάστασης: Είναι πρόκληση ότι κάνουν κάτι απαγορευμένο, του οποίου έχουν τον απόλυτο έλεγχο αφού είναι δύσκολα εντοπίσιμοι.

Ισχυρά κίνητρα –διαφορετικά .Οι περισσότεροι έχουν ένα ισχυρό κίνητρο το οποίο μπορεί να είναι η επιθυμία πλουτισμού, σεξουαλική ικανοποίηση, πολιτικά κίνητρα ή κάποια βαθύτερη αιτία που κινείται στον χώρο της ψυχικής ασθένειας. Ξεχωρίζοντας το κίνητρο είναι ένα σημαντικό κριτήριο για να κατασκευάσουμε το προφίλ του κυβερνοεγκληματία.

4.2 Αναγνωρίζοντας τα κίνητρα των «cybercriminals». [42]

Πολλοί πιστεύουν ότι η απάντηση στο ερώτημα «Τι ωθεί τους εγκληματίες στην διάπραξη αξιόποινων πράξεων» είναι «γιατί είναι εγκληματίες». Όμως η απάντηση δεν είναι τόσο απλή. Οι άνθρωποι σπάζουν τα όρια των νόμων για πολλούς και διαφορετικούς λόγους. Κάποιοι από τους λόγους αυτούς είναι εν μέρει δικαιολογήμενοι, όπως όταν η μητέρα δεν έχει χρήματα για να αγοράσει το γάλα του παιδιού της, κλέβει ένα μπουκάλι γάλα.

Γιατί έχει σημασία το κίνητρο; Σε πολλά δικονομικά συστήματα, το λεγόμενο τρίγωνο του εγκλήματος απαρτίζεται από: τον τρόπο διάπραξης , το κίνητρο (ο λόγος διάπραξης του εγκλήματος) και η δυνατότητα (να είσαι στο σωστό μέρος την κατάλληλη στιγμή για την διάπραξη του εγκλήματος). Έτσι καταλαβαίνοντας το κίνητρο, μας εξυπηρετεί στην εξιχνίαση του εγκλήματος.

Τα συνηθέστερα κίνητρα για την διάπραξη ενός cybercrime είναι:

α) Διασκέδαση

β) Χρηματικό όφελος.

γ) Θυμό, εκδίκηση και άλλου τύπου συναισθήματα.

δ) Πολιτικά κίνητρα.

ε) Σεξουαλικά κίνητρα.

στ) Σοβαρές ψυχικές ασθένειες.

Θα προσπαθήσουμε να αναλύσουμε τα κίνητρα αυτά .

---

[42] . Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 113-118

α) ΔΙΑΣΚΕΔΑΣΗ

Νεαροί hackers είναι αυτοί που εμπίπτουν σε αυτή την κατηγορία. Σύμφωνα με τον J. Maxwell in the Electronic Processing Audit, Control and Security Newsletter , οι hachers αυτής της κατηγορίας μπορούν να ταξινομηθούν σε περαιτέρω κατηγορίες:

Pioneer types: οι οποίοι μαγεύονται από την τεχνολογία. Βρίσκουν ενδιαφέρον πως λειτουργεί ένα σύστημα και προσπαθούν να «σπάσουν» τα συστήματα ασφαλείας του και έτσι το κάνουν για εμπειρία.

Scamps:οι οποίοι δεν ενδιαφέρονται να κάνουν ζημιά. Είναι τύποι που τους ενδιαφέρει να μπούν σε κάποια σελίδα και να αφήσουν ένα μήνυμα τύπου «Η Μαρία ήταν εδώ».

Explorers:οι οποίοι ικανοποιούνται «μπαίνοντας εκεί που άλλοι hackers δεν έχουν μπει»- η τουλάχιστον «μπαίνοντας εκεί που οι ίδιοι δεν έχουν ξαναμπεί». Η περιέργεια τους είναι εκείνη που ωθεί να δουν πράγματα που δεν έχουν ξαναδεί.

Game players: οι οποίοι προσπαθούν να μπούν σε ένα σύστημα βλέποντας το σαν παιχνίδι και προσπαθούν να σπάσουν τα συστήματα ασφαλείας για να κερδίσουν το παιχνίδι.

Addict: είναι οι τύποι εκείνοι οι οποίοι ξεκινώντας από μια από τις παραπάνω κατηγορίες, μετατράπηκε σε ψυχικά εξαρτώμενος από αυτές. Στην περίπτωση αυτή το έχουν ανάγκη να χακάρουν για να νοιώθουν καλά ή φυσιολογικά.

Όλοι αυτοί των ανωτέρω κατηγοριών το βλέπουν ως παιχνίδι, δεν έχουν κάποιο οικονομικό όφελος.

β) Χρηματικό όφελος.

Το χρήμα αποτελεί, όπως συχνά λέγεται, τη ρίζα του κακού, και φυσικά αυτό ισχύει και για την διάπραξη ενός ηλεκτρονικού εγκλήματος. «Hacking για χρήμα» μπορεί να καλύπτει διάφορα αδικήματα πχ ξέπλυμα χρήματος . Επίσης μπορεί κάποιος να πουλάει της υπηρεσίες του σε κάποιον άλλο για την απόκτηση χρήματος χωρίς ωστόσο αυτός να αποκομίζει ο ίδιος όφελος από την αυτή την πράξη καθ ΄αυτή. Σε αυτή την κατηγόρια ανήκουν άτομα όλων των κατηγοριών , άντρες ,γυναίκες, παιδιά.

γ) Θυμό, εκδίκηση και άλλου τύπου συναισθήματα.

Το χρήμα δεν αποτελεί το μόνο κίνητρο για την διάπραξη εγκλημάτων. Έχει παρατηρηθεί ότι ο θυμός μπορεί να οδηγήσει τον άνθρωπο σε πράξεις που υπό άλλες συνθήκες δεν θα μπορούσε να φανταστεί ότι θα τις έκανε. Ψυχολόγοι επισημαίνουν ότι η κατάσταση υπό θυμό προσομοιάζει με μια κατάσταση υπό επήρρεια αλκοόλ ή ναρκωτικών.

δ) Πολιτικά κίνητρα.

Cybercriminals υποκεινούμενοι από πολιτικά κίνητρα περιλαμβάνουν εξτρεμιστές, οι οποίοι χρησιμοποιούν το Ιντερνετ για να σπείρουν την προπαγάνδα τους, να επιτεθούν σε ιστοσελίδες και δίκτυα των πολιτικών εχθρών τους, να κλέψουν χρήματα, να βρούν χρήματα για τις μαχητικές δραστηριότητες τους ή να σχεδιάσουν και να οργανώσουν τα εγκλήματα τους στον πραγματικό κόσμο.

Παράδειγμα αποτελεί ο κυβερνοπόλεμος μεταξύ ΗΠΑ και Κίνας το καλοκαίρι του 2000 ως επακόλουθο της Αμερικάνικης Κατασκοπίας στην Κίνα.

Οι cybercriminals της κατηγορίας αυτής έχουν ένα ευρύ φάσμα ως προς την δραστηριότητα τους από το να διαδόσουν τις πολιτικές πεποιθήσεις τους ή να κάνουν γνωστή την ύπαρξη μίας πολιτικής οργάνωσης.

ε) Σεξουαλικά κίνητρα.

Το σεξ αποτελεί ένα από τα δυνατότερα ένστικτα των ζώων συμπεριλαμβανομένου και του ανθρώπου. Στην κατηγορία αυτή συμπεριλαμβάνονται οι ακόλουθοι τύποι:

«Παθητικοί παιδόφιλοι»: οι οποίοι χρησιμοποιούν το ίντερνετ για να έχουν πρόσβαση και να κατεβάζουν παιδικό πορνό, χρησιμοποιούν φωτογραφίες και ιστορίες στις οποίες συμμετέχουν παιδιά, βλέποντας τα να ικανοποιούν τις δικές τους φαντασιώσεις.

«Ενεργητικοί παιδόφιλοι»: οι οποίοι χρησιμοποιούν το Ιντερνετ για να βρίσκουν τα θύματα τους. Αυτοί συλλέγουν και υλικό στο οποίο συμμετέχουν παιδιά αλλά δεν αρκούνται σε αυτό. Συνήθως χρησιμοποιούν chat rooms με παιδιά, αρχίζουν συζήτηση αποκτούν την εμπιστοσύνη τους και στην συνέχεια τα παρασύρουν σε μια συνάντηση. Συνήθως επακολουθεί βιασμός του παιδιού .

«Οπαδοί του σαδομαζοχιστού σεξ»: οι οποίοι ικανοποιούνται προκαλώντας πόνο σε άλλους (σαδιστής) ή ικανοποιώντας πόνο στον εαυτό

τους (μαζοχιστής). Παρόλο που γενικά η συμπεριφορά αυτή μεταξύ ενηλικών δεν είναι συνιστά έγκλημα, ωστόσο η ανεύρεση παρτενερ μέσο ιντερνετ, και η πέραν από τα συμφωνηθέντα μεταξύ των δύο οδηγεί πολλές φορές στον τραυματισμό ή και στον θάνατο.

«**Κατ΄ εξακολούθηση βιαστές (serial rapist)»:** οι οποίοι αναπτύσσουν σχέση online και στην συνέχεια προσκαλούν τα θύματα τους να τους συναντήσουν στην πραγματική ζωή, με απώτερο σκοπό τον βιασμό και μόνο. Είναι άτομα τα οποία αντιμετωπίζουν προβλήματα στην σεξουαλική ζωή τους. Ικανοποιούνται μόνο όταν το σεξ είναι βίαιο . Οι ψυχολογοι αποκαλούν τον βιασμό ως πράξη βίας, και το σεξ αποτελεί απλά το εργαλείο /μέσο του εγκλήματος.

«**Κατ εξακολούθηση sexual killers»**, οι οποίοι προσομοιάζουν με τους κατ εξακολούθηση βιαστές, σερφάρουν στα chat rooms και forums αναζητώντας θύματα. Το λεξικό της ψυχιατρικής αναγνωρίζει δύο κατηγορίες: τους οργανωμένους (organized) και τους ανοργάνωτους (disorganized). Οι organized δολοφόνοι συχνά είναι άτομα με δείκτη ευφυΐας πάνω από το μέσο όρο, ευγενικοί, παντρεμένοι ή συζούν . Οι disorganized killers είναι άτομα ακριβώς το αντίθετο: το IQ τους είναι κάτω του μέσου όρου, είναι άτομα μοναχικά και έχουν πολύ άγχος κατά την διάπραξη του εγκλήματος. Στην πράξη οι sexual serial killers, παρότι το κίνητρο διάπραξης των εγκλημάτων τους είναι σεξουαλικό, ανήκουν στην κατηγορία κινήτρου: σοβαρή ψυχιατρική ασθένεια.

<u>στ) Σοβαρές ψυχικές ασθένειες.</u>

Μία εγκληματική συμπεριφορά, δεν είναι από μόνο της ενδεικτική ψυχικής ασθένειας γιατί αν ήταν πιθανόν να μπορούσε να θεραπευτεί φαρμακευτικά. ‘Ατομα τα από οποία πάσχουν από σχιζοφρένεια, διπολική συναισθηματική διαταραχή, επιθετικότητα, μελαγχολία , διαταραχές προσαρμογής και διαταραχές σεξουαλικής φύσης είναι σύμφωνα Psychiatric Illness Associated with Criminality , by William H. Wilson, MD and Kathleen A. Trott, MD.

4.3 Χαρακτηριστικά ενός ερευνητή [43]:

Ένας καλός ερευνητής (cyber-investigator) πρέπει να συγκεντρώνει όλα τα χαρακτηριστικά ενός καλός ερευνητή οποιοδήποτε εγκλήματος και συγκεκριμένα:

Παρατηρητικότητα: Στο πιο μικρό πράγμα.

Καλή μνήμη: Πρέπει να θυμάται γεγονότα, ονόματα, μέρη και ημερομηνίες διαφορετικά μπορεί να χάσει ζωτικής σημασίας πληροφορίες.

Οργανωτική Σκέψη: Δεν αρκεί να θυμάται πληροφορίες, αλλά πρέπει να οργανώνει σε μια λογική συνέχεια.

Ικανότητα καταγραφής: Πρέπει να καταγράφει με λεπτομέρεια κάθε πληροφορία και να μην την κρατάει στο μυαλό του, ετσι ώστε να μπορεί να τις μοιράζεται με όλους τους συμμετέχοντες στην έρευνα.

Αντικειμενικότητα: Δεν πρέπει να επιτρέπει προσωπικές διαφορές, σχέσεις ή συναισθήματα να εμπλέκονται στην διαδικασία της έρευνας, έτσι ώστε να διασφαλίζεται η αντικειμενικότητα του.

Γνώση: Ένας καλός ερευνητής είναι γνώστης των νόμων των κανονισμών, της θυματολογίας, της ψυχολογίας του εγκληματία, των ερευνετικών διαδικασιών και των αποδεικτικών μέσων.

Ικανότητα να σκέφτεται σαν εγκληματίας: Οι καλύτεροι των ερευνητών έχουν την ικανότητα να βάζουν τον εαυτό τους στην θέση του εγκληματία, οπότε μπορούν να καταλάβουν τον τρόπο που ένας εγκληματίας θα προστατεύσει την πράξη του.

Περιέργεια: Οι καλύτεροι των ερευνητών έχουν μία έμφυτη περιέργεια δεν αρκούνται στο γεγονός ότι διαπράχθηκε ένα έγκλημα, αλλά θέλουν να ξέρουν πως και γιατί διαπράχθηκε.

Αντοχή και Υπομονή: Πολλές φορές απαιτούνται πολλές ώρες έρευνας, οπότε θα πρέπει να έχει αντοχή ώστε να ανταπεξέλθει.

Αγάπη για γνώση:Πέρα από τα ανωτέρω χαρακτηριστικά που πρέπει να έχει και τα ειδικότερα χαρακτηριστικά που εξάρτώνται από την ίδια φύση του ηλεκτρονικού εγκλήματος.

[43] Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 113-118

Βασικές γνώσεις Η/Υ: Όσα περισσότερα γνωρίζει για το πώς δουλεύει ο Η/Υ (υλικό και λογισμικό) τόσο το καλύτερο.

Γνώση της αργκό των Η/Υ: Πρέπει να είναι σε θέση «να μιλήσει την γλώσσα αυτή».

Να μπορεί να καταλάβει την κουλτούρα των hackers: Πρέπει να είναι σε θέση να καταλάβει την κουλτούρα και τον τρόπο σκέψη ενός χακερ για να μπορέσει να τον «πιάσει».

Γνώση των κανόνων ασφαλείας των Η/Υ και του δικτύου: Για να είναι σε θέση να διελευκάνει μια υπόθεση χακινγκ ή επίθεση σε ένα δικτύου, πρέπει να είναι γνώστης των κανόνων ασφαλείας , των κανόνων ασφαλείας και των πρακτικών καθώς και των προίοντων ασφαλείας που κυκλοφορούν.

ΚΕΦΑΛΑΙΟ 5^{Ο}
ΜΕΤΡΑ ΠΡΟΛΗΨΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Σε αυτό το κεφάλαιο αναφέρονται οι βασικότερες έννοιες που αφορούν την ασφάλεια, την πρόληψη καθώς και κάποιες από τις πλέον διαδομένες τακτικές προς αποφυγή της θυματοποίησης του πολίτη με την χρήση ηλεκτρονικού υπολογιστή.

5.1. Βασικές Έννοιες της Ασφάλειας .[44]

α) Εμπιστευτικότητα.

Η εμπιστευτικότητα αναφέρεται στην προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών. Για την επίτευξη της εμπιστευτικότητας απαιτείται περιορισμός της πρόσβασης σε συστήματα και δεδομένα μόνο στους νόμιμους χρήστες.

β) Ακεραιότητα.

Η διατήρηση της ακεραιότητας συνδέεται με την προστασία των δεδομένων από τυχόν τροποποίηση (προσθήκη, διαγραφή). Η αλλοίωση της ακεραιότητας μπορεί να προκύψει εξαιτίας κάποιου λάθους στο σύστημα ή ακόμα να είναι αποτέλεσμα δόλιας ενέργειας.

γ) Διαθεσιμότητα

Η διαθεσιμότητα σχετίζεται με τη δυνατότητα άμεσης προσπέλασης των συστημάτων και των δεδομένων, όταν ή όποτε απαιτείται. Στις επιθέσεις άρνησης εξυπηρέτησης υπάρχει παραβίαση της διαθεσιμότητας, όταν δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στους πόρους του συστήματος.

5.2. Βασικά προληπτικά εργαλεία και πώς αυτά λειτουργούν.

α) Χρήση Λογισμικού Ασφαλείας -Λογισμικό Antivirus

Η διασπορά ιών είναι μια από τις πιο διαδεδομένες μορφές επίθεσης στο διαδίκτυο. Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους. Ένα τέτοιο πρόγραμμα που πρέπει να είναι

[44] Χρ. ΤΣΟΥΡΑΜΑΝΗΣ, Ψηφιακή Εγκληματικότητα, εκδόσεις Β.Ν.Κατσαρού Αθήνα 2005, σελ. 2-3-4

εγκατεστημένο σε κάθε ηλεκτρονικό υπολογιστή επιτελεί τρείς βασικές λειτουργίες. Αυτές είναι:

1. Ανίχνευση των ιών : Η λειτουργία αυτή πραγματοποιείται κατόπιν ενέργειας του χρήστη (έλεγχος του σκληρού δίσκου μέσω του antivirus λογισμικού) ή μπορεί να γίνει και αυτόματα (έλεγχος από το antivirus λογισμικό που είναι φορτωμένο στη μνήμη RAM του ηλεκτρονικού υπολογιστή).

2. Προσδιορισμός ταυτότητας ιών: Στην περίπτωση που το σύστημα έχει προσβληθεί από κάποιον ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητα του.

3. Καθαρισμός των ιών : Αφού έχει προηγηθεί ο εντοπισμός του ιού, ακολουθεί η αφαίρεσή του. Το λογισμικό antivirus επιδιορθώνει το μολυσμένο από τον ιό αρχείο ή ακόμα μπορεί και να το διαγράψει.

β) Πιστοποίηση του χρήστη. :Η πιο συνηθισμένη τεχνική πιστοποίησης της ταυτότητας ενός χρήστη είναι η δημιουργία και η χρήση συνθηματικών λέξεων ή συμβόλων. Έτσι το όνομα χρήστη (user id) και ο κωδικός πρόσβασης (password) είναι απαραίτητα στοιχεία προκειμένου να επιτραπεί η είσοδος του εξουσιοδοτημένου χρήστη στο σύστημα.

γ) Firewalls : Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπιση τους. Η σωστή πρακτική είναι το firewall να ρυθμίζεται έτσι ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και

ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

Τα Firewalls δρουν ως φράκτες ανάμεσα στο ιντερνέτ και στο εσωτερικό δίκτυο ή έναν υπολογιστή και σταματάει διάφορους κινδύνους και επιθέσεις, συμπεριλαμβανομένων και ορισμένων ιών (virus). Τα Firewalls μπορεί να είναι λογισμικό που τρέχει σε έναν υπολογιστή (πχ. το windows firewall), λογισμικό που προστατεύει το δίκτυο (πχ. Microsoft ISA Server) ή συσκευή hardware συνδεμένη στο δίκτυο. Τα firewalls φιλτράρουν την πληροφορία που εισέρχεται στο δίκτυο ή εξέρχεται από αυτό, με βάση κανόνες τους οποίους έχουμε θέσει. Με τον τρόπο αυτό προστατεύεται το δίκτυο από εισβολείς (hackers, ορισμένους ιούς κλπ). Επιπλέον, απαγορεύεται η αποστολή πληροφορίας από τους υπολογιστές του δικτύου, όπως π.χ. ποιοί τύποι αρχείων επιτρέπεται να αποστέλλονται.

Στα μειονεκτήματα των Firewalls καταλογίζονται το υψηλό οικονομικό κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και τέλος το γεγονός ότι η προστασία που παρέχουν είναι εντελώς σχετική. Είναι γνωστό για παράδειγμα πως τα modems αποτελούν ένα σημείο εισόδου στο δίκτυο το οποίο υπερφαλαγγίζει κάθε firewall.

Ένας σημαντικός τρόπος για προστασία από πολλά είδη επιθέσεων είναι η σχεδιάση της τοπολογίας του δικτύου ώστε να είναι δύσκολο να γίνει εισβολή.

Ένα firewall είναι ένα επιπλέον επίπεδο προστασίας τοποθετημένο γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Ένα firewall που προστατεύει ένα δίκτυο θα περιλαμβάνει συνήθως ένα δρομολογητή (router) που μπορεί να προγραμματιστεί ώστε να μην επιτρέπει επιλεκτικά την πρόσβαση σε ένα δίκτυο, για παράδειγμα θα απορρίπτει πακέτα που δεν στέλνονται σε συγκεκριμένες επιτρεπόμενες θύρες.

Όταν ένα πακέτο φτάνει στον δρομολογητή του firewall, αυτός το επεξεργάζεται και αποφασίσει αν θα το αφήσει να περάσει στο δίκτυο που προστατεύει ή όχι. Μια ακόμα ισχυρότερη χρήση ενός firewall είναι σε ένα σενάριο δυο επιπέδων προστασίας, όπου χρησιμοποιείται ένας δρομολογητής που παρακολουθεί την επικοινωνία με το ιντερνέτ και ένας ακόμη που παρακολουθεί την επικοινωνία στο εσωτερικό δίκτυο.

5.3 Κρυπτογραφία και Ασφάλεια[45]

Κρυπτογράφηση καλείται η διαδικασία της επεξεργασίας και κωδικοποίησης της ψηφιακής πληροφορίας κατά τέτοιο τρόπο ώστε αυτή να παραμένει αναγνώσιμη στην κατανοητή μορφή της μόνο από τους εξουσιοδοτημένους παραλήπτες που διαθέτουν το κατάλληλο «κλειδί» - κώδικα, δηλαδή η πληροφορία καθίσταται εμπιστευτική. Αρχικά η τεχνολογία της κρυπτογράφησης δημιουργήθηκε με σκοπό την προστασία του απορρήτου του μηνύματος. Στην πορεία, η εξέλιξη της κρυπτογράφησης προσφέρει στον αποστολέα του μηνύματος μεγαλύτερη ασφάλεια σχετικά με το ακέραιο αλλά και το απόρρητο του μηνύματος κατά την αποστολή του. Ένα κρυπτογραφικό σύστημα αποτελεί ένα σύνολο λειτουργιών οι οποίες είναι παραμετροποιημένες από κλειδιά και χρησιμοποιούνται για τη διατήρηση εχεμύθειας στην επικοινωνία. Με τις ενσωματωμένες λειτουργίες της ένκρυψης και της απόκρυψης, το σύστημα παρέχει ασφάλεια και προστασία στην ιδιωτικότητα, αποκλείοντας έτσι την χωρίς εξουσιοδότηση πρόσβαση σε υλικό που ορίστηκε να παραμείνει απόρρητο. Το κρυπτογραφικό περιεχόμενο δεν μπορεί να γίνει προσβάσιμο από οποιονδήποτε που θα προσπαθήσει να το προσπελάσει χωρίς να γνωρίζει τι περιέχει. Συνεπώς, αποκλείεται η έκθεση σε βλαπτικό υλικό για όποιον θα μπορούσε να προσβληθεί ακόμα και αν αυτό συνέβαινε τυχαία.

Ένα σύγχρονο σύστημα κρυπτογράφησης αποτελείται από τέσσερα (4) κύρια σημεία. Αυτά είναι:

1. Το αρχικό μήνυμα.
2. Το κρυπτογραφικό σύστημα αποτελούμενο από έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο αποκρυπτογράφησης.
3. Το κρυπτογραφημένο μήνυμα. Πρόκειται για το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη.
4. Το κλειδί, το οποίο είναι μια συμβολοσειρά. Η συμβολοσειρά αυτή χρησιμοποιείται στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης από τους αλγορίθμους.

---

[45] . Βλαχόπουλος Κωνσταντίνος, «Ηλεκτρονικό Έγκλημα», Νομική βιβλιοθήκη, Αθήνα 2007, σελ95

Οι βασικότεροι στόχοι που επιτυγχάνονται με την κρυπτογράφηση είναι:

- **Η Αυθεντικοποίηση** . Το μήνυμα δε θα διαρρεύσει σε χρήστη που δεν έχει δικαίωμα πρόσβασης.

-. **Η Ακεραιότητα**. Το μήνυμα θα φτάσει στον παραλήπτη του χωρίς να έχει υποστεί αλλοίωση ή μετατροπή.

- **Η Μη Αποποίηση της Παραλαβής-Αποστολής**. Ο αποστολέας ή ο παραλήπτης του μηνύματος δε θα αρνηθούν ότι έστειλαν το μήνυμα

5.4. Προληπτικά Μέτρα- Συμβουλές[46].

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

5.4.α. 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.

[46] www.safeinternet.gr , www.astynomia.gr , www.efpolis.gr πρόσβαση 12/10/2012

5.4.β . 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 αισθάνεσθε «άβολα». Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάστετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε.

• Αν αισθανθείτε άβολα την ώρα που συνομιλείται 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 ό,τι διαβάζετε στο Διαδίκτυο. Μην εμπιστεύεστε αμέσως ό,τι δείτε.

• Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν «σερφάρετε» στο Internet.

5.4.γ. Συμβουλές για γονείς.

• Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε από αυτά.

• Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.

• Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.

• Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.

• Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.

• Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.

• Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο.

5.4.δ. Συμβουλές για ασφαλείς οικονομικές συναλλαγές.

1. 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.

2. Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείται για τις διαδικτυακές συναλλαγές:

• 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 οιεσδήποτε 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.

3. Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet Banking.

4. Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.

5. 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.

6. Φροντίστε να διατηρείται σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας.

Ειδικότερα:

• 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 εξουσιοδοτένων χρηστών.

7. Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mail):

• Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιν γνωστό σας.

• Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μη στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail). Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.

8. Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων. Ειδικότερα:

• Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά.

• Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα Α.Τ.Μ.

(Βλαχόπουλος, 2007)

ΚΕΦΑΛΑΙΟ 6[47]

«ΕΘΙΣΜΟΣ » ΚΑΙ INTERNET

Στο έκτο κεφάλαιο γίνεται μία συνοπτική ιστορική αναδρομή στο φαινόμενο του εθισμού, τα κλινικά κριτήρια που τον οριοθετούν καθώς και τα αίτια και οι ηλιακές ομάδες οι οποίες εμφανίζουν συχνότερα εθισμό. Κατόπιν παρουσιάζεται έρευνα με τίτλο «ΧΡΗΣΗ ΚΑΙ ΚΑΤΑΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ (INTERNET): ΣΥΣΧΕΤΙΣΕΙΣ ΜΕ ΨΥΧΟΚΟΙΝΩΝΙΚΟΥΣ ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΧΡΗΣΤΕΣ –ΑΠΟΤΕΛΕΣΜΑΤΑ»που διεξήγαγε η Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.),/Πανεπιστήμιο Αθηνών και τα αποτελέσματα της :

6.1. Ιστορική αναδρομή φαινομένου.

Το φαινόμενο της εξάρτησης είδε το φως της δημοσιότητας το 1997, στις Η.Π.Α. Το πρώτο Κέντρο Απεξάρτησης λειτούργησε το 1995, στην Πενσυλβάνια των Η.Π.Α., ενώ την ίδια χρονιά ο Νεοϋορκέζος ψυχίατρος Ivan Goldberg, εν μέρει αστειευόμενος, υιοθέτησε πρώτος τον όρο Internet addiction («εθισμός» στο Internet). Οι πρώτες περιπτώσεις αφορούσαν ενήλικες, ωστόσο τα επόμενα χρόνια το φαινόμενο επεκτάθηκε ραγδαία σε εφήβους και νέους. Λόγω του ότι η Αμερικανική Ψυχιατρική Εταιρεία δεν έχει αποδεχθεί την κατάχρηση διαδικτύου ως κατάσταση αληθούς εθισμού, και υπάρχει γενικά συζήτηση στην διεθνή βιβλιογραφία περί τούτου, ο όρος «εθισμός» ή «εξάρτηση» χρησιμοποιούνται σε εισαγωγικά.

6.2 Κριτήρια εθισμού.

Κριτήρια που οριοθετούν την υπερβολική χρήση είναι η ύπαρξη τουλάχιστον τριών από τα παρακάτω :

- Συμπτώματα Συνδρόμου Απόσυρσης, όπως ψυχοκινητική διέγερση, εκούσια ή ακούσια κίνηση δακτυλογράφησης των δακτύλων του χεριού, άγχος, έμμονη σκέψη για το Internet, όνειρα για το Internet.
- Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης.
- Παραμονή on-line για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο.

[47] www.youth-health.gr πρόσβαση 01/12/2012

- Κατανάλωση υπερβολικού χρόνου ή/και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο (λογισμικό, σκληροί δίσκοι κ.λπ).
- Έκπτωση λειτουργικότητας του ατόμου (σε κοινωνικό, οικογενειακό, προσωπικό επίπεδο, παραμέληση προσωπικής φροντίδας και υγιεινής, απώλεια ύπνου, ενδοοικογενειακές συγκρούσεις, σχολική αποτυχία).
- Συνέχιση χρήσης παρά την γνώση της παραπάνω έκπτωσης.

6.3 Αίτια του φαινομένου και ηλικιακές ομάδες παιδιών που εμφανίζουν εθισμό.

Από τα πρώτα στοιχεία που προκύπτουν από τα 35 (τριάντα πέντε) παιδιά και εφήβους που προσήλθαν στη Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) με αίτημα την αντιμετώπιση της υπερβολικής χρήσης του διαδικτύου προκύπτουν ότι :

1. το φαινόμενο είναι συχνότερο στα αγόρια,
2. σε δυσλειτουργικές οικογένειες,
3. σε παιδιά με καταθλιπτικό συναίσθημα ή διάσπαση προσοχής-υπερκινητικότητα.

Φαίνεται ότι πάνω από τα μισά παιδιά παρουσιάζουν κάποιο ψυχικό υπόστρωμα που πιθανώς συμβάλλει στην ανάπτυξη κατάχρησης διαδικτύου (κυρίως σύνδρομο υπερκινητικότητας-διάσπασης προσοχής ή/ και καταθλιπτικό συναίσθημα), ενώ στα υπόλοιπα σημαντικό ρόλο φαίνεται να παίζουν περιβαλλοντικοί παράγοντες (κυρίως έλλειψη επικοινωνίας και εφαρμογής ορίων από την οικογένεια). Οι νέες κοινωνικές συνθήκες (αύξηση της επίπτωσης του διαζυγίου, έλλειψη επικοινωνίας, απουσία επίβλεψης από τους γονείς λόγω εργασίας έξω από το σπίτι) παίζουν το ρόλο τους στην ανάπτυξη του φαινομένου.

Το φαινόμενο μπορεί να εμφανιστεί σε εφήβους κατά την πρώϊμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι πιο συχνό κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και κατά την όψιμη εφηβεία (> 17 ετών). Οι περισσότεροι εξαρτημένοι έφηβοι ασχολούνται με «παιχνίδια», στο σπίτι ή τα internet cafe.

Μπορεί να σταματήσουν το σχολείο, να απομονωθούν από την οικογένεια και τους φίλους, να είναι επιθετικοί με τους γονείς, να κλέβουν χρήματα από την οικογένεια για να «παίζουν», να ζουν σε ένα δωμάτιο, να

μην τρώνε ή το αντίθετο (να παχύνουν πολύ), να μην γυμνάζονται και να μην κοιμούνται για 24ωρα. Μπορεί ακόμη να μην αλλάζουν ρούχα, να παραμελούν την υγιεινή τους και την καθαριότητα.

Τα παραπάνω μπορεί να εμφανιστούν σε ηπιότερη μορφή κατά την πρώϊμη εφηβεία. Όσο ο έφηβος μεγαλώνει και πλησιάζει την μέση εφηβεία, ο πειραματισμός και η περιέργεια, η μη συνειδητοποίηση του κινδύνου και η φυσιολογική αντίδραση σε κάθε καταπίεση, γίνονται βασικά χαρακτηριστικά του (αποτελεί ακόμη αναπτυσσόμενο άτομο), και τον καθιστούν ευάλωτο και ευαίσθητο σε εξαρτήσεις. Τα παραπάνω δεν είναι απόλυτα, αφού η χρονολογική ηλικία μπορεί να μην συμβαδίζει πάντα με το αναπτυξιακό ψυχοκοινωνικό και γνωστικό στάδιο : π.χ. ένας έφηβος 10 ετών μπορεί να βρίσκεται αναπτυξιακά στη μέση εφηβεία και να συμπεριφέρεται ανάλογα κ.λπ.

6.4 Αποτελέσματα έρευνας σε δείγμα εφήβων Ν. Αττικής 15 ετών(Μ.Ο. : 14.85 έτη) Αντιπροσωπευτικό δείγμα 897 εφήβων (430 αγόρια, 467 κορίτσια)[48]:

- 53.4% χρησιμοποιούσαν το διαδίκτυο για χρονικό διάστημα μεγαλύτερο του 1 έτους

- 26% ανέφεραν καθημερινή χρήση και

- 8% χρήση μεγαλύτερη 20 ωρών / εβδομαδιαίως.

- Τα αγόρια χρησιμοποιούσαν το διαδίκτυο σημαντικά περισσότερο από τα κορίτσια ($p < 0.05$).

- Σύμφωνα με το ερωτηματολόγιο :

- 1% από τους εφήβους του δείγματος παρουσίαζαν υπερβολική χρήση διαδικτύου («εθισμός») και

- 12,8% παρουσίαζαν περιοδικά ή συχνά προβλήματα σχετικά με την κατάχρηση διαδικτύου (κατάσταση πριν το «εθισμό»)

- Ο πιο συχνός λόγος χρήσης του διαδικτύου ήταν τα διάφορα παιχνίδια ($p < 0.05$)

[48] Πηγή : Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.), Πανεπιστήμιο Αθηνών «ΧΡΗΣΗ ΚΑΙ ΚΑΤΑΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ (INTERNET): ΣΥΣΧΕΤΙΣΕΙΣΜΕ ΨΥΧΟΚΟΙΝΩΝΙΚΟΥΣ ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΧΡΗΣΤΕΣ –ΑΠΟΤΕΛΕΣΜΑΤΑ»

- 4.2% του δείγματος είχαν δεχτεί απειλές μέσω διαδικτύου (cyber bulling victims).

- Χρήση του διαδικτύου >10 ώρες εβδομαδιαίως έχει συσχετισθεί με μεγαλύτερη πιθανότητα υπερβολής και επακόλουθων προβλημάτων

- Η ενασχόληση με το διαδίκτυο στο πλαίσιο του σχολείου αποδεικνύεται προστατευτικός παράγοντας έναντι της ανάπτυξης προβληματικής χρήσης

- Υπήρξε θετική συσχέτιση της χρήσης διαδικτύου και της διάσπασης προσοχής-υπερκινητικότητας, σύμφωνα με την κατάταξη στο SDQ ($p< 0.01$)

.- Θετικές συσχετίσεις παρατηρήθηκαν και μεταξύ χρήσης διαδικτύου και παραβατικότητας ($p< 0.05$), καθώς και ανάπτυξης δυσλειτουργικών σχέσεων με τους συνομηλίκους ($p< 0.05$).

6.5 Συμπεράσματα –Συστάσεις :

Η χρήση διαδικτύου είναι δημοφιλής στους Έλληνες εφήβους, και ενδέχεται να οδηγήσει σε ψυχοκοινωνικά προβλήματα, όταν υπάρχει υπερβολή. 35 έφηβοι με «εθισμό» απευθύνθηκαν στη Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) και παρακολουθούνται γι' αυτό. Ας σημειωθεί ότι ενώ σε πρώϊμα στάδια το φαινόμενο αντιμετωπίζεται σχετικά εύκολα με γνωσιακή εκπαίδευση (ημερολόγιο, στόχοι, δημιουργία κινήτρων, ανταμοιβές σε θετική συμπεριφορά, προβληματισμός σε στασιμότητα), καθώς κι αντιμετώπιση της συνοδού νοσηρότητας εάν υπάρχει. Μετά την πλήρη οργάνωσή του προβλήματος, με τα περισσότερα κριτήρια, ο έφηβος δεν αναγνωρίζει ότι υπάρχει πρόβλημα, δεν συνεργάζεται, δεν θέλει καν να επισκεφθεί τη Μ.Ε.Υ., μπορεί να λέει ψέματα, να χειρίζεται και να εξαπατά γονείς και θεραπευτές και γενικά έχει συμπεριφορά ατόμου εξαρτημένου από ουσίες (ναρκωτικά). Στο πρόγραμμα της Μ.Ε.Υ., από τα 35 παιδιά που προσήλθαν έως σήμερα, 15 παρουσίασαν σημαντική βελτίωση, 4 σχετική βελτίωση, 9 βρίσκονται υπό παρακολούθηση και 6 δεν συνεργάστηκαν.

Γονείς θα πρέπει να ανησυχούν αν τα παιδιά τους παρουσιάζουν κάποιες από τις ακόλουθες συμπεριφορές.

-υπερβολικός χρόνος ενασχόλησης, η μονομανία, η παραμέληση των υποχρεώσεων και άλλων ασχολιών, η απότομη πτώση της σχολικής επίδοσης, η απομόνωση και η μείωση του χρόνου δραστηριοτήτων και του

χρόνου που περνούν με φίλους, η επιθετικότητα, η μεταβολή της συμπεριφοράς, η αδιαφορία για πράγματα που παλιά τον/την ευχαριστούσαν, οι πονοκέφαλοι, η ξηρότητα οφθαλμών

Ο καθένας από το πόστο του μπορεί να συμβάλει καθοριστικά για την αντιμετώπιση αυτής της νέας μάστιγας και ειδικότερα:

1. Σχολικό περιβάλλον.

- Ευαισθητοποίηση των εκπαιδευτικών-ενημέρωση για την ύπαρξη του φαινομένου
- Εκπαίδευση των εκπαιδευτικών στη χρήση ηλεκτρονικών υπολογιστών, προκειμένου να πραγματοποιούνται σχολικές εργασίες μέσω
- Εκπαίδευση των μαθητών για τις διάφορες εφαρμογές και τη διευκόλυνσή τους στη χρήση διαδικτυακών μηχανών αναζήτησης
- Παροχή διαδικτύου μέσα στο σχολικό περιβάλλον, με password/login και μέγιστο χρόνο χρήσης (π.χ. 45 λεπτά/ημέρα). Φίλτρα που απαγορεύουν την είσοδο σε ακατάλληλες ιστοσελίδες θα πρέπει να χρησιμοποιούνται.
- Ενημέρωση των γονέων μέσω του σχολείου για το φαινόμενο και τα σημεία αναγνώρισης της προβληματικής χρήσης
- Ύπαρξη σχολικού ψυχολόγου με εκπαίδευση στην αντιμετώπιση της κατάχρησης διαδικτύου, προκειμένου να αντιμετωπισθούν τα παιδιά που θα αντιμετωπίσουν ανάλογο πρόβλημα
- Προαγωγή της χρήσης του υπολογιστή ως εργαλείο μελέτης και ενημέρωσης, και όχι αποκλειστικά σαν μέσο ψυχαγωγίας

2. Σπίτι- Γονείς.

α. Από μικρή ηλικία θα πρέπει να τίθενται όρια (για πολλά θέματα) και να τηρούνται μέσα στην οικογένεια. Τα όρια (όταν δεν είναι υπερβολικά ή ιδιαίτερα αυστηρά) δεν καταπιέζουν τα παιδιά, αλλά τα κατευθύνουν και σημαίνουν ενδιαφέρον. Είναι σημαντικά για θέματα ασφάλειας. Όσο το παιδί μεγαλώνει, τα όρια που θα ισχύσουν είναι καλό να συζητώνται, ώστε να λαμβάνεται η γνώμη του παιδιού και του εφήβου. Ο σεβασμός της προσωπικότητας παιδιών και εφήβων από πολύ μικρή ηλικία, είναι στοιχείο πολύ σημαντικό για την εφαρμογή πειθαρχίας.

β. Αφιερώστε χρόνο και διάθεση ώστε να ασχοληθείτε με θέματα διαδικτύου ΜΑΖΙ με τα παιδιά.

γ. Τοποθετείστε τον υπολογιστή σε κοινόχρηστο χώρο, ώστε να μη δίνεται η δυνατότητα απομόνωσης του παιδιού και να υπάρχει έλεγχος.

δ. Χρήση φίλτρων για επιβλαβείς ιστοσελίδες και συμμετοχή στις επιλογές του εφήβου (χωρίς υπερβολές ή/και παράλογες απαγορεύσεις), συμβάλλουν σε ένα θετικό αποτέλεσμα.

ε. Ενημερώστε τα παιδιά με απλά λόγια από μικρή ηλικία για τα φαινόμενα «εθισμού» και παρενόχλησης.

στ. Μην χρησιμοποιείτε τη χρήση του υπολογιστή για επιβράβευση ή τιμωρία

ζ. Εάν παρατηρήσετε υπερβολική χρήση ή/και συμπεριφορές εθισμού αναζητήστε ΑΜΕΣΩΣ βοήθεια.

3. Κοινωνικό Περιβάλλον.

- Να συζητηθεί εάν χρειάζεται όριο ηλικίας για την είσοδο σε internet cafes.- Φίλτρα και όριο χρήσης (π.χ. 3 ώρες σε ημερήσια επίσκεψη) σε internet cafes
- Ενημέρωση γονέων και παιδιών με σχετικές καταχωρήσεις σε Μέσα Μαζικής Ενημέρωσης για το φαινόμενο, τις μονάδες ενημέρωσης και αντιμετώπισης, τις συμβουλευτικές τηλεφωνικές γραμμές κ.α.
- Παροχή πληροφορίας για την ασφαλή χρήση διαδικτύου με έντυπο υλικό σε μέρη που συχνάζουν οι έφηβοι (σινεμά, ταχυφαγεία, βίντεο/club, bowling), καθώς και μέσα από ιστοσελίδες που επισκέπτονται, με την βοήθεια οργανισμών ή/και ιδιωτικών σχετικών εταιρειών.

4. Υπηρεσίες υγείας.

- Ενημέρωση των ιατρών, ειδικευομένων και φοιτητών για την υπερβολική χρήση διαδικτύου
- Το θέμα να συμπεριλαμβάνεται σε συνέδρια και ημερίδες, ώστε να ευαισθητοποιηθούν οι ειδικοί υγείας που θα έρθουν αντιμέτωποι με τα προβλήματα (παιδίατροι, παιδοψυχίατροι, ψυχολόγοι κ.α.)

5. Κρατική μέριμνα.

- Ενημέρωση του κοινού (έφηβοι και γονείς)
- Εφαρμογή των μέτρων για το σχολικό περιβάλλον (ανωτέρω)

- Νομοθεσία για την λειτουργία των internet cafe[49]

[49] Άρτεμις Κ. Τσίτσικα, Παιδίατρος - Εφηβική Ιατρική Επιστημονική Υπεύθυνος Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.)Β' Παιδιατρική Κλινική Πανεπιστημίου Αθηνών Νοσοκομείο Παίδων "Παν. & Αγλ. Κυριακού

ΚΕΦΑΛΑΙΟ 7^{Ο}

ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΙΑ ΚΑΙ Ο ΡΟΛΟΣ ΤΗΣ ΕΛ.ΑΣ.

7.1 Ο ρόλος της Ελληνικής Αστυνομίας

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί ζήτημα ύψιστης σημασίας για τις αστυνομικές αρχές, όπως άλλωστε και τα κοινά διαπραχθέντα εγκλήματα.

Συγκεκριμένα, όσο αφορά τα ηλεκτρονικά εγκλήματα, που έχουν εισέλθει στην καθημερινότητα μας τα τελευταία χρόνια, το ενδιαφέρον της αστυνομίας εστιάζεται περισσότερο στις ασταμάτητες αλλαγές που προκύπτουν στους κόλπους της τεχνολογίας και έτσι καθιστούν το ηλεκτρονικό έγκλημα ένα σχετικά δύσκολα ανιχνεύσιμο έγκλημα, τόσο στο εξωτερικό όσο και στον Ελλαδικό χώρο. Έτσι, αυτό που φαίνεται να κάνει αποτελεσματικότερο το έργο των διωκτικών αρχών είναι η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού της αστυνομικής αρχής σε θέματα κυρίως τεχνικής φύσεως σχετικά με τη διερεύνηση και τη δίωξη του ηλεκτρονικού εγκλήματος. Στην Ελλάδα, η Ελληνική Αστυνομία (ΕΛ.ΑΣ.), έχει προχωρήσει στη σύσταση Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος. Οι καταγγελίες των πολιτών που διαπιστώνουν ότι έχουν παραβιαστεί προσωπικά τους δεδομένα ή ότι έπεσαν θύματα κάποια ηλεκτρονικής απάτης ή γενικότερα έχουν αντιληφθεί κάτι ύποπτο σχετικά με το διαδίκτυο ή τη χρήση Η/Υ, θα πρέπει να απευθύνονται άμεσα στην αρμόδια αρχή.

Επιπλέον στην Ελλάδα, σχετικός με καταγγελίες για το ηλεκτρονικό έγκλημα είναι και ο ιστότοπος www.saferinternet.gr . Στο συγκεκριμένο ιστότοπο

Δράσης , Ενημέρωσης και Επαγρύπνισης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου (υπό την αιγίδα της Ευρωπαϊκής Ένωσης) υπάρχουν πολλές, χρήσιμες πληροφορίες και συμβουλές για την ορθή χρήση του Διαδικτύου, του κινητού τηλεφώνου και άλλων διαδραστικών τεχνολογιών.

7.2 Εντοπισμός του Ηλεκτρονικού Εγκληματία στο Διαδίκτυο

Στην ενότητα αυτή θα αναφερθούν κάποιοι από τους πιο βασικούς τρόπους που χρησιμοποιούνται από τους ειδικούς για την εξιχνίαση υποθέσεων σχετιζόμενων με το ηλεκτρονικό έγκλημα.

7.2.1. Εντοπισμός IP

Η εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε δίκτυα από τις διωκτικές αρχές βασίζεται στον εντοπισμό της IP διεύθυνσης. Οι ηλεκτρονικοί εγκληματίες για να πραγματοποιήσουν επίθεση σε ένα σύστημα προκειμένου να παραπλανήσουν τις διωκτικές αρχές, χρησιμοποιούν πλαστές IP διευθύνσεις. Κάθε διεύθυνση στο Διαδίκτυο έχει και έναν αντίστοιχο αριθμό IP. Το Σύστημα Ονομάτων Χώρου (Domain Name System D.N.S.) μετατρέπει τα ονόματα των διευθύνσεων σε αριθμούς (IP διευθύνσεις), έτσι ώστε να μπορεί να τις επεξεργαστεί το δίκτυο[50]. Ο επιτιθέμενος λοιπόν κατά την εκδήλωση μιας επίθεσης πλαστογραφεί τη διεύθυνση του με σκοπό να φαίνεται ότι είναι ένας νόμιμος χρήστης, δεν μπορεί όμως να πλαστογραφήσει την IP διεύθυνση. Συσκευές όπως τα firewalls καθώς και άλλα εργαλεία λογισμικού και on-line δικτυακοί τόποι έχουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να αποτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη.

[50] Διακονικολάου Γεώργιος, «Επιχειρησιακή Διαδικτύωση», εκδόσεις Κλειδάριθμος, Αθήνα 2007, σελ.65

7.2.2. Συναγερμοί (Alarms) [51]

Τα Firewalls αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένους παραλήπτες όταν διαπιστωθεί κάποια ύποπτη δραστηριότητα. Τα μηνύματα αυτά αποστέλλονται με e-mail στο διαχειριστή του συστήματος και παράλληλα η ύποπτη δραστηριότητα αποθηκεύεται στα αρχεία καταγραφής. Η συγκεκριμένη λειτουργία των firewalls είναι εξαιρετικά μεγάλης σημασίας καθώς μπορεί να αποτρέψει την επίθεση κατά τη διαδικασία γέννησης της.

7.2.3. Αναφορές (Reports) [52]

Μια αναφορά δίνει αρκετές πληροφορίες για την εκδήλωση της επίθεσης όπως για παράδειγμα τη συχνότητα αποτυχημένων προσπαθειών για την απόκτηση μη εξουσιοδοτημένης πρόσβασης, τη συχνότητα σφαλμάτων και άλλα.

7.2.4. Αρχεία καταγραφής (Log- Files)[53]

Στα αρχεία καταγραφής αποθηκεύονται πληροφορίες σχετικές με τη λειτουργία του συστήματος. Η χρησιμότητα τους μεγιστοποιείται όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές (group policies). Εφόσον δεν έχει οριστεί συγκεκριμένη πολιτική ασφαλείας για μια ομάδα χρηστών, τα security logs παραμένουν κενά. Ο διαχειριστής του συστήματος είναι υπεύθυνος για τον καθορισμό πολιτικών ασφαλείας.

[51] www.netsecurity.about.com προσβαση 07/08/2012
[52] www.netsecurity.about.com προσβαση 07/08/2012
[53] www.ip.gr/el/dictionary/155-Log_File πρόσβαση 07/08/2012

Ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί με τη βοήθεια των αρχείων καταγραφής να εξακριβώσει εάν κάποια συγκεκριμένη εφαρμογή χρησιμοποιήθηκε από χρήστη και αν ο χρήστης αυτός είχε ή όχι εξουσιοδοτημένη πρόσβαση στο σύστημα.

7.2.5 Μηνύματα Ηλεκτρονικού Ταχυδρομείου (E-mail)

Η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί βασική εργασία προς την αναζήτηση και τον εντοπισμό ηλεκτρονικών ιχνών του δράστη. Το ηλεκτρονικό ταχυδρομείο είναι πολύ διαδεδομένο μέσο για τη διάπραξη πολλών αδικημάτων όπως η μετάδοση κακόβουλου λογισμικού, οι απάτες, οι απειλές κλπ. Η αναγραφή των στοιχείων του αποστολέα-δράστη στο μήνυμά του και στην περίπτωση πάντα που τα στοιχεία αυτά δεν είναι παραπλανητικά, οδηγεί εύκολα τις διωκτικές αρχές στον εντοπισμό του. Τα μηνύματα ηλεκτρονικού ταχυδρομείου καθώς μεταβαίνουν από τον αποστολέα στον παραλήπτη, διέρχονται από ενδιάμεσους υπολογιστές, καθένας από τους οποίους προσθέτει στην επικεφαλίδα του μηνύματος τις δικές του πληροφορίες. Αυτές οι πληροφορίες στην επικεφαλίδα του μηνύματος είναι καταγεγραμμένες σε διάφορα πεδία που αφορούν τις επικεφαλίδες του παραλήπτη και του αποστολέα, τις επικεφαλίδες ημερομηνίας και άλλες. Στην αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι κρίσιμες πληροφορίες βρίσκονται στις επικεφαλίδες του αποστολέα. Αυτές είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, το μονοπάτι (διεύθυνση) προς τον αποστολέα και τους διακομιστές από τους οποίους πέρασε το μήνυμα για να φτάσει στον τελικό παραλήπτη του. Ο εντοπισμός του αποστολέα ενός μηνύματος

ηλεκτρονικού ταχυδρομείου είναι μια εξαιρετικά δύσκολη διαδικασία. Υπάρχουν διάφοροι μέθοδοι που βοηθούν τους δράστες στην απόκρυψη των στοιχείων της ταυτότητας τους.

ΕΠΙΛΟΓΟΣ

Οι νέες τεχνολογίες αλλάζουν τους τρόπους και τα μέσα τέλεσης συμβατικών εγκλημάτων, ενώ νέες μορφές αμιγώς ηλεκτρονικών εγκλημάτων με οικονομικό αντίκτυπο τις περισσότερες φορές, κάνουν την εμφάνιση τους με αποτέλεσμα το έργο των διωκτικών αρχών, η νομοθεσία και γενικά όλοι οι τομείς που επηρεάζουν την μεθοδολογία διερεύνησης των εγκλημάτων καθώς και το σύστημα απονομής δικαιοσύνης σε κάθε χώρα να μεταβάλλεται εξαιτίας ελλείψεων.

Ο ηλεκτρονικός εγκληματίας, λειτουργώντας από την μία πλευρά στην αφάνεια και αφήνοντας ελάχιστα ίχνη και από την άλλη με σύμμαχο την έλλειψη τεχνογνωσίας, καταφέρνει καθημερινά να εισβάλει ακόμα και σε εκείνο το σπίτι με το τελειότερα συστήματα ασφαλείας έχοντας σχεδόν πάντα σαν σκοπό την απολαβή οικονομικού οφέλους. Παράλληλα οι μορφές των εγκληματικών ενεργειών του καλύπτουν σχεδόν όλο το φάσμα του ποινικού κώδικα, αλλά και των αναφερθέντων νομικών κενών όσον αφορά τον ηλεκτρονικό χώρο δρα ανενόχλητος.

Για την αντιμετώπιση των φαινομένων αυτών κάθε οργανισμός πρέπει να λάβει τα μέτρα του κατά της εκδήλωσης αυτών των επιθέσεων, αλλά ταυτόχρονα να είναι σε θέση να αποκαταστήσει τη ζημιά που προκλήθηκε με όσο το δυνατότερο λιγότερες οικονομικές απώλειες, εφόσον αυτός είναι ο πρωτεύον σκοπός του εγκληματία.

Στο νέο αυτό περιβάλλον, οι αρχές καλούνται να αντιμετωπίσουν το έγκλημα εκσυγχρονίζοντας της υπηρεσίες Δίωξης Ηλεκτρονικού εγκλήματος με τα κατάλληλα τεχνικά μέσα.

Απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών υποστάσεων εγκλημάτων, που να θέτουν όρια στην συμπεριφορά όσον χρησιμοποιούν το διαδίκτυο κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθούν υπόψη η ελεύθερη διακίνηση ιδεών και οι λοιπές συνταγματικές αρχές. Τέλος απαραίτητη καθίσταται και η εκπαίδευση όλων των εμπλεκόμενων φορέων (Εισαγγελικών-Δικαστικών-Αστυνομικών Αρχών) σε θέματα διαδικτύου καθώς και η ενημέρωση των πολιτών στην χρήση του .

ΠΑΡΑΡΤΗΜΑ Α΄

Ελληνική Νομοθεσία

Νόμοι

- Ν.2225/1994 « Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»

- Ν. 2246/1994 «Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»

- Ν.2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»

- Ν. 2672/1998 «Διακίνηση εγγράφων με ηλεκτρονικά μέσα»

- Ν.2774/1999 «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»

-Ν.2867/2000 «Οργάνωση και λειτουργία των τηλεπικοινωνιών»

-Ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών»

- Ν.3431/2006 ««Περί ηλεκτρονικών επικοινωνιών»

- Ν. 3471/2006 «Προστασία Δεδομένων Προσωπικού Χαρακτήρα»

Προεδρικά διατάγματα

- Π.Δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».

- ΠΔ. 342/2002 «Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο»

-Π.Δ. 131/2003 «Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των

υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.»

- ΠΔ.47/2005 «Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών»

Άρθρα Ποινικού Κώδικα Σχετικά με το Ηλεκτρονικό Έγκλημα

Άρθρο 13 γ΄ ΠΚ

Πλαστογραφία σε ηλεκτρονικό έγγραφο

Έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. "Εγγραφο είναι και κάθε μέσο στο οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία".

Άρθρο 348Α ΠΚ

Πορνογραφία ανηλίκων

Σύμφωνα με το άρθρο 348 Α ΠΚ, το οποίο θεσπίστηκε με το Ν. 3064/2002, «1. Όποιος από κερδοσκοπία παρασκευάζει, κατέχει, προμηθεύεται, αγοράζει, μεταφέρει, διακινεί, διαθέτει, πωλεί ή θέτει με οποιονδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

2. Πορνογραφικό υλικό κατά την έννοια της προηγούμενης παραγράφου συνιστά κάθε περιγραφή ή πραγματική ή εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση, σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο.

3. Αν κάποια από τις πράξεις της πρώτης παραγράφου αφορά πορνογραφικό υλικό που συνδέεται με την εκμετάλλευση της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας ή της απειρίας ανηλίκου ή με την άσκηση σωματικής βίας κατ' αυτού, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ και αν η πράξη είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ.»

Άρθρο 370Α

Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση. Η χρησιμοποίηση από το δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκε με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνητά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων, τιμωρείται με φυλάκιση. Με την ίδια ποινή τιμωρείται και όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου. Το δεύτερο εδάφιο της παραγρ. 1 αυτού του άρθρου εφαρμόζεται και σ' αυτή την περίπτωση.

3. Με φυλάκιση τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Η πράξη της παραγρ.3 δεν είναι άδικη αν η χρήση έγινε ενώπιον οποιουδήποτε δικαστηρίου, ανακριτικής ή άλλης δημόσιας αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος που δε μπορούσε να διαφυλαχθεί διαφορετικά και ιδίως σε ποινικό δικαστήριο για την υπεράσπιση του κατηγορουμένου και γενικά αν η χρήση έγινε για την εκπλήρωση καθήκοντος του κατηγορουμένου ή για τη διαφύλαξη έννομου ή άλλου δικαιολογημένου ουσιώδους δημοσίου συμφέροντος.

5. Η ποινική δίωξη της πράξης της παραγράφου 3 γίνεται μόνο με έγκληση.

6. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι ιδιωτικός αστυνομικός ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή απέβλεπε στην είσπραξη αμοιβής επιβάλλεται φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή.

7. Όποιος διαθέτει στο εμπόριο ή μ' άλλο τρόπο προσφέρει για εγκατάσταση τεχνικά μέσα ειδικά μόνο για την τέλεση των πράξεων των παραγράφων 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους, τιμωρείται με φυλάκιση και με χρηματική ποινή.

Άρθρο 370 Β

Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα ηλεκτρονικών υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά τα ανωτέρω πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση.

Άρθρο 370Γ

Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή

διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386Α

Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Ευρωπαϊκή Νομοθεσία (Οδηγίες Ε.Ε.)

- Οδηγία 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη (τροποποιείται με την Οδηγία 90/88/ΕΟΚ).

- 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).

- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών.

-Οδηγία 96/9/ΕΟΚ της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

- Οδηγία 1999/93/ΕΚ, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

- 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).

-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).

- 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).

-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).

- 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).

- 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).

-Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

ΠΑΡΑΡΤΗΜΑ Β

(http://www.tovima.gr/science/psychology-sociology/article/?aid=456829

πρόσβαση 12/11/2012)

Ένα νέο κενό ασφαλείας που ανακαλύφθηκε πρόσφατα στο Facebook μπορούσε να επιτρέψει σε οποιονδήποτε να δει τις ηλεκτρονικές διευθύνσεις που αντιστοιχούν σε ορισμένους λογαριασμούς χρηστών, ενώ κάποιοι από αυτούς ήταν προσβάσιμοι αυτόματα, χωρίς την ανάγκη εισαγωγής κωδικού.

Ένα μέλος του Hacker News ανακάλυψε πως μόνο με την επίσκεψη σε μια συγκεκριμένη συντόμευση (link), η οποία περιέχει το User ID ενός χρήστη, ο οποιοσδήποτε μπορούσε να δει το e-mail που αντιστοιχούσε στον εν λόγω λογαριασμό. Κάνοντας κλικ στο κουμπί «continue» μάλιστα, μπορούσε να μπει κανονικά στο προφίλ χωρίς να έχει τον απαιτούμενο κωδικό.

Αυτό σημαίνει πως στην καλύτερη περίπτωση, επιτήδειοι θα μπορούσαν να ανακαλύψουν την ηλεκτρονική διεύθυνση των χρηστών του Facebook, στην χειρότερη θα μπορούσαν να αποκτήσουν τον έλεγχο του λογαριασμού τους στο κοινωνικό δίκτυο.

«Όλα ξεκίνησαν όταν ένας φίλος μου έστειλε ένα e-mail που περιείχε link κοινοποίηση μιας ομάδας του Facebook», είπε ο nico-roddz, το μέλος που ανακάλυψε το πρόβλημα. «Όταν έκανα κλικ στο link μπήκα αυτόματα στον λογαριασμό του φίλου μου. Είναι λοιπόν σίγουρα ένα ζήτημα ασφαλείας του Facebook.

Σαν να μην έφτανε αυτό, η «βασική» μορφή της συντόμευσης διέρρευσε στο διαδίκτυο, θέτοντας σε κίνδυνο εκατομμύρια λογαριασμούς χρηστών.

Όπως εξήγησε ο μηχανικός λογισμικού Matt Jones, αυτές οι διευθύνσεις στέλνονται μόνο στους ίδιους τους χρήστες μέσω email «για την διευκόλυνση τους» και δεν πρέπει να δημοσιοποιούνται, ενώ πρόσθεσε πως λήγουν μετά από κάποιο χρονικό διάστημα και λειτουργούν μόνο για ορισμένους χρήστες.

Προς το παρόν λόγω της αποκάλυψης της ύπαρξης τους από το Hacker News αλλά της διαρροής τους στο διαδίκτυο, το Facebook έχει απενεργοποιήσει το συγκεκριμένο χαρακτηριστικό ενώ έχει ήδη ξεκινήσει να λαμβάνει μέτρα για την προστασία όσων λογαριασμών επηρεάστηκαν από το κενό ασφαλείας.

(http://www.inews.gr/196/o-ethismos-sto-Facebook-borei-na-prokalesei-katathlipsi.htm πρόσβαση 12/11/2012)

Σύμφωνα με τους επιστήμονες, μεγαλύτερο κίνδυνο να εμφανίσουν εθισμό στο Facebook αντιμετωπίζουν οι γυναίκες και γενικά τα αγχώδη και κοινωνικά ανασφαλή άτομα

Εάν φίλοι και συγγενείς επιμένουν ότι είστε «κολλημένοι» με το Facebook, τότε ενδεχομένως να έχουν δίκιο. Προκειμένου να βοηθήσουν όσους έχουν εθιστεί στην φημισμένη ιστοσελίδα κοινωνικής δικτύωσης να συνειδητοποιήσουν την κατάστασή τους, ειδικοί του Πανεπιστημίου του Μπέργκεν (UiB) δημιούργησαν ένα τεστ, ικανό να σημάνει το «καμπανάκι» του κινδύνου.

Μετρώντας τις ηλεκτρονικές… «επισκέψεις»

Το τεστ, γνωστό και ως Bergen Facebook Addiction Scale, βασίζεται σε έξι κριτήρια, τα οποία ο ενδιαφερόμενος καλείται να αξιολογήσει σε μια κλίμακα από το ένα μέχρι το πέντε – όπου το ένα αντιστοιχεί σε «πολύ σπάνια», το δύο σε «σπάνια», το τρία σε «μερικές φορές», το τέσσερα σε «συχνά» και το πέντε σε «πολύ συχνά».

Ιδού λοιπόν τα έξι κριτηρια του εύκολου και γρήγορου τεστ, που μας βοηθούν να "διαγνώσουμε" την εξάρτησή μας από το FB

Περνάτε πολλή ώρα σκεπτόμενοι το FB, ή σχεδιάζοντας πώς θα χρησιμοποιήσετε το FB.

Αισθάνεστε την ανάγκη να χρησιμοποιείτε το FB ολοένα και περισσότερο.

Χρησιμοποιείτε το FB για να ξεχάσετε το προσωπικά σας προβλήματα.

Έχετε προσπαθήσει να ελαττώσετε την χρήση του FB αλλά χωρίς αποτέλεσμα.

Αν σας απαγορεύσουν να χρησιμοποιήσετε το FB νιώθετε ανησυχία ή ταραχή.

Χρησιμοποιείτε το FB τόσο πολύ ώστε να έχει αρνητική επίπτωση στην εργασία ή στις σπουδές σας.

Αν κάνατε το παραπάνω τεστ και απαντήσατε «συχνά» ή «πολύ συχνά» σε τουλάχιστον 4 από τα 6 κριτήρια, πιθανότατα είστε εθισμένοι στη συγκεκριμένη ιστοσελίδα κοινωνικής δικτύωσης. Και, κατά τους επιστήμονες, δεν είστε μόνοι.

«Η χρήση του Facebook έχει αυξηθεί κατακόρυφα. Εμείς μελετάμε μια υπό-ομάδα εθισμού στο Διαδίκτυο που αφορά τα social media» αναφέρει η επικεφαλής της μελέτης δρ Σέσιλι Σου Αντρεασεν.

Τα μοτίβα του εθισμού

Στη μελέτη, η οποία δημοσιεύεται στο επιστημονικό έντυπο «Psychological Reports», έλαβαν μέρος συνολικά 423 φοιτητές (227 γυναίκες και 196 άνδρες). Διαπιστώθηκε ότι υπάρχουν κάποια ξεκάθαρα μοτίβα που υποδηλώνουν εθισμό στο Facebook.

«Ο συγκεκριμένος τύπος εθισμού φαίνεται να πλήττει κυρίως μικρότερες ηλικίες. Είδαμε ακόμα ότι άτομα αγχώδη ή κοινωνικά ανασφαλή χρησιμοποιούν το Facebook περισσότερο από άλλους, καθώς βρίσκουν την επικοινωνία μέσω των social media ευκολότερη συγκριτικά με την κατά πρόσωπο επικοινωνία» υποστηρίζει η δρ Αντρεασεν.

Οι ερευνητές διαπίστωσαν ακόμη, ότι τα οργανωμένα και φιλόδοξα άτομα αντιμετωπίζουν μικρότερο κίνδυνο στο να πέσουν στα δίχτια του εθισμού στο FB. Χρησιμοποιούν, παρόλα αυτά, συχνά τα social media για σκοπούς που σχετίζονται με τη δουλειά τους και για την δικτύωσή τους με άλλους.

«Εκείνες που κινδυνεύουν περισσότερο να εθιστούν στο Facebook είναι οι γυναίκες, ίσως λόγω της κοινωνικής φύσης της συγκεκριμένης σελίδας» προσθέτει η ειδικός.

Η μελέτη έδειξε ακόμα ότι ο εθισμός στο FB σχετίζεται επίσης με το πόσο εξωστρεφής είναι κανείς.

(www.astynomia.gr πρόσβαση 12-02-2013)

Χρησιμοποιούσαν στον ιστότοπό τους, παραλλαγές της ονομασίας «Thessalonikiairport», εξαπατώντας και δίνοντας την εντύπωση ότι διαχειριστής τους είναι η Υπηρεσία Πολιτικής Αεροπορίας

Σχηματίστηκε δικογραφία από την Υπηρεσία Οικονομικής Αστυνομίας & Δίωξης Ηλεκτρονικού Εγκλήματος, για απάτη μέσω διαδικτύου κατ΄εξακολούθηση, που αφορά τέσσερις (4) ιστοσελίδες.

Ειδικότερα, η διερεύνηση της υπόθεσης σχετικά με τους ανωτέρω ιστότοπους, ξεκίνησε ύστερα από καταγγελίες της Διεύθυνσης Αεροπορικής Εκμετάλλευσης, της Υπηρεσίας Πολιτικής Αεροπορίας, καθώς και του Κρατικού Αερολιμένα Θεσσαλονίκης «Μακεδονία».

Συγκεκριμένα, χαρακτηριστικό των ιστοσελίδων αυτών είναι ότι χρησιμοποιούν παραλλαγές της αγγλικής ονομασίας «Thessaloniki airport», εξαπατώντας και δίνοντας την εντύπωση ότι αφορούν τον Κρατικό Αερολιμένα Θεσσαλονίκης «Μακεδονία» και ότι διαχειριστής τους είναι η Υπηρεσία Πολιτικής Αεροπορίας. Επίσης, με απατηλό τρόπο παρέχουν τη δυνατότητα κράτησης αεροπορικών εισιτηρίων και ανακριβείς - μη έγκυρες πληροφορίες για το αεροδρόμιο της Θεσσαλονίκης.

Στο πλαίσιο ενδελεχούς ψηφιακής ανάλυσης που πραγματοποίησαν στελέχη της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, προέκυψε ότι οι ανωτέρω ιστοσελίδες φιλοξενούνται σε διακομιστές (servers) που βρίσκονται σε χώρες του εξωτερικού και συγκεκριμένα την Ολλανδία, τη Μεγάλη Βρετανία και τις Ηνωμένες Πολιτείες της Αμερικής.

Για την ύπαρξη των ιστοσελίδων αυτών, μέσω της Interpol της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας, ενημερώθηκαν οι αρμόδιες αρχές του εξωτερικού.

Η δικογραφία που σχηματίστηκε υποβλήθηκε στον κ. Εισαγγελέα Πρωτοδικών Αθηνών.

Σημειώνεται ότι οι πολίτες θα πρέπει να είναι προσεκτικοί, προς αποφυγή πιθανής εξαπάτησης από τους παραπάνω ή άλλους απατηλούς ιστότοπους.

Επίσης όταν επιθυμούν σχετική ενημέρωση, θα πρέπει να επισκέπτονται την επίσημη ιστοσελίδα www.hcaa.gr, της Υπηρεσίας Πολιτικής Αεροπορίας.
(http://dialogoi.enet.gr πρόσβαση 10/10/2012)

Ξέρω, όπως όλοι μας, ότι κυκλοφορεί άφθονο πορνογραφικό υλικό στο web, αλλά δεν είχα ως τώρα κάποια αφορμή να εστιάσω σε αυτό. Την αφορμή την πήρα όταν έκανα την έρευνα για το άρθρο Βρέφη ενάντια στην παιδική βία, όταν μελετούσα στοιχεία για την ανατριχιαστική αύξηση της σεξουαλικής βίας στα παιδιά. Εκεί έπεσα σε ένα άρθρο της Mary Anne Layden, η οποία είναι θεραπεύτρια σεξουαλικών τραυμάτων σε κάποιο Κέντρο του πανεπιστημίου της Πενσιλβάνια. Το άρθρο υποδείκνυε ότι η πορνογραφία στο Ίντερνετ είναι χειρότερο ναρκωτικό και από το κρακ: Τα λεγόμενα της Layden με εντυπωσίασαν, έψαξα στοιχεία για την πορνογραφία στο Διαδίκτυο και σας τα παρουσιάζω:

Υπολογίσθηκε ότι κάθε δευτερόλεπτο που περνά, ξοδεύονται 3,075.64$ για τα πορνογραφικά site. Ο αριθμός των ατόμων, ανά δευτερόλεπτο, που βλέπουν πορνογραφικό υλικό στο Ιντερνετ, ανέρχεται σε 28,258, ενώ ο αριθμός των ατόμων που πληκτρολογεί στις μηχανές αναζήτησης , ανά δευτερόλεπτο, λέξεις που οδηγούν σε πορνό, είναι 372 (που μας κάνει 22.320 άτομα το λεπτό). Μία άλλη πληροφορία είναι ότι στις ΗΠΑ φτιάχνεται μια καινούρια βιντεοταινία πορνό κάθε 39 λεπτά. Η πορνογραφία δεν αποτελεί απλώς βιομηχανία, είναι μία από τις ισχυρότερες, αφού κερδίζει περισσότερα χρήματα από τις εταιρείες: Microsoft, Google, Amazon, eBay, Yahoo, Apple και Netflix, μαζεμένες. Τα κέρδη της ανέρχονται στα $97.06 δισεκατομμύρια δολάρια το χρόνο!
(http://www.wired.com/science/discoveries/news/2004/11/65772 πρόσβαση 12-10-2013)

(http://www.astynomia.gr πρόσβαση 17-02-2013)

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

ΔΕΛΤΙΟ ΤΥΠΟΥ

Σύλληψη 34χρονου ημεδαπού στη Μυτιλήνη, για πορνογραφία ανηλίκων

Συνελήφθη, χθες (16-02-2013) το μεσημέρι στη Μυτιλήνη, μετά από μεθοδευμένη επιχείρηση αστυνομικών της Υποδιεύθυνσης Ασφαλείας Μυτιλήνης και του Τμήματος Δίωξης Ναρκωτικών Μυτιλήνης, ένας (1) ημεδαπός ηλικίας 34 ετών, σε βάρος του οποίου σχηματίστηκε δικογραφία για πορνογραφία ανηλίκων.

Ειδικότερα, σε έρευνα που πραγματοποιήθηκε στην οικία του 34χρονου, παρουσία εκπροσώπου της δικαστικής Αρχής, βρέθηκαν και κατασχέθηκαν τα παρακάτω:

Τρεις (3) ηλεκτρονικοί υπολογιστές

Διάφορα φορητά ψηφιακά μέσα αποθήκευσης (σκληροί δίσκοι, USB sticks)

Πλήθος ψηφιακών οπτικοακουστικών δίσκων (cd , dvd)

Πέντε (5) τραπεζικές κάρτες

Από την επιτόπια αυτοψία που πραγματοποιήθηκε στα παραπάνω ψηφιακά αποθηκευτικά μέσα, εντοπίστηκε μεγάλος αριθμός αρχείων με «σκληρό» υλικό παιδικής πορνογραφίας.

Ο συλληφθείς θα οδηγηθεί στην Εισαγγελία Πρωτοδικών Μυτιλήνης, ενώ την προανάκριση και τις έρευνες διενεργεί η Υποδιεύθυνση Ασφαλείας Μυτιλήνης.

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

Αθήνα, 29 Ιανουαρίου 2013

ΔΕΛΤΙΟ ΤΥΠΟΥ

Συνελήφθη από τη Δίωξη Ηλεκτρονικού Εγκλήματος 52χρονη ημεδαπή, ιδιωτική υπάλληλος-καθηγήτρια ξένων γλωσσών, για πορνογραφία ανηλίκων

Στην κατοχή της βρέθηκαν περιοδικά παιδοφιλικού περιεχομένου, εγχειρίδιο για επαφές μεταξύ ενηλίκων και παιδιών και τετράδιο με σημειώσεις σχετικά με παιδοφιλικό κίνημα στην Αθήνα

Από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος συνελήφθη χθες (28.01.2013), στην Αθήνα, στο πλαίσιο της αυτόφωρης διαδικασίας, 52χρονη ημεδαπή, ιδιωτική υπάλληλος-καθηγήτρια ξένων γλωσσών, σε βάρος της οποίας σχηματίστηκε δικογραφία για πορνογραφία ανηλίκων.

Είχε προηγηθεί, μέσω ηλεκτρονικού ταχυδρομείου, καταγγελία στη Δίωξη Ηλεκτρονικού Εγκλήματος, από δημοσιογράφο τηλεοπτικής εκπομπής της Ολλανδίας, ότι συνάδελφοι της, στο πλαίσιο δημοσιογραφικής έρευνας για

γνωστό παιδόφιλο στην Ολλανδία, ήρθαν σε επαφή, μέσω ηλεκτρονικού ταχυδρομείου, μεταξύ άλλων και με την 52χρονη, κάτοικο Αθήνας, η οποία εμφανίζεται ως ενεργό μέλος σε πολλές οργανώσεις παιδόφιλων, ανά τον κόσμο.

Σύμφωνα με τα στοιχεία της υπόθεσης, η δημοσιογράφος επισκέφτηκε την Ελλάδα και υποδυόμενη την παιδόφιλο συνάντησε την κατηγορουμένη, η οποία την προέτρεψε να έχει σεξουαλικές επαφές με ανήλικους.

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διερευνώντας την υπόθεση κατάφερε να εντοπίσει το σπίτι της ημεδαπής, όπου χθες πραγματοποιήθηκε νομότυπη έρευνα, παρουσία Εισαγγελικού Λειτουργού. Κατά τη διάρκεια της έρευνας βρέθηκαν και κατασχέθηκαν:

Ένας (1) σκληρός δίσκος Η/Υ, ο οποίος θα αποσταλεί στη Διεύθυνση Εγκληματολογικών Ερευνών για περαιτέρω εργαστηριακή εξέταση,

Τριάντα τέσσερα (34) περιοδικά παιδοφιλικού περιεχομένου,

Ένα (1) εγχειρίδιο για σεξουαλικές επαφές μεταξύ ενηλίκων και παιδιών,

Ένα (1) τετράδιο με χειρόγραφες σημειώσεις σχετικά με παιδοφιλικό κίνημα στην Αθήνα, καθώς και με ονόματα πουσυμμετείχαν σε συνεδριάσεις του, και

Η 52χρονη, με τη δικογραφία που σχηματίστηκε σε βάρος της οδηγείται σήμερα (29-01-2013) στην Εισαγγελία Πρωτοδικών Αθηνών, ενώ ερευνάται η περαιτέρω συμμετοχή της σε δραστηριότητες παιδοφιλικού χαρακτήρα, εντός και εκτός της χώρας μας. Σημειώνεται ότι είναι η πρώτη γυναίκα που συλλαμβάνεται στην χώρα μας για τέτοια αδικήματα.

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

Αθήνα, 24 Ιανουαρίου 2013

ΑΝΑΚΟΙΝΩΣΗ

Από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, μετά από διαδικτυακές έρευνες και ψηφιακή διερεύνηση καταγγελιών, ανακοινώνεται ότι έχει εντοπιστεί προσπάθεια αλίευσης και υποκλοπής κωδικών (Phishing Attack) από τραπεζικούς πελάτες, οι οποίοι είναι χρήστες υπηρεσιών e-banking, με σκοπό την διενέργεια συναλλαγών και τη μεταφορά χρημάτων τους σε τραπεζικούς λογαριασμούς τρίτων προσώπων στο εξωτερικό.

Ειδικότερα, οι δράστες χρησιμοποιούν κακόβουλο λογισμικό, που εγκαθίσταται στους υπολογιστές των χρηστών διαδικτυακών υπηρεσιών

internet banking και παγιδεύει τον ηλεκτρονικό υπολογιστή τους, με αποτέλεσμα να υφαρπάζει τους κωδικούς ασφαλείας και η συναλλαγή (π.χ. για μεταφορά χρημάτων ή πληρωμή πιστωτικής κάρτας) να ολοκληρώνεται από τρίτα πρόσωπα, τα οποία μεταφέρουν σε δικούς τους λογαριασμούς χρηματικά ποσά, χωρίς την έγκριση του δικαιούχου.

Διευκρινίζεται ότι οι παραβιάσεις ή επιθέσεις έχουν εντοπιστεί σε χρήστες υπηρεσιών internet banking και όχι σε υπολογιστικά συστήματα Ελληνικών Τραπεζών.

Στο πλαίσιο αυτό η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συμβουλεύει τους πολίτες:

Να μην συνεχίζουν τη διαδικασία εισαγωγής στην Υπηρεσία internet banking, εφόσον παρατηρήσουν διαφορετική λειτουργικότητα από τη συνηθισμένη και να επικοινωνούν καταρχήν με την Τράπεζα ή/και με την Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος στο τηλέφωνο 11012 ή στο 210-6476464 .

Να έχουν ενημερωμένο λογισμικό για προστασία από ιούς και malware.

Σε περίπτωση που διαπιστώσουν ότι ο υπολογιστής τους έχει μολυνθεί από το κακόβουλο λογισμικό να εκτελέσουν ένα ενημερωμένο πρόγραμμα προστασίας, προκειμένου να απομακρύνουν το κακόβουλο λογισμικό από τον υπολογιστή τους.

Να αλλάξουν τον κωδικό πρόσβασης μετά τον καθαρισμό του υπολογιστή από το κακόβουλο λογισμικό.

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος διενεργεί έρευνα για τον εντοπισμό των δραστών σε διεθνές επίπεδο.

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

Αθήνα, 16 Ιανουαρίου 2013

ΔΕΛΤΙΟ ΤΥΠΟΥ

Έρευνα της Δίωξης Ηλεκτρονικού Εγκλήματος σε εταιρεία που κατείχε παράνομα μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα.

Σε υπολογιστές της εταιρείας εντοπίστηκαν ψηφιακές βάσεις με εκατοντάδες χιλιάδες δεδομένα προσωπικού χαρακτήρα, όπως ονοματεπώνυμα, στοιχεία οχημάτων και ιδιοκτητών, ποσά εισοδημάτων, αριθμοί απόρρητων τηλεφώνων, φορολογικά στοιχεία κ.ά.

Συνελήφθη με την αυτόφωρη διαδικασία, ο ιδιοκτήτης και νόμιμος εκπρόσωπος της εταιρείας
Κατασχέθηκαν, τρεις εσωτερικοί σκληροί δίσκοι συνολικής χωρητικότητας παραπάνω από 13.000 GB

Αστυνομική έρευνα πραγματοποιήθηκε χθες (15.01.2013) από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, σε εταιρεία, η οποία δραστηριοποιείται στο χώρο της επικοινωνίας και όπως διαπιστώθηκε κατείχε και διακινούσε παράνομα μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα.
Συνελήφθη για την υπόθεση αυτή, ο ιδιοκτήτης και νόμιμος εκπρόσωπος της εταιρείας (45χρονος ημεδαπός), σε βάρος του οποίου σχηματίστηκε ποινική δικογραφία για παραβίαση των νομικών διατάξεων περί προστασίας των προσωπικών δεδομένων.
Προηγήθηκε κατάλληλη αξιοποίηση πληροφοριών από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, σχετικά με ύπαρξη εταιρείας η οποία εμπορεύεται παράνομα δεδομένα προσωπικού χαρακτήρα. Με βάση τα στοιχεία που προέκυψαν από την έρευνα κλιμάκιο αστυνομικών εντόπισε την έδρα της εταιρείας, σε περιοχή του κέντρου της Αθήνας και πραγματοποίησε έρευνα στα γραφεία της.
Από την επιτόπια έρευνα στα γραφεία της εταιρείας, εντοπίστηκαν, σε τρεις (3) ηλεκτρονικούς υπολογιστές ψηφιακές βάσεις με εκατοντάδες χιλιάδες καταχωρήσεις δεδομένων προσωπικού χαρακτήρα, όπως ονοματεπώνυμα, στοιχεία οχημάτων, αριθμοί απόρρητων τηλεφωνικών συνδέσεων, ποσά εισοδημάτων, φορολογικά στοιχεία (π.χ. Α.Φ.Μ.), για τα οποία η εταιρεία δεν κατείχε την προβλεπόμενη άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
Κατασχέθηκαν, τρείς (3) εσωτερικοί σκληροί δίσκοι συνολικής χωρητικότητας 13.200 GB, οι οποίοι θα αποσταλούν στα Εγκληματολογικά Εργαστήρια της Ελληνικής Αστυνομίας για τις απαραίτητες εργαστηριακές εξετάσεις.
Σημειώνεται ότι στη διερεύνηση της υπόθεσης και στις σχετικές έρευνες συμμετείχε ανώτατο στέλεχος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ο 45χρονος συλληφθείς θα οδηγηθεί σήμερα στον κ. Εισαγγελέα Πλημμελειοδικών Αθηνών.

Η έρευνα συνεχίζεται προκειμένου να προσδιοριστεί επακριβώς ο αριθμός των προσωπικών δεδομένων, καθώς επίσης η προέλευση αλλά και η περαιτέρω διαχείριση – διάθεση τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Βλαχόπουλος Κ.(2007), «Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση», Αθήνα, Νομική Βιβλιοθήκη.
2. Τσουραμάνης Χρ.(2005), «Ψηφιακή Εγκληματικότητα - Η (αν)ασφαλής όψη του διαδικτύου», Αθήνα, Εκδ.Β.Ν. Κατσαρού.
3. Νικολαΐδης Χρ.(1999), «Η σκοτεινή πλευρά του Internet», Αθήνα, Εκδ.Anubis.
4. Συκιώτου Αθ.(2009), «Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης» Αθήνα, Αντ. Ν. Σάκκουλας.
5. Λάζος Γρ. (2001), «Πληροφορική και Έγκλημα», Αθήνα, Νομική Βιβλιοθήκη.
6. Βελέντζας Ε.Ι. (2008), «Δίκαιο Τεχνολογίας και Καινοτομίας», Θεσσαλονίκη, Εκδ.Ius
7. Ζάννη Αν.(2005), «Το διαδικτυακό έγκλημα, Αθήνα», Αντ. Ν. Σάκκουλας.
8. Κιούπης Δ. - Ιωαννίδου Α. (2007), «Η παιδική πορνογραφία στο διαδίκτυο»,Αθήνα, Νομική Βιβλιοθήκη.
9. Κριθαράς Θ. (2009), «Ποινικό Δίκαιο και Διαδίκτυο», Αθήνα, Νομική Βιβλιοθήκη.
10. Καϊάφα - Γκμπάντι Μ. - Συμεωνίδου-Καστανίδου Ε. (2004), «Ποινικός Κώδικας και Ειδικοί Ποινικοί Νόμοι», β΄έκδοση, Αθήνα, Νομική Βιβλιοθήκη.
11. Furnell St., (2006), «Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας», (μετάφραση: Φ. Μηλιώνη), Αθήνα, Εκδόσεις Παπαζήση.
12. Γ.Α. Μαγκάκης «Ποινικό Δίκαιο», έκδοση γ΄βελτιωμένη, εκδόσεις Παπαζήση ,1984

13. Debra Littlejohn Shinder, Ed Tittel, “Scence of cybercrime Computer Forensic Handbook.

Ιστοσελίδες

http://www.saferinternet.gr
http://www.e-crime.gr
http://www.astynomia.gr
http://www.microsoft.com/hellas
http://www.eett.gr
http://www.dpa.gr
http://www.dart.gov.gr/
http://www.europa.eu/index_el.htm
http:// www. go-online.gr
http://www. it.security.gr
http://www. sch .gr
http:// www.computer.howstaffworks.com
http:// www.pharming-fishing.gr
http:// www.netsecurity.about.com
http:// www.threatpost.com.enus
http:// www.greeklaw.voidpress.com
http:// www.en.wikipedia.org
http:// www.fbi.gov
http:// www.youth-health.gr
http:// www.ip.gr
http://www.tovima.gr/science/psychology-sociology/article/?aid=456829