ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ Δ.Ο.Ε.Π&Τ.Μ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΦΟΙΤΗΤΗΣ:ΚΟΥΓΙΑΣ ΙΩΑΝΝΗΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΣΩΤΗΡΗΣ

ΠΥΡΓΟΣ, 2018

ΠΙΣΤΟΠΟΙΗΣΗ

Πιστοποιείται ότι η πτυχιακή εργασία με θέμα:

«Η ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

του φοιτητή του Τμήματος**Δ.Ο.Ε.Π &Τ.Μ**

ΚΟΥΓΙΑΣ ΙΩΑΝΝΗΣ

Α.Μ.: 739

παρουσιάστηκε δημόσια και εξετάσθηκε στο Τμήμα**Δ.Ο.Ε.Π &Τ.Μ**

στις

_____ / _____ / _____

Ο ΕΠΙΒΛΕΠΩΝ

ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΣΩΤΗΡΗΣ

Ο ΠΡΟΕΔΡΟΣ ΤΟΥ ΤΜΗΜΑΤΟΣ

Δρ. ΙΩΑΝΝΗΣ ΚΟΥΓΙΑΣ
ΚΑΘΗΓΗΤΗΣ

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Ακόμα δηλώνω ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα προσωπικά και αποκλειστικά και ειδικά για την συγκεκριμένη πτυχιακή εργασία και ότι θα αναλάβω πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχθεί ότι δεν μου ανήκει.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 1	ΑΜ	ΥΠΟΓΡΑΦΗ
ΚΟΥΣΙΑΣ ΙΩΑΝΝΗΣ	739	
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 2 *(σε περίπτωση που είναι απαραίτητο)*	**ΑΜ**	**ΥΠΟΓΡΑΦΗ**
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 3 *(σε περίπτωση που είναι απαραίτητο)*	**ΑΜ**	**ΥΠΟΓΡΑΦΗ**

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον Επιβλέποντα Καθηγητή μου κύριο ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΣΩΤΗΡΗ για την καθοδήγηση και την υποστήριξή του, καθ' όλη τη διάρκεια εκπόνησης της παρούσας πτυχιακής εργασίας.

Τέλος, εκφράζω τις θερμές μου ευχαριστίες στην οικογένεια μου για την ανιδιοτελή αγάπη, την αμείωτη συμπαράσταση, ενθάρρυνση και πολύπλευρη στήριξη τους κατά την διάρκεια των σπουδών μου.

ΠΡΟΛΟΓΟΣ

Η ανάπτυξη της τεχνολογίας και ως επακόλουθο η ανάπτυξη της πληροφορικής και του Διαδικτύου έχουν καταστήσει τους υπολογιστές αναπόσπαστο μέρος της καθημερινότητας μας. Αυτή η εξέλιξη έφερε μαζί με τα θετικά και αρκετά αρνητικά στοιχεία. Ένα από αυτά τα αρνητικά στοιχεία είναι η εμφάνιση μιας νέας μορφής εγκλήματος το λεγόμενο ως «Διαδικτυακό Έγκλημα».

Με την χρήση των ηλεκτρονικών υπολογιστών και με ή χωρίς τη χρήση του διαδικτύου διαπράττονται καθημερινά αμέτρητα εγκλήματα. Ακόμη και ο ίδιος ο υπολογιστής μπορεί να είναι το θύμα της επίθεσης. Απειλές, απάτες, υποκλοπές και κάθε είδους παρανομίες συμβαίνουν με αποτέλεσμα το θύμα να μην αντιλαμβάνεται την κατάσταση.

Το «Διαδικτυακό Έγκλημα» πήρε τεράστιες διαστάσεις και ο κάθε οργανισμός και μεμονωμένος χρήστης πρέπει να ενημερωθεί για τους κινδύνους και τους τρόπους με τους οποίους θα προστατευθεί ο ίδιος και το πληροφοριακό του σύστημα από κάθε είδους κακόβουλη απειλή

ΠΕΡΙΛΗΨΗ

Με τις τεχνολογίες της πληροφορίας, το διαδίκτυο και οι τεχνολογίες των επικοινωνιών να εισχωρούν ολοένα και περισσότερο στην καθημερινότητα μας, πολλαπλασιάζονται, όχι μόνο οι ευκαιρίες και οι δυνατότητες για τους πολίτες και τις επιχειρήσεις, αλλά και οι κίνδυνοι εμφάνισης διαφόρων εγκληματικών δραστηριοτήτων.

Τα νέα δεδομένα που προκύπτουν από την ραγδαία ανάπτυξη της επιστήμης της πληροφορικής καθώς και η κυριαρχία της πληροφορικής τεχνολογίας, οδήγησαν στην εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς, που διαφοροποιούνται σημαντικά μεταξύ τους.

Σύμφωνα με τη Δίωξη του Ηλεκτρονικού Εγκλήματος, ως διαδικτυακό έγκλημα «θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία».

Αξίζει να σημειωθεί ότι στην ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη ποινικού δικαίου.

Από τη δεκαετία του 1970 ήδη παρουσιάστηκε η εγκληματικότητα μέσω των ηλεκτρονικών υπολογιστών ως φαινόμενο που άπτεται του ποινικού ενδιαφέροντος, γεγονός που οδήγησε σταδιακά στη λήψη ειδικών ποινικών νομοθετικών μέτρων. Τα τελευταία χρόνια όμως έκαναν την εμφάνισή τους και περιπτώσεις κατάχρησης του κυβερνοχώρου που δεν παρουσιάζουν πάντα τα χαρακτηριστικά της εγκληματικότητας μέσω των ηλεκτρονικών υπολογιστών.

Έχουν γίνει πολλές προσπάθειες κατά καιρούς ώστε να ορισθεί το διαδικτυακό έγκλημα. Οι ForesterandMorrison την χρονολογία του 1994 έδωσαν έναν ορισμό ο οποίος προσδιόρισε το διαδικτυακό έγκλημα ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Παρ' όλα αυτά, το διαδικτυακό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το διαδικτυακό έγκλημα ποικίλουν: e-crime, cybercrime, computercrime, internetrelatedcrime, και, hitech-crime.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι διαδικτυακό έγκλημα, ηλεκτρονικό έγκλημα και έγκλημα του κυβερνοχώρου. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους. Βασικό συστατικό στοιχείο του διαδικτυακού εγκλήματος αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως είναι ο ηλεκτρονικός υπολογιστής. Η εξάπλωση της πληροφορικής τεχνολογίας και η δυνατότητα πρόσβασης σε αυτήν, καθιστούν το διαδικτυακό έγκλημα μία πρόκληση για την εγκληματολογία, την κοινωνιολογία και επιβάλλουν την κοινωνική αγωγή, ειδικότερα του χρήστη της τεχνολογίας.

ABSTRACT

With information technologies, the Internet and communication technologies becoming more and more in our everyday life, not only opportunities and opportunities for citizens and businesses, but also the risks of various criminal activities are multiplied.

The new data emerging from the rapid development of computer science and the dominance of information technology have led to the emergence of new forms of criminal behavior that differ greatly from one another.

According to the Prosecution of Electronic Crime, "criminal offense" means criminal offenses committed with the use of computers and data processing systems and punished by specific penalties under Greek law.

It is worth noting that in Greek law there is no law that deals exclusively with Internet issues and regulates the behavior of Internet users in terms of criminal law.

Since the 1970s, computer crime has already been presented as a criminal phenomenon, which has gradually led to specific criminal law measures. In recent years, however, they have also emerged cyber-abuse cases that do not always present the characteristics of crime through computers.

Many attempts have been made at times to define online crime. Forester and Morrison in 1994 gave a definition that identified online crime as "a criminal act in which the computer is used as its principal agent". Nonetheless, online crime is not so simple, nor can we generalize it. In English, the terms used to describe cybercrime vary: e-crime, cybercrime, computer crime, internet related crime, and hitech-crime.

Similarly, in Greek, the terms used are online crime, cybercrime and cybercrime. The element of networking is included in the last two terms. A key component of the internet crime is the existence of an electronic data-processing device, such as a computer. The spread of information technology and the ability to access it make online crime a challenge for criminology, sociology, and impose social education, in particular the technology user.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Διαδικτυακή Εγκληματικότητα, Διαδίκτυο, Έγκλημα, Μορφές, Πρόληψη, Τρόποι Αντιμετώπισης, Νομοθεσία.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει ευρύτατες και πολύ σημαντικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων της σύγχρονης κοινωνίας, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής του σύγχρονου ανθρώπου, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας, στις οποίες βασικό ρόλο έχει ο ηλεκτρονικός υπολογιστής (Η/Υ) θεσμοθετούνται με τον όρο «Διαδικτυακό Έγκλημα», ενώ πλέον τις περισσότερες φορές το έγκλημα τελείται μέσω του διαδικτύου, οπότε μιλάμε για το «Ηλεκτρονικό Διαδικτυακό Έγκλημα».

Στην παρούσα πτυχιακή εργασία θα ασχοληθούμε αναλυτικά με το διαδικτυακό έγκλημα, με τις μορφές του ηλεκτρονικού εγκλήματος, καθώς και για την νομοθεσία.

Στο ***1ο κεφάλαιο*** ορίζονται οι έννοιες του εγκλήματος και του διαδικτύου ξεχωριστά. Στη συνέχεια του ίδιου κεφαλαίου, παρουσιάζονται τα κύρια χαρακτηριστικά της Διαδικτυακής Εγκληματικότητας καθώς και η ιστορική εξέλιξη.

Στο ***2ο κεφάλαιο***, αναλύονται διεξοδικά οι απειλές της διαδικτυακής εγκληματικότητας, καθώς και οι τρόποι αντιμετώπισης και τα μέτρα πρόληψης που μπορούν να παραχθούν.

Στο***3ο κεφάλαιο***, γίνεται αναφορά σε νομοθετικά ζητήματα γύρω από τη διαδικτυακή εγκληματικότητα.

Στο ***4ο κεφάλαιο***, γίνεται αναφορά σε μελέτες περίπτωση στο διαδικτυακό έγκλημα

Στο ***5ο κεφάλαιο,*** παρουσιάζεται το ερωτηματολόγιομε βάση την έρευνα που έγινε σε διάφορους χρήστες όλων την ηλικιών.

1 ΔΙΕΡΕΥΝΩΝΤΑΣ ΤΗΝ ΔΙΑΔΙΚΤΥΑΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ

1.1 Ιστορική Αναδρομή του Εγκλήματος

Τον 18^{ο} αιώνα η βιομηχανική επανάσταση, έφτασε στο αποκορύφωμά της στις δύο πρώτες δεκαετίες του 19^{ου} αιώνα και έθεσε τις βάσεις για την πρώτη διεθνή κοινωνία και το μετασχηματισμό της ανθρωπότητας σε κοινωνικούς σχηματισμούς με εθνικά κράτη που ανταλλάσσουν μεταξύ τους μαζικής παραγωγής τυποποιημένα εμπορεύματα. Σε πολύ σύντομο χρονικό διάστημα μετά τον 2^{ο} παγκόσμιο πόλεμο, μέσα σε δύο γενιές, άρχισε να εξελίσσεται η πληροφορική επανάσταση. Η διάδοση καθώς και η ταχύτητα ανάπτυξης και η εφαρμογή της πληροφορικής προσφέρει σημαντικά πλεονεκτήματα σε πολλαπλούς τομείς της κοινωνικής ζωής, έτσι αυτό είχε ως αποτέλεσμα σήμερα να γίνεται λόγος για μία αυξανόμενη εξάρτηση του κράτους, της οικονομίας αλλά και της παιδείας και του πολιτισμού από την πληροφορική (Τσουραμάνης, 2005). *Ο Edwards (1995)* αναφέρει ότι, η σύγχρονη κοινωνία τείνει να φθάσει στο σημείο όπου τα πάντα θα εξαρτώνται από τα λογισμικά. Ο κύριος όγκος των πληροφοριών κάθε είδους που διακινούνται καθημερινά στον πλανήτη μας, μεταβιβάζεται μέσω των συστημάτων της πληροφορικής. Αλλά και αντίστροφα, κάθε πληροφορία, άξια λόγου, τείνει να θεωρείται η πληροφορία που μπορεί να μεταβιβασθεί μέσω των συστημάτων αυτών. Η έρευνα στη γενετική και στην υγεία καθώς και η εφαρμογή τους, ο έλεγχος των συγκοινωνιών σε διεθνή και εθνική κλίμακα, η εθνική άμυνα και η λειτουργία του κρατικού μηχανισμού εξαρτώνται από τις εφαρμογές της τεχνολογίας της πληροφορικής. Για τον κύριο όγκο των χρηματικών συναλλαγών μεταξύ των επιχειρήσεων και τη διαχείριση των οικονομικών τους μεγεθών ισχύει επίσης το ίδιο. Όλο και πιο συχνά, ο η ρύθμιση και ο έλεγχος της παραγωγικής διαδικασίας μιας επιχείρησης εξαρτάται απόλυτα από τη λειτουργική ικανότητα του συστήματος επεξεργασίας των δεδομένων (data-processingsystem) που διαθέτει.

Η πληροφοριακή επανάσταση αποτελεί μια κοινωνική σχέση και ένα εργαλείο που έχουν ως κύριο στόχο να παραμείνουν στην κοινωνία με όλα της τα υλικά (hardware) και άυλα (software) συστατικά.

Η προσπάθεια ελέγχου της χρήσης της ως μέσου και ως πεδίου της τέλεσης των εγκλημάτων, είναι μία προσπάθεια ελέγχου της πληροφορικής επανάστασης. Έτσι, δεν είναι δυνατό να αντιμετωπιστούν οι κίνδυνοι από την ανάπτυξη της πληροφορικής τεχνολογίας. Η προσπάθεια αυτή όμως είναι αναγκαία.

Η επανάσταση της πληροφορικής δεν περιορίζεται σε τεχνολογικά ζητήματα και αποφάσεις, όπως αυτά που κατανοούνται και ορίζονται είτε από τους ειδικούς, είτε από τα κράτη, ή ακόμα και από ιδιωτικές επιχειρήσεις. Ο Hughes την χρονολογία του 1880 έως το 1930, αναφέρει ότι η τεχνολογία προωθείται σε ένα ευρύ κοινωνικό μέτωπο. Η εφεύρεση μιας καινοτομίας δεν συμπίπτει αναγκαστικά με την πρακτική αποδοχή της. Η εφεύρεση ενός νέου τρόπου οργάνωσης ή διαχείρισης των ανθρώπων, των πραγμάτων και των συμβόλων δεν συνιστά κάτι παραπάνω από μία πρόταση η οποία να απευθύνεται στην κοινωνία. Η πρακτική και η αφομοίωση αυτής της εφαρμογής της καινοτομίας αποτελεί προϊόν πολυέξοδων, πολύπλοκων, καθώς και χρονοβόρων διευθετήσεων οι οποίες δεν λαβαίνουν χώρα μόνο στο τεχνολογικό επίπεδο, αλλά και στο οικονομικό, κοινωνικό, πολιτικό, πολιτιστικό, ακόμα και στο ηθικό αξιακό επίπεδο (Λάζος, 2001).

Οι καινοτομίες και οι τεχνολογικές εξελίξεις δημιουργούν προβλήματα μέχρι να ενσωματωθούν στα επικρατούντα πρότυπα των κοινωνικών σχέσεων και της κοινωνικής

εξουσίας και μέχρι να μορφοποιηθούν με τρόπους που θα αμβλύνουν ή θα ελαχιστοποιηθούν τις προοπτικές διάσπασης αυτών των προτύπων (Λάζος, 2001).

Έτσι συντάσσεται η πλειονότητα των επιστημόνων οι οποίοι ασχολούνται με το πληροφοριακό έγκλημα, νομικοί, εγκληματολόγοι και κοινωνιολόγοι όπως είναι η Nelson, oHollinger, oMeier και ο Thomas συνιστούν την προσοχή σε μία πολύ σημαντική εκκρεμότητα: η κοινωνία δεν έχει ακόμη αποφασίσει ως προς τις ηθικές και τις πολιτιστικές συντεταγμένες των σχέσεων που δημιουργήθηκαν με την ταχύτατη ανάπτυξη των νέων τεχνολογιών, δεν έχει αποφασίσει ως προς το τι είναι πληροφορική κακοχρησία και τι είναι το πληροφορικό έγκλημα. Ο νόμος δεν έρχεται τόσο να επικυρώσει κάποια κοινά συμφωνημένα ηθικά και πολιτιστικά πρότυπα για τις σχέσεις και τη χρήση της πληροφορικής, αλλά μάλλον να επιβάλλει τα όρια στα οποία τα πρότυπα αυτά θα πρέπει να αναπτυχθούν (Λάζος, 2001)

1.2 Ορισμός του Εγκλήματος

Ένα ανυπόστατο κομμάτι κάθε κοινωνίας είναι το έγκλημα, το οποίο συμπεριφέρεται σαν ένας ζωντανός οργανισμός που διαρκώς οι μορφές του μεταβάλλονται, τα μέσα διάπραξης καθώς και η νομοθεσία που το διέπει. Ανάλογα με τις πολιτικές, τις κοινωνικές και τις ηθικές τάσεις κάθε εποχής το έγκλημα με διαφορετικό περιτύλιγμα αλλά και με ουσία πολλές φορές, παραμένει παρόν, κινούμενο πάντα σε τρείς βασικούς άξονες, με τα απαραίτητα συστατικά στοιχεία του, αυτά που το ορίζουν. Ποια είναι όμως αυτά τα στοιχεία; (Μανωλεδάκης, 2005).

Το φαινόμενο του εγκλήματος εμφανίζεται στον κοινωνικό χώρο ως σύνθεση των παρακάτω στοιχείων που παρουσιάζονται στον *Πίνακα 1:*

Πίνακας 1-1ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ

Κοινωνικό Αγαθό	Προσβολή Κοινωνικού Αγαθού	Αντίδρασηστην Προσβολή
Α.Υλικό αντικείμενο, φυσική ιδιότητα υλικού αντικειμένου ή κοινωνική ιδιότητα υλικού αντικειμένου.	Συμπεριφορά που θίγει την ύλη ή αναιρεί ή αλλοιώνει τις φυσικές ή κοινωνικές ιδιότητες των κοινωνικών αγαθών	Οργανωμενη η κοινωνική αντίδραση με προσβολή αγαθών του δράστη και έντονα στοιχεία αποδοκιμασίας και στιγματισμού.

(Μανωλεδάκης, 2005, σελ. 65).

Το φαινόμενο του εγκλήματος αποτελεί κοινωνικό και ιστορικό φαινόμενο, διότι ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Έτσι τα χαρακτηριστικά του, όπως είναι τα κοινωνικά αγαθά, το έγκλημα και η ποινή έχουν και αυτά ιστορικότητα, δηλαδή σχετικότητα, διαφοροποιούμενα από εποχή σε εποχή και από τόπο σε τόπο (Μανωλεδάκης, 2005).

Σημαντικό ρόλο και μάλιστα ευκαταφρόνητο σχετικά με το εγκληματικό φαινόμενο είναι η διαχρονικότητα του στο πέρασμα των αιώνων. Αν και σε κάθε έγκλημα, υπήρχε, υπάρχει και θα υπάρχει ποινή , απεναντίας καμία κοινωνία δεν μπορεί να απαλλαχθεί από αυτό. Συνήθως, αυτό που παρατηρείται είναι μια συνεχής αύξηση του εγκληματικού φαινομένου και συγχρόνως η εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς (Μανωλεδάκης, 2005).

Υπάρχουν άνθρωποι που θεσπίστηκαν τυπικά ή άτυπα προκειμένου να διαφυλαχθούν από τα κοινωνικά αγαθά, που παραβαίνουν τους κοινωνικούς κανόνες. Το αποτέλεσμα της προσβολής των αγαθών αυτών είναι η επιβολή διαφόρων κυρώσεων στους παραβάτες. Η ποινή ή αλλιώς επιβληθείσα κύρωση θα μπορούσαμε να πούμε ότι αποτελεί τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Το είδος και η αντίδραση της ποινής, απευθύνεται στον παραβάτη των κοινωνικών κανόνων και βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό (Πιπερόπουλος, 1998).

Το έγκλημα είναι αναμενόμενο στα πλαίσια της κοινωνικής πραγματικότητας. Είναι το βαθύ σημάδι μιας κοινωνίας που γερνά, το εμφανές σύμπτωμα της κοινωνικής κρίσης, της διάρρηξης του κοινωνικού ιστού. Όπως αναφερθήκαμε και παραπάνω υπάρχουν οι κανόνες οι οποίοι ρυθμίζουν την ομαλή συμβίωση των μελών μιας οργανωμένης κοινωνίας. Παρ' όλα αυτά είναι αδύνατον όλα τα μέλη να συμμορφώνονται με τους ίδιους κανόνες, διότι η τήρηση τους είναι στενά συνδεδεμένη και με τη διαφορετική προσωπικότητα του κάθε ατόμου (Πιπερόπουλος, 1998).

Τα κύρια στοιχεία του εγκληματικού φαινομένου, όπως για παράδειγμα είναι ο κανόνας, το έγκλημα και η κύρωση, αποτελούν μεταξύ τους έναν αδιάσπαστο κύκλο. Εδώ είναι ξεκάθαρη η αλληλεξάρτηση των στοιχείων. Η κύρωση δεν υφίσταται αν δεν υπήρχε έγκλημα. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή την παράβασή του. Ο κανόνας δημιουργήθηκε για να προστατέψει και να οργανώσει τα κοινωνικά αγαθά από κάθε προσβολή τους μέσα στα πλαίσια της κοινωνικής συμβίωσης. Έπειτα, και αφού επέλθει η προσβολή του έννομου αγαθού (δηλαδή, αυτό που προστατεύεται από τον κανόνα – νόμο), έρχεται η κύρωση (ποινή). Η κύρωση με λίγα λόγια ονομάζεται η συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή στην κοινωνία. Ωστόσο, η ποινή αποτελεί την εκτόνωση της κοινωνικής αντίδρασης στο έγκλημα. Μπορεί δε, να εμφανιστεί με πολλούς διαφορετικούς τρόπους, όσον αφορά την ιδεολογική της προσέγγιση, όπως ως αποκατάσταση της διαταραχθείσας από το έγκλημα της κοινωνικής τάξης ή ως μέσο για την ηθική βελτίωση του παραβάτη (Πιπερόπουλος, 1998).

1.3 Ορισμός του Διαδικτύου

Ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, θα μπορούσαμε να περιγράψουμε το διαδίκτυο (internet) το οποίο διασύνδεει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων (Ζάννη, 2005).

Είναι ένας εικονικός, απέραντος, κόσμος στον οποίο μπορούν εύκολα να έχουν πρόσβαση χρήστες οποιαδήποτε ηλικίας. Με την μορφή που κυριαρχεί πλέον στις μέρες μας (WorldWideWeb – www), εισέβαλε στη ζωή μας πριν από 20 περίπου χρόνια, αλλάζοντας ριζικά την πλειοψηφία των ανθρώπινων δραστηριοτήτων. Οι ηλεκτρονικοί υπολογιστές (Η/Υ), και κατ' επέκταση το διαδίκτυο έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητάς μας, τόσο ως μέσα ενημέρωσης, ψυχαγωγίας, όσο και το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης των επαγγελματικών υποχρεώσεων και των δραστηριοτήτων (Ζάννη, 2005).

Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες των πληροφοριών/δεδομένων που καθημερινά μεταδίδονται, επεξεργάζονται, διαδίδονται και είναι ανυπολόγιστες σε αριθμό αλλά και σε όγκο (Ελαφρός, 2006).

1.4 Ορισμός Διαδικτυακού Εγκλήματος

Ως «Διαδικτυακό Έγκλημα» ορίζονται όλες οι αξιόποινες πράξεις που τελούνται με τη χρήση των ηλεκτρονικών υπολογιστών και των συστημάτων επεξεργασίας (Σφακιανάκης, 2007).

Ανάλογα με τον τρόπο διάπραξης του διαδικτυακού εγκλήματος, διαχωρίζεται σε έγκλημα τελούμενο με τη χρήση του ηλεκτρονικού υπολογιστή (computercrime) και σε κυβερνοέγκλημα (cybercrime), αν τελεσθεί μέσω διαδικτύου (Σφακιανάκης, 2007).

Τα πεδία δράσης για την τέλεση των διαδικτυακών εγκλημάτων είναι (Σφακιανάκης, 2007):

- τα εταιρικά δίκτυα,
- τα δίκτυα κινητής τηλεφωνίας,
- τα δίκτυα τραπεζών, και,
- το διαδίκτυο

Άλλωστε το «έγκλημα» παραμένει έγκλημα ακόμα και όταν πραγματοποιείται ηλεκτρονικά (Παπαντωνίου, 2007).

Τα συνηθέστερα διαδικτυακά εγκλήματα μέσω του Internet, είναι:

- Η απάτη (Άρθρο 386 και 386Α Ποινικού Κώδικα)
- Η παραβίαση δεδομένων προσωπικού χαρακτήρα (Νόμος 2472/97)
- Η παραβίαση απορρήτων (Άρθρο 370Γ Ποινικού Κώδικα)
- Η καταστρατήγηση πνευματικής ιδιοκτησίας (Νόμος 2121/1993)
- Τα εγκλήματα κατά της τιμής και της αξιοπρέπειας (Άρθρο 361)
- Η διακίνηση υλικού παιδικής πορνογραφίας (Άρθρο 348Α Ποινικού Κώδικα) (Παπαντωνίου, 2007).

1.5 Χαρακτηριστικά της Διαδικτυακής Εγκληματικότητας

Ο όρος διαδικτυακό έγκλημα, χρησιμοποιείται όλο και πιο συχνά, καθώς η νέα αυτή μορφή εγκλήματος φέρει ορισμένα ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το κοινό έγκλημα (Ζάννη, 2005).

1. Είναι γεγονός ότι το διαδικτυακό έγκλημα διαπράττεται άμεσα, σε ελάχιστα δευτερόλεπτα και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Ο επιτιθέμενος με την χρήση ενός ηλεκτρονικού υπολογιστή συνδεδεμένος στο διαδίκτυο, μπορεί να εισβάλει στα υπολογιστικά συστήματα ενός οργανισμού ή μιας επιχείρησης σε οποιοδήποτε σημείο του κόσμου. Δεν απαιτείται η φυσική μετακίνηση του, καθώς οι ενέργειες μπορούν να ολοκληρωθούν είτε από την οικία του είτε σε άλλο χώρο, με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή (Ζάννη, 2005).
2. Φαινομενικά, η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολο. Ωστόσο, η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επίθεσης, αποτελεί πλέον μύθο. Στο διαδίκτυο υπάρχουν ελεύθερες εφαρμογές λογισμικού, οι οποίες επιτρέπουν στους επίδοξους hackers να εισβάλλουν σε δίκτυα και σε υπολογιστικά συστήματα, τη διασπορά ιών και την πραγματοποίηση πλήθους άλλων ηλεκτρονικών επιθέσεων, καθιστώντας περισσότερο εύκολη την διάπραξη του διαδικτυακού εγκλήματος σε σχέση με το κοινό – συμβατικό (Ζάννη, 2005).
3. Επιπλέον, μπορεί να διαπραχθεί χωρίς τη φυσική μετακίνηση του δράστη. Το διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο (e-mail), τα δωμάτια συζητήσεων (chatrooms) και οι ομάδες ειδήσεων (newsgroups), επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα. Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων, όπως για παράδειγμα είναι η παιδοφιλία, η παιδική πορνογραφία και η ανεπιθύμητη αλληλογραφία (spamming). Στις περιπτώσεις αυτές, τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών επικοινωνίας , που προσφέρει το Διαδίκτυο (Ζάννη, 2005).
4. Είναι έγκλημα «χωρίς πατρίδα». Πολλές φορές για να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος, καθίσταται αδύνατο διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου, αρκεί να έχει στην διάθεση του έναν ηλεκτρονικό υπολογιστή.

5. Επιπρόσθετα, είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσης τους, καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από τον χρόνο κατά τον οποίο αυτό συνέβη. Επίσης, συχνά είναι δυνατή η διαγραφή από τον εισβολέα των «ιχνών» του ηλεκτρονικού εγκλήματος κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευση του (Ζάννη, 2005).
6. Σε μια διαδικτυακή έρευνα, συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (δηλαδή του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία), τα δε αρμόδια όργανα των διωκτικών αρχών πρέπει να κατέχουν εξειδικευμένες γνώσεις και να εκπαιδεύονται συνεχώς στις νέες τεχνολογικές εξελίξεις. Σε ορισμένες περιπτώσεις, τέτοιου είδους γνώσεις απαιτείται να κατέχουν και όσοι άλλοι ασχολούνται με τη δίωξη του ηλεκτρονικού εγκλήματος όπως δικαστές, εισαγγελείς και δικηγόροι (Ζάννη, 2005).
7. Δυστυχώς δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον Ελληνικό αλλά και στον Διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του διαδικτύου καταγγέλλονται, και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων, οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια, οι διαστάσεις της εγκληματικότητας στο χώρο του διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον «κοινό» εγκληματικό χώρο (Ζάννη, 2005).

1.6 Τα Χαρακτηριστικά του Ηλεκτρονικού Εγκληματία (Hacker)

Πλέον οι δικαστικές αποφάσεις αφορούν κυρίως εγκλήματα που τελούνται με ηλεκτρονικούς υπολογιστές (computercrimes) και όχι αποκλειστικά εγκλήματα του κυβερνοχώρου (cybercrimes) (HollingerRichard, 1997).

Το διαδικτυακό έγκλημα είναι γρήγορο από άποψη χρόνου τέλεσης και ολοκλήρωσης του και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Είναι εύκολο και ανέξοδο στη διάπραξή του, για όσους διαθέτουν τον κατάλληλο εξοπλισμό και τις απαραίτητες γνώσεις πληροφορικής (HollingerRichard, 1997).

Δεν απαιτεί τη φυσική μετακίνηση του δράστη, ο οποίος μπορεί να πλήττει, πολλαπλούς στόχους, από τον υπολογιστή του σπιτιού ή του γραφείου του (HollingerRichard, 1997).

Είναι διασυνοριακό έγκλημα, «χωρίς πατρίδα» και οι συνέπειες του μπορεί να πραγματοποιούνται ταυτόχρονα σε διαφορετικές χώρες, ενώ είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεώς του καθιστώντας αρκετά δύσκολη τη διερεύνηση του και τον εντοπισμό του δράστη (HollingerRichard, 1997).

Οι εγκληματίες του διαδικτυακού εγκλήματος ειδικότερα, πολλές φορές χρησιμοποιούν εικονική ταυτότητα και ψεύτικα στοιχεία χωρίς να εμφανίζονται με την πραγματική τους ταυτότητα (HollingerRichard, 1997).

Για τη διερεύνησή του εγκλήματος στο διαδίκτυο απαιτείται συνεργασία των αρχών δύο ή περισσότερων κρατών, συνήθως του κράτους στο οποίο εκδηλώνεται αρχικά το έγκλημα και του κράτους όπου πιθανά βρίσκονται τα αποδεικτικά στοιχεία (HollingerRichard, 1997).

Ο «σκοτεινός αριθμός» της διαδικτυακής εγκληματικότητας είναι μεγαλύτερος από ότι είναι για το «κοινό» έγκλημα. Τα στατιστικά στοιχεία δεν είναι επαρκή τόσο για τον Ελληνικό, όσο και για τον Διεθνή χώρο επειδή είναι ελάχιστες οι περιπτώσεις των διαδικτυακών εγκλημάτων που καταγγέλλονται. Όπως και για το έγκλημα του λευκού περιλαιμίου η απροθυμία καταγγελίας, ειδικά από τα θύματα, οφείλεται στην προσπάθεια να μην αμφισβητείται η αξιοπιστία τους, οι οποίοι κατά κανόνα είναι εταιρείες (HollingerRichard, 1997).

Η αστυνομική διερεύνησή του είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις απαιτούνται και όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (δικαστές, εισαγγελείς, δικηγόρους) (HollingerRichard, 1997).

1.6.1 Τα Κίνητρα του Δράστη Διαδικτυακού Εγκλήματος

Ο δικηγόρος και διευθυντής του Εθνικού Κέντρου Δεδομένων για το Πληροφορικό Έγκλημα (NationalCenterforComputerData) Bloombecker, ασχολήθηκε κυρίως με την κατηγοριοποίηση των μορφών του διαδικτυακού εγκλήματος σε σχέση με τα κίνητρα των δραστών του (HollingerRichardC., 1997). Θεωρούσε την ευαισθησία της ασφάλειας των υπολογιστικών δικτύων επικοινωνίας ως τη πιο σημαντική εξέλιξη στον τομέα της ασφάλειας των υπολογιστών. Στην αναφορά του ComputerCrime, ComputerSecurity, ComputerEthics, το 1986, επισήμανε ότι η εστίαση αποκλειστικά στους οικονομικούς κινδύνους οι οποίοι προέρχονται από την δράση των hackers, άφηνε κενά ασφάλειας και θα έπρεπε να δοθεί η απαραίτητη προσοχή σε όλες τις μορφές του διαδικτυακού εγκλήματος επειδή οι εγκληματίες υπολογιστών δεν είναι απαραίτητα ιδιοφυές στους υπολογιστές και διακρίνονται ολοένα και λιγότερο από τους κοινούς εγκληματίες, ενώ θύμα τους θα μπορούσε να αποτελέσει ο καθένας(BloomBecker, 1997).

Ο Πίνακας 1.2 απεικονίζει τα συνήθη κίνητρα του δράστη διαδικτυακού εγκλήματος (Shinder, 2002).

Πίνακας 1-2Κίνητρα του δράστη διαδικτυακού εγκλήματος

Απλή Διασκέδαση	Αυτό το κίνητρο, σύμφωνα με τον J. Maxwell, δεν αφορά την επιδίωξη κανενός είδους οικονομικού οφέλους αλλά αφορά κυρίως τους νεαρούς hacker, που αντιμετωπίζουν το διαδίκτυο με διάθεση για παιχνίδι και που αντίθετα μπορεί να αποτελεί ένα ακριβό χόμπι που απαιτεί τη χρήση εξελιγμένων υπολογιστικών συστημάτων.
Οικονομικό Κέρδος	Αποτελεί το συνηθέστερο κίνητρο του τυπικού ηλεκτρονικό – οικονομικού εγκληματία που αποκτά παράνομη πρόσβαση σε υπολογιστικά συστήματα για να αποκομίσει κάποιο χρηματικό κέρδος. Περικλείει αρκετές επιμέρους μορφές οικονομικών εγκλημάτων όπως η κατάχρηση, η βιομηχανική κατασκοπεία, ακόμα και η μίσθωση των υπηρεσιών του σε άλλους για παράνομη διαδικτυακή δράση. Οι εγκληματίες του λευκού περιλαιμίου αυτής της περίπτωσης είναι μορφωμένοι, επαγγελματίες σε επαγγελματική αδράνεια ή καταστροφή
Κάλυψη Συναισθηματικών Αλλαγών (θυμός, εκδίκηση, απόκτηση αναγνώρισης, κύρους και προσοχής	Οι εγκληματίες στο διαδίκτυο που δρουν από εκδίκηση ή θυμό είναι κυρίως απογοητευμένοι εραστές ή σύζυγοι, απολυμένοι υπάλληλοι, συνεργάτες που αισθάνονται εξαπατημένοι ή άλλοι που πιστεύουν ότι έχουν υποστεί κάποια αδικία ή κακό. Τα διαδικτυακά εγκλήματα με τέτοια κίνητρα μπορεί να είναι κυβερνο-τρομοκράτηση, απειλές, δυσφήμιση, διασπορά ιών, επιθέσεις άρνησης υπηρεσιών κλπ
Πολιτικά Κίνητρα	Οι επιθέσεις σε ιστοσελίδες και δίκτυα κάθε είδους εξτρεμιστών ή τρομοκρατών που προσπαθούν να διασπείρουν προπαγάνδα και μίσος, να επιτεθούν σε κυβερνητικές υπηρεσίες, να αποκομίσουν κέρδη για την χρηματοδότηση ή τον προγραμματισμό

	της δράσης τους.
Σεξουαλικά Κίνητρα	Τέτοια είναι αυτά των παιδόφιλων που λαμβάνουν ή διακινούν υλικό παιδικής πορνογραφίας, που προσεγγίσουν παιδιά με σκοπό την προσέλκυση τους σε φυσική συνάντηση, δολοφόνων και βιαστών που μέσω της γνωριμίας με τα υποψήφια θύματα στο διαδίκτυο αποκτούν την εμπιστοσύνη τους και αφού τα συναντήσουν στον φυσικό κόσμο τα βιάζουν ή/και τα δολοφονούν
Ψυχικές Ασθένειες (όπως σχιζοφρένεια, παράνοια, παραισθήσεις και άλλες σοβαρές ψυχικές διαταραχές)	Αυτά τα άτομα είναι ευκολότερο να καλύψουν την ασθένεια από τους άλλους στο ψηφιακό που δεν υπάρχει φυσική επαφή παρά στο φυσικό περιβάλλον όπου θα ήταν άμεσα αντιληπτοί.

(Shinder, 2002, σελ. 124).

Στον Πίνακα 1-3 Παρουσιάζονται οι Τύποι Διαδικτυακών Εγκλημάτων με βάση το κίνητρο.

Πίνακας 1-3 Τύποι Διαδικτυακών Εγκλημάτων με βάση το κίνητρο.

1. Κλοπή χρημάτων	(45% για το '86 και 36% για το ’88)
2. Κλοπή πληροφοριών	(16% και 12% αντίστοιχα)
3. Ζημία σε λογισμικό	(16% και 2%)
4. Κακόβουλη αλλοίωση	(6% και 6%)
5. Αλλοίωση για απάτη	(6% και 2%)
6. Κλοπή υπηρεσιών	(10% και 34%)
7. Παρενόχληση	(0% και 2%)
8. Εκβιασμός	(0% και 4%)

(BloomBecker, 1997, σελ. 87).

Εδώ μπορούμε να παρατηρήσουμε ότι τόσο η συσχέτιση όσο και η ταύτιση των κατηγοριών του διαδικτυακού εγκλήματος με αυτές των κινήτρων που οδηγούν τους κάθε είδους δράστες στη διάπραξή τους, χωρίς να δίδεται ο απαραίτητος ορισμός, μάλλον προκαλούν εννοιολογικές και ταξινομικές συγχύσεις, παρά να συμβάλλουν στην ομαλή διεξαγωγή κάθε ασφαλούς διαλόγου και προβληματισμού. Αμφισβητήσιμο είναι μάλλον το κατά πόσο ένα ποσοστό της τάξης του 0 έως 2% μπορεί να οδηγήσει τον θεωρητικό στον σχηματισμό μιας διακριτής και στατιστικά σημαντικής κατηγορίας. Αμφισβητήσιμη είναι επίσης, η παραπάνω κατηγοριοποίηση που πρότεινε ο Bloombecker «σε σχέση με τα κίνητρα» καθώς φαίνεται να συγχέονται τα κίνητρα με το στόχο του εγκλήματος (Λάζος, 2001).

Στη συνέχεια, ο Bloombecker, αναγνωρίζοντας ότι ο δραστικός περιορισμός του διαδικτυακού εγκλήματος αποτελεί μάλλον μία ουτοπία, προσπαθεί να εστιάσει την προσοχή των ενδιαφερόμενων μερών, όχι τόσο στη νομοθεσία, αλλά στην επαύξηση των μέτρων ασφαλείας με διαρκή ενημέρωση των υπεύθυνων συστημάτων ασφάλειας, ιδιαίτερα από τους πιο ειδικευμένους στο αντικείμενο που δεν είναι άλλοι από τους ίδιους τους παραβάτες.

Ο Hayes υποστηρίζει ότι τα διαδικτυακά εγκλήματα υποδηλώνουν τη δύναμη εκατομμυρίων εργαζομένων να προωθήσουν τα πολιτικά τους συμφέροντα απέναντι στους απανταχού εργοδότες (Λάζος, 2001).

2. ΑΠΕΙΛΕΣ ΤΗΣ ΔΙΑΔΙΚΤΥΑΚΗΣΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

Εισαγωγή

Οι μορφές του Διαδικτυακού Εγκλήματος είναι ποικίλες και με την συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για αυτό τον λόγο, ρυθμίζονται και τιμωρούνται ξεχωριστά από άλλα ειδικότερα νομοθετήματα τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση (Ε.Ε.) όσο και στο διεθνή χώρο γενικότερα.

2.1 Οικονομικό Έγκλημα

Ο κύριος όγκος των πληροφορικών εγκλημάτων εντάσσεται στην υποκατηγορία των πληροφορικών οικονομικών εγκλημάτων. Πιο συγκεκριμένα, τα πληροφορικά οικονομικά εγκλήματα απαρτίζουν, τον κύριο όγκο των διαπιστωμένων πληροφορικών εγκλημάτων και τα εγκλήματα που τραβούν την προσοχή της πλειονότητας των ερευνητών του πληροφορικού εγκλήματος. Στη διεθνή βιβλιογραφία, αναφέρεται η αναλογία μεταξύ των διαφόρων υποκατηγοριών του πληροφορικού εγκλήματος που απασχολούν τους ειδικούς είναι χαρακτηριστική: σε κάθε δώδεκα περιπτώσεις πληροφορικού οικονομικού εγκλήματος αναλογεί μόλις μία περίπτωση των άλλων κατηγοριών (Λάζος, 2001).

Ένας παράγοντας που συμβάλλει σε αυτή τη δυσαναλογία ως προς ενδιαφέρον αποτελεί το ευκολότερο διαπιστώσιμο, το «χειροπιαστό», του πληροφορικού οικονομικού εγκλήματος (Λάζος, 2001).

Ένας δεύτερος παράγοντας, είναι το γεγονός ότι μεγάλο ενδιαφέρον έχουν δείξει οι ίδιες οι επιχειρήσεις για αυτό τον τύπο πληροφορικού εγκλήματος και έχουν διαθέσει πολύ σημαντικούς πόρους για τη διερεύνησή του. Συνεπώς, η ισχύς των επιχειρήσεων συμβάλλει στην αύξηση της αντιπροσώπευσης του πληροφοριακού οικονομικού εγκλήματος μέσα στο ευρύτερο πληροφοριακό έγκλημα (Λάζος, 2001).

Ένας τρίτος παράγοντας είναι, ότι συχνά το πληροφορικό οικονομικό έγκλημα είναι ευκολότερα ανακοινώσιμο, σε σύγκριση με μία σημαντική μερίδα υπερατομικών πληροφορικών εγκλημάτων όπως για παράδειγμα είναι οι περιπτώσεις κατασκοπείας (Λάζος, 2001).

Η απάτη μέσω του ηλεκτρονικού υπολογιστή (Η/Υ) στο πλαίσιο των πληροφορικών οικονομικών εγκλημάτων περιλαμβάνει την παραποίηση κάποιων πληροφοριών ή δεδομένων ή σε προγράμματα με κύριο σκοπό το οικονομικό κέρδος (Λάζος, 2001).

Συγκεκριμένα, αφορά κυρίως στην διαγραφή, κλοπή, προσθήκη ή αλλοίωση πληροφοριών ή δεδομένων με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος. Κύριος στόχος της συγκεκριμένης μορφής της απάτης είναι τα δεδομένα που φιλοξενούνται στον ηλεκτρονικό υπολογιστή (Η/Υ) και αφορούν τα οικονομικά μεγέθη. Στο πέρασμα του χρόνου η συγκεκριμένη απάτη μετεξελίχτηκε από ένα ομοιογενές σύνολο αδικημάτων, της εποχής των κεντρικών πληροφορικών συστημάτων, σε μία διαφοροποιημένη ενότητα που περιγράφει ένα μεγάλο φάσμα διαφορετικών υποθέσεων στο πεδίο του οικονομικού εγκλήματος (Λάζος, 2001).

2.1.1 Παραποίηση Λογιστικών Λογαριασμών

Η απάτη σε έναν ιδιώτη ή σε μία επιχείρηση μέσω της παραποίησης και εστίασης, τόσο σε δεδομένα όσο και σε πληροφορίες, που αφορούν άμεσα και έμμεσα, και έχει να κάνει με τους άυλους πόρους, όπως για παράδειγμα τις χρηματικές καταθέσεις, τους οικονομικούς τίτλους (ομόλογα, και λογιστικά μεγέθη, όπως ισολογισμούς). Συχνά, υπάρχουν περιπτώσεις βελτίωσης της πίστης (creditrating)

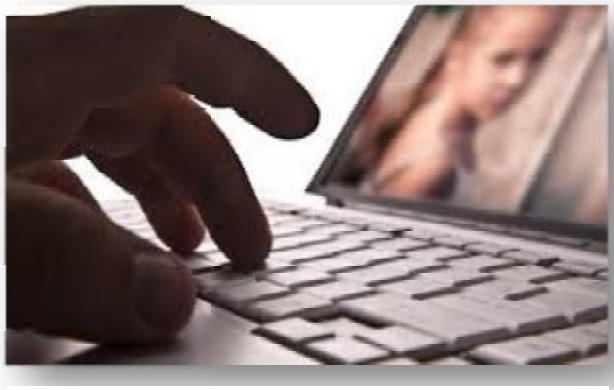
Εικόνα1-1Αυτό είναι ένα χαρτί

μέσω της παραποίησης των δεδομένων που αναφέρονται σε μία επιχείρηση ή ένα άτομο για παράδειγμα, να μπορεί να πάρει δάνειο ή να πάρει δάνειο με καλύτερους όρους, αλλά και χειροτέρευσης της φερεγγυότητας ενός ατόμου ή μιας για τους αντίθετους λόγους, που μπορεί να πραγματοποιηθεί από κάποιο άτομο ή επιχείρηση εχθρικά διακείμενων ή αντίθετων συμφερόντων (Λάζος, 2001).

3. Όσον αφορά με τους άυλους πόρους, μία περίπτωση που αποτελεί ένα παράδειγμα τυπικής παραποίησης είναι η περίπτωση ενός υπαλλήλου που εργαζόταν ως χειριστής και ελεγκτής δεδομένων στο τμήμα επεξεργασίας δεδομένων τράπεζας στη περιοχή της Ζυρίχης, μιας από τις μεγαλύτερες τράπεζες της Ελβετίας. Ο υπάλληλος πέτυχε να θέσει μερικώς, υπό τον έλεγχό του, το αυτόματο σύστημα μεταβίβασης ξένων πληρωμών. Στη συνέχεια, υπέκλεψε πολλές και διάφορες εντολές μεταβίβασης από τους συνεργάτες του και στο σύστημα κωδικοποίησης της τράπεζας. Κάθε φορά τροφοδοτούσε τα εν λόγω ποσά με ανακριβή δεδομένα αντί να τροφοδοτεί τον ηλεκτρονικό υπολογιστή (Η/Υ) με τα ακριβή ποσά μεταβίβασης. Με αρκετό χρόνο στη διάθεσή του, παρέκαμψε τα μέτρα ασφαλείας της τράπεζας που είχαν οργανωθεί με σκοπό την αποτροπή τέτοιων χειρισμών. Έτσι, για παράδειγμα, όταν 98 Γερμανικά μάρκα καταθέτονταν στην Φρανκφούρτη, οι συνεργοί του – αποσύροντας τα χρήματα στο Λουγκάνο και το Νταβός – δεν παραλάμβαναν 100 αλλά 100.000 Ελβετικά φράγκα. Παρόμοια, για μία κατάθεση 97 δολαρίων στην Νέα Υόρκη, δεν αποκόμιζαν 251 αλλά 251.000 Ελβετικά φράγκα. Κατ’ αυτό τον τρόπο, οι δράστες αποκόμισαν συνολικά κέρδη της τάξης των 700.000 Ελβετικών φραγκών (Λάζος, 2001).

2.2 Πορνογραφία

Μία μορφή οικονομικής εκμετάλλευσης της γενετήσιας ζωής αποτελεί η πορνογραφία ανηλίκων, που στρέφεται με βάναυσο τρόπο ενάντια στην ατομική τους αξιοπρέπεια και τραυματίζει την εξέλιξή τους. Το άρθρο 348Α του Ελληνικού Ποινικού Κώδικα, όπως τροποποιήθηκε πρόσφατα με το Νόμο 3625/2007, δίνει τον ακόλουθο ορισμό σχετικά: «Υλικό παιδικής πορνογραφίας συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο». Αξίζει να σημειωθεί ότι, οι



Εικόνα1-2 Αυτό είναι ένα πληκτρολόγιο

νομικοί ορισμοί που δίδονται από τις επιμέρους εθνικές νομοθεσίες για την παιδική πορνογραφία διαφοροποιούνται μεταξύ τους σε σημαντικό βαθμό. Σε γενικές γραμμές, όμως, φαίνεται να συγκλίνουν, οι περισσότερες τουλάχιστον, στην ευρεία παραδοχή ότι παιδική πορνογραφία αποτελεί οποιαδήποτε αναφορά γενετήσιας δραστηριότητας που αναμειγνύει ένα πρόσωπο προεφηβικής ηλικίας (Ζάννη, 2005).

Κατά το ελληνικό δίκαιο, όποιος με πρόθεση παράγει, επιδεικνύει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ. Επιπλέον, όποιος με πρόθεση προσφέρει, παράγει, πωλεί ή με οποιονδήποτε τρόπο διανέμει, διαθέτει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή αξίας πενήντα χιλιάδων ευρώ (50.000) (Ζάννη, 2005).

2.3 Κλοπή Προσωπικών Δεδομένων

Ένα από τα πλέον σοβαρά διαδικτυακά εγκλήματα αποτελεί και η κλοπή ταυτότητας (IdentityTheft). Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς (π.χ.: εμπορικούς, ιατρικούς, διαφημιστικούς). Είναι εύκολο για τον καθέναν, να αναζητήσει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών (Newman, 2004).

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δύο στάδια. Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διαφόρους τρόπους, συμβατικούς και ψηφιακούς όπως:

- Αφαιρώντας πορτοφόλια από τσάντες, αυτοκίνητα ή ακόμη και από την τσέπη ανυποψίαστων περαστικών.
- Υποκλέπτοντας την αλληλογραφία, παραβιάζοντας μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλοντας ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών κ.α.
- Αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενο τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου.
- Εισβάλλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα.
- Χρησιμοποιώντας ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων του διαδικτύου (Newman, 2004).

Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων. Αυτή μπορεί να πραγματοποιηθεί:

- Ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, τους οποίους και χρησιμοποιεί για την αγορά αγαθών μέσω του Διαδικτύου.
- Ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους, χρεώνει με ακάλυπτες επιταγές.
- Δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος.
- Υποβάλλοντας μη πραγματικές φορολογικές δηλώσεις (και μέσω Διαδικτύου), για να εισπράξει επιστροφή φόρου (Newman, 2004).

2.4 Ηλεκτρονικός Εκφοβισμός (Cyberbullyng)

Η συχνή χρήση της τεχνολογίας και των σύγχρονων ηλεκτρονικών μέσων στις μέρες μας, σε συνάφεια με τον καθοριστικό ρόλο που διαδραματίζει το Διαδίκτυο στη κοινωνική

Εικόνα1-3Αυτό είναι πληκτρολόγιο

ζωή των ατόμων και ιδιαίτερα των εφήβων, οδήγησαν εκτός των άλλων και στη δημιουργία μιας νέας μορφής ηλεκτρονικού εκφοβισμού (Καμαριώτης, 2013).

Από τον Καναδό BillBelsey υιοθετήθηκε ο όρος «Cyberbullyng» ο οποίος συνδέεται με τον κοινό εκφοβισμό (σωματικό ή ψυχολογικό) που έχει στόχο να προκαλέσει ζημιά και να βλάψει αρκετά το θύμα (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

Με τον ψηφιακό εκφοβισμό ο θύτης θέτει ως κύριο στόχο την άσκηση ψυχολογικής βίας. Με τον τρόπο αυτό, επιθυμεί να πλήξει το κύρος της προσωπικότητας του θύματος, να το γελοιοποιήσει, να το συκοφαντήσει και να του προκαλέσει συναισθηματικά προβλήματα. Πολλές φορές, ο εκφοβισμός ξεκινά στα πλαίσια της πλάκας λη του αστείου και προέρχεται από κοντινά πρόσωπα (Γουλτίδης, 2014).

Αυτό που καθιστά τον διαδικτυακό εκφοβισμό τόσο επικίνδυνο είναι το ότι «ο καθένας μπορεί να τον πράξει, χωρίς να χρειάζεται να αντιμετωπίσει το θύμα του. Υπάρχουν κάποια χαρακτηριστικά του ηλεκτρονικού εκφοβισμού που τον διαφοροποιούν από τον κοινό και εξηγούν τους λόγους για τους οποίους έχει λάβει τόσο μεγάλη έκταση (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

Αρχικά, το άτομο που προκαλεί τον εκφοβισμό μπορεί να «κρύβεται» πίσω από την ανωνυμία που του προσφέρει το διαδίκτυο. Έτσι, η ανωνυμία δίνει στο δράστη την ασφάλεια πως δεν θα ταυτοποιηθεί και άρα δεν θα τιμωρηθεί για την πράξη του (Καπατζιά, 2008).

Επιπρόσθετα, στο διαδίκτυο δεν υπάρχει η κατά πρόσωπο επαφή. Αυτό έχει ως αποτέλεσμα ο δράστης να αποστασιοποιείται από τις πράξεις του. Δεν μπορεί να αντικρύσει τη συνέπεια που έχει ο εκφοβισμός στο θύμα, με αποτέλεσμα να μην αντιλαμβάνεται το επιβλαβές της ενέργειας του και να μην προσπαθεί να αποκαταστήσει ή να σταματήσει το καταστροφικό του σχέδιο (Καμαριώτης, 2013).

Η επανάληψη αποτελεί το βασικό χαρακτηριστικό της ηλεκτρονικής εκφοβιστικής δράσης. Ο δράστης μπορεί να φωτογραφήσει ή να βιντεοσκοπήσει το θύμα και χωρίς την άδειά του να αναρτήσει το υλικό στο διαδίκτυο. Μπορεί ακόμη να το προωθήσει σε άλλα άτομα, τα οποία με τη σειρά τους θα το χρησιμοποιήσουν ποικιλοτρόπως. Με αυτό τον τρόπο, ο εκφοβισμός επαναλαμβάνεται αυτόματα και για μεγάλο χρονικό διάστημα. Το θύμα κάθε φορά που πλοηγείται στο διαδίκτυο, έρχεται αντιμέτωπο με το υλικό του εκφοβισμού του και αισθάνεται ανήμπορο να αντιδράσει (Hinduja&Patchin, 2007).

Η επίθεση και η προσβολή στο διαδίκτυο είναι πολύ δύσκολο να αφαιρεθεί το εκφοβιστικό υλικό από τον Παγκόσμιο Ιστό. Στα πλαίσια του εκφοβισμού, ο γραπτός λόγος έχει μεγαλύτερη ισχύ και πιο δυσάρεστες συνέπειες από τον προφορικό λόγο. Είναι διαφορετικό να σε χαρακτηρίζουν προσβλητικά με γραπτό τρόπο και μάλιστα «μέσα» από την οθόνη του ηλεκτρονικού υπολογιστή σου, από το να σου πουν την ίδια λέξη προφορικά στην αυλή του σχολείου ή στο δρόμο(Hinduja&Patchin, 2007).

Στον ψηφιακό εκφοβισμό το άτομο αισθάνεται πως δεν μπορεί να προστατευθεί από τις επιθέσεις που δέχεται, επειδή είναι εκτεθειμένο καθ' όλη τη διάρκεια της ημέρας, ακόμη και όταν βρίσκεται μόνο στο σπίτι του. Ιδίως, στο χώρο του σπιτιού μπορεί να βιώνει σε εντονότερο βαθμό τον εκφοβισμό,

καθώς έχει τη δυνατότητα να συνδέεται για πολλές ώρες στο Διαδίκτυο (Hinduja&Patchin, 2007).

Η ανισορροπία δύναμης μεταξύ θύτη και θύματος αποτελεί ένα άλλο στοιχείο του διαδικτυακού εκφοβισμού. Η δύναμη των δραστών έχει να κάνει με την καλή γνώση των ηλεκτρονικών υπολογιστών και με την έλλειψη εποπτείας στο διαδίκτυο και όχι τόσο με την σωματική διάπλαση. Πολλές φορές θύματα του παραδοσιακού εκφοβισμού γίνονται θύτες του ηλεκτρονικού για να εκδικηθούν (Καμαριώτης, 2013).

Τα μόνα που είναι απαραίτητα για να πραγματοποιηθεί διαδικτυακά μια εκφοβιστική ενέργεια είναι μια ηλεκτρονική συσκευή και πρόσβαση στο Internet. Μάλιστα, με την διάδοση των έξυπνων τηλεφώνων (smartphone) με τα οποία μπορεί κανείς να συνδεθεί στο Διαδίκτυο, δεν υφίσταται πλέον διαχωρισμός στις διαδικτυακές δυνατότητες των δύο συσκευών (ηλεκτρονικού υπολογιστή και κινητού τηλεφώνου). Στον πίνακα 2.1 παρουσιάζονται κάποιες μορφές εκφοβισμού στο Διαδίκτυο (Καμαριώτης, 2013)1Μορφές Εκφοβισμού στο Διαδίκτυο.

Αποστολή υβριστικών μηνυμάτων ή «Ανάφλεξη» (Flaming).	Πρόκειται για την αποστολή εχθρικών μηνυμάτων από ένα άτομο ή ομάδα ατόμων στο θύμα, με αποτέλεσμα τον έντονο διαπληκτισμό.
Παρενόχληση (Harassment)	Αφορά στη συνεχή αποστολή προσβλητικών ή απειλητικών μηνυμάτων και έχει στόχο την συναισθηματική και ψυχική αναστάτωση του παραλήπτη. Η διαφορά της παρενόχλησης από την «ανάφλεξη» είναι ότι η παρενόχληση διαρκεί περισσότερο και συνήθως είναι μονόπλευρη.
Διαδικτυακή Καταδίωξη (Cyberstalking).	Αναφέρεται στη χρήση ηλεκτρονικής επικοινωνίας (συνεχής παρενόχληση, αποστολή απειλητικών μηνυμάτων) από κάποιο άτομο με στόχο την συνεχή παρακολούθηση και καταδίωξη του θύματος.
Δυσφήμηση (denigration).	Η δυσφήμηση αφορά στην διάδοση μιας αναληθούς και υποτιμητικής πληροφορίας για κάποιον, σε στόχο να τον βλάψει σε προσωπικό, κοινωνικό, επαγγελματικό ή άλλο επίπεδο. Η

	πληροφορία αυτή μπορεί να δημοσιευθεί σε μια ιστοσελίδα ή να αποσταλεί με μηνύματα σε άλλα πρόσωπα.
Προσωποποίηση ή πλαστοπροσωπία (Impersonation).	Με τη μέθοδο αυτή ο δράστης δημιουργεί ένα ψεύτικο προφίλ, χρησιμοποιώντας το όνομα του θύματος και κάνει αναρτήσεις σε ιστοσελίδες ή στέλνει απρεπή μηνύματα στους διαδικτυακούς του «φίλους». Σε άλλες περιπτώσεις, υποκλέπτει τον κωδικό πρόσβασης του θύματος και χρησιμοποιεί τον λογαριασμό του, με τρόπο που να τον εξευτελίζει στον κοινωνικό του περίγυρο.
Εξαπάτηση ή έξοδος και απάτη (OutingandTrickery).	Σε αυτή την περίπτωση ο δράστης επικοινωνεί με το θύμα και το προσεγγίζει φιλικά, προκειμένου να αποσπάσει με ύπουλο τρόπο προσωπικές πληροφορίες, να τις δημοσιεύσει ή να τις προωθήσει και στη συνέχεια να «εξαφανιστεί».
Αποκλεισμός (Blockade).	Αφορά στον αποκλεισμό ενός ατόμου από ηλεκτρονικούς χώρους διαδικτυακής επικοινωνίας
Χαρούμενο Χαστούκισμα (Happy Slapping).	Πρόκειται για μια νέα μέθοδο εκφοβισμού στο Διαδίκτυο που πρωτοεμφανίστηκε στην Αγγλία. Η διαδικασία έχει ως εξής: Συνήθως έφηβοι περπατούν και χαστουκίζουν κάποιον ανυποψίαστο περαστικό, επίσης έφηβο. Κάποιος από την παρέα των συνομηλίκων καταγράφει το βίαιο περιστατικό, χρησιμοποιώντας την κάμερα του τηλεφώνου του και στη συνέχεια αναρτά το βίντεο στο Διαδίκτυο.

.(Καμαριώτης, 2013, σελ.119).

2.5 Παραβίαση Προσωπικών Δεδομένων

Η παραβίαση προσωπικών δεδομένων αποτελεί ένα από τα συχνότερα προβλήματα που έχει να αντιμετωπίσει η δίωξη ηλεκτρονικού εγκλήματος. Πολλά άτομα που διαθέτουν προφίλ σε πλατφόρμες κοινωνικής δικτύωσης όπως είναι το facebook, το twitter κτλ., παρατηρούν παράξενες δραστηριότητες σχετικές με τον προσωπικό λογαριασμό τους. Επίσης, είναι πιθανό να δημιουργηθεί παράνομα από κακοπροαίρετους ένα δεύτερο προφίλ που να φέρει το όνομά του θύματος και σε αυτό να αναρτώνται ψευδείς πληροφορίες ή προσωπικά στοιχεία για το άτομό του. Οι παραπάνω ενέργειες έχουν σκοπό τη συκοφαντία, τον ευτελισμό ή τον εκφοβισμό και διώκονται ποινικά(Σφακιανάκη, Σιώμου, Φλώρου, 2012).

2.6 Πειρατεία Λογισμικού

Πειρατεία λογισμικού ονομάζεται η αναπαραγωγή ή/και η διάθεση προγραμμάτων του ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους (Βλαχόπουλος, 2007).

<u>Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:</u>

1. **Χρήση ενός προγράμματος σε περισσότερους ηλεκτρονικούς υπολογιστές και υπέρβαση της αδείας χρήσης:**Αποτελεί τη πιο συνηθισμένη μορφή παράνομης χρήσης εφόσον απαιτείται ξεχωριστή άδεια για κάθε ηλεκτρονικό υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα εκδηλώνεται δε ως εξής:
    i. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.
    ii. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρεία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών υπολογιστών.
    iii. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών .
    iv. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους.

Συνήθως, 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 εγκατεστημένα προγράμματα. Το λογισμικό αυτό δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για προγράμματα (Βλαχόπουλος, 2007).

2. **Πλαστογράφηση ή Απομίμηση του Προϊόντος:**Η παράνομη αναπαραγωγή και πώληση λογισμικού γίνεται με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει

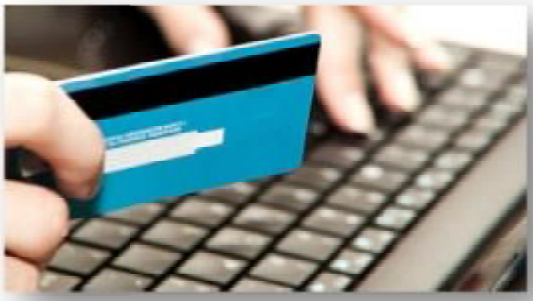
πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό καθώς και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης πλαστών προϊόντων. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν(Βλαχόπουλος, 2007).

2.7 Ηλεκτρονική Απάτη

Οι πιο συνηθισμένες μορφές ηλεκτρονικής απάτης είναι οι παρακάτω:

- **Απάτες 419 ή Νιγηριανές Απάτες:**Χιλιάδες e-mail αποστέλλονται καθημερινά σε τυχαίους παραλήπτες σε διάφορες χώρες, με κύριο σκοπό να καταβάλλει το θύμα ένα αρχικά μικρό ποσό προκειμένου να κερδίσει ένα πολύ μεγαλύτερο κέρδος.

  Συνήθως, με τα μηνύματα που αποστέλλουν «πληροφορούν» ότι κάποιος κάτοχος μεγάλης περιουσίας έχει αποβιώσει και δεν υπάρχει κανείς κληρονόμος. Υποτίθεται ότι το θύμα λόγω ομοιότητας του ονόματός του με



Εικόνα1-4 Αυτή είναι μια κάρτα

  τον ενδημήσαντα έχει επιλεγεί για να κληρονομήσει την περιουσία (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

  «Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο, απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία όπως για παράδειγμα αριθμούς τραπεζικών λογαριασμών και πιστωτικών καρτών, προκειμένου να επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών» (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

- **Απάτες με τη χρήση πιστωτικών καρτών σε on-line αγορές:** Συχνό είναι το φαινόμενο κατά το οποίο υποκλέπτονται ή παραχαράσσονται αριθμοί πιστωτικών καρτών από χρήστες του διαδικτύου που πραγματοποιούν διαδικτυακές αγορές. Υπάρχουν αρκετές περιπτώσεις δημιουργίας ψεύτικων ιστοσελίδων οι οποίες στοχεύουν στην συγκέντρωση στοιχείων και αριθμών από πιστωτικές κάρτες χρηστών του διαδικτύου, οι οποίοι πιστεύουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν ανυποψίαστα τις αγορές τους.
- **Phishing:** Είναι μια πολύ διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων. Κυρίως πρόκειται για στοιχεία τα οποία αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.) (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

2.8 Διακίνηση Ναρκωτικών

Στις μέρες μας, τόσο οι έμποροι όσο και οι διακινητές ναρκωτικών εκμεταλλεύονται τη ραγδαία εξέλιξη της τεχνολογίας και την απήχηση που έχει το Internet στις νεαρές ηλικίες, προκειμένου να πουλήσουν παράνομες ουσίες. Συνήθως, προσεγγίζουν τα θύματά τους μέσα από chatrooms και δημοφιλείς νεανικές ιστοσελίδες κοινωνικής δικτύωσης (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

2.9 Hacking

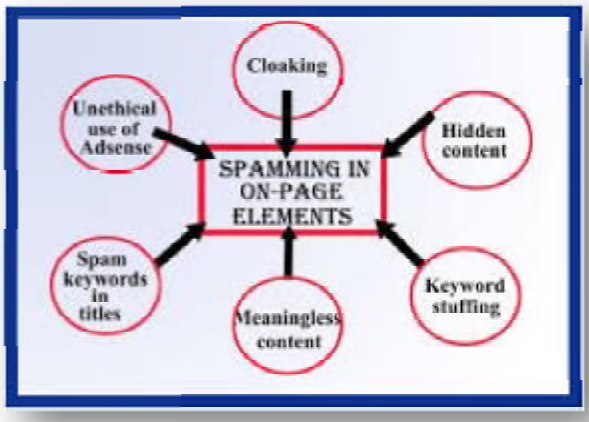
Το hacking ονομάζεται η διαδικασία κατά την οποία γίνεται είσοδος σε υπολογιστικά συστήματα και προγράμματα, από ανθρώπους που δεν επιτρέπεται και δεν είναι αρμόδιοι να το κάνουν. Συντελείται χωρίς άδεια και αυτό την καθιστά παράνομη. Οι hackers συνήθως δεν καταστρέφουν και δεν υποκλέπτουν πάντοτε δεδομένα και πληροφορίες. Ο κύριος σκοπός τους είναι να αποδείξουν τόσο στον εαυτό τους όσο και στους άλλους το επίπεδο της γνώσης και των δεξιοτήτων τους και όχι να προκαλέσουν βλάβες στα υπολογιστικά συστήματα (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

Συχνά «αφήνουν» ηλεκτρονικά μηνύματα στο πέρασμά τους, προκειμένου οι υπεύθυνοι φορείς να διορθώσουν τις ελλείψεις του προγράμματός τους και να το καταστήσουν ασφαλέστερο (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

Οι hackers, χρησιμοποιούν τις δεξιότητες τους στη χρήση του ηλεκτρονικού υπολογιστή για να παραποιήσουν δεδομένα ή να υποκλέψουν κωδικούς ή να αντιγράψουν παράνομα αρχεία και γενικά να πραγματοποιήσουν ηλεκτρονικές παρανομίες για χρηματικά οφέλη, λέγονται crackers (Σφακιανάκη, Σιώμου, Φλώρου, 2012).

2.10 Ανεπιθύμητη Αλληλογραφία (Spamming)

Η ανεπιθύμητη αλληλογραφία ή spamming ονομάζεται η μαζική αποστολή μεγάλου αριθμού μηνυμάτων του ηλεκτρονικού ταχυδρομείου και 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



Εικόνα1-5 Αυτό είναι ένα σχεδιάγραμμα

στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπλέον, για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηρισθεί ως «ενοχλητικό» γι' αυτόν που το λαμβάνει. Η αλληλογραφία αυτή χαρακτηρίζεται ως«απρόκλητη», καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες των διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας. Στον *Πίνακα 2.2.* παρουσιάζονται τα κυριότερα χαρακτηριστικά του spamming (Λάζος, 2001).

Πίνακας 2-2 Τα κυριότερα χαρακτηριστικά του Spamming

Απρόκλητο:	Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα, η οποία θα δημιουργούσε 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.

(Λάζος, 2001, σελ. 56).

Για να προστατευθεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα στο ηλεκτρονικό ταχυδρομείο πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, κι αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Απαραίτητο είναι κάθε χρήστης να εγκαταστήσει στον ηλεκτρονικό του υπολογιστή ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων, όπως επίσης, να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει (Λάζος, 2001).

2.11 Ηλεκτρονικό Ψάρεμα (Phishing – Farming)

Phishing

Το ηλεκτρονικό ψάρεμα ή αλλιώς Phishing ονομάζεται η κατάσταση κατά την οποία ο hacker προσπαθεί, μέσω των μηνυμάτων που στέλνει, να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία τραπεζικού λογαριασμού, πιστωτικής κάρτας, κλπ. Αρχικά, το υποψήφιο θύμα λαμβάνει ένα e-mail, αποστολές του οποίου φαίνεται να είναι η τράπεζά 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 ηλεκτρονικό υπολογιστή της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί αυτόματα. Το e-mail αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, ο οποίος όμως δεν είναι πραγματικός και έτσι, το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα (Τσουραμάνης, 2005).

Το Vishing είναι η προσαρμογή του ηλεκτρονικού ψαρέματος (phishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το VoIP (VoiceoverIPtools). Ο χρήστης λαμβάνει ένα 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 (Τσουραμάνης, 2005).

2.12 Διασπορά Κακόβουλου Λογισμικού

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται κυρίως ε 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 (Trojanhorses) (Dorothy, 2004).

2.12.1 Ιοί (Viruses)

Ένας ιός είναι ένα τμήμα κώδικα, το οποίο κολλάει τον εαυτό του σε άλλες εντολές του ηλεκτρονικού υπολογιστή όπου περιλαμβάνονται ο κωδικός εφαρμογών του προγράμματος που χρησιμοποιείται για την εκκίνηση ενός ηλεκτρονικού υπολογιστή, καθώς και μακροεντολές, οι οποίες έχουν τοποθετηθεί σε έγγραφα. Ο χρήστης ή το σύστημα σε οποιαδήποτε περίπτωση δίνει μία εντολή στον ηλεκτρονικό υπολογιστή, ο ιός ενεργοποιείται παράλληλα κι αυτός. Ο κωδικός του ιού προστίθεται στον κώδικα του ηλεκτρονικού υπολογιστή με τέτοιο τρόπο, ώστε όταν αυτός ο τελευταίος φορτώνεται στη μνήμη για να εκτελεστεί, ο ιός είναι εκείνος που ενεργοποιείται πρώτος. Αρχικά, ο ιός ενεργοποιείτε από μόνος του και έπειτα αποκτά τον έλεγχό του ηλεκτρονικού υπολογιστή, που τον φιλοξενεί. Καθώς ενεργοποιείται, ο ιός μπορεί να τοποθετήσει ένα αντίγραφο του εαυτού του στην μνήμη του ηλεκτρονικού υπολογιστή, όπου αυτό παραμένει «εγκατεστημένο» έως ότου να κλείσει ο υπολογιστής. Αυτό το εγκατεστημένο αντίγραφο αναζητάει για μη μολυσμένους ηλεκτρονικούς υπολογιστές. Όταν βρει κάποιον, του μεταβιβάζει ένα αντίγραφο του εαυτού του. Έπειτα, ο ιός εκτελεί ένα «ωφέλιμο φορτίο», το οποίο μπορεί να κάνει οτιδήποτε από το να δείξει ένα πολιτικό ή ένα ψυχαγωγικό μήνυμα έως ότου να διαγράψει αρχεία από τον σκληρό δίσκο. Παραδείγματος χάρη, ο ιός του Smiley απεικονίζει χαμογελαστά πρόσωπα τα οποία χοροπηδάνε στην οθόνη. Ο ιός που είναι γνωστός είναι ο Michelangelo, ο οποίος δεν είναι ιδιαίτερα αβλαβής. Ξαναγράφει τους πρώτους κυλίνδρους του σκληρού δίσκου εφόσον ενεργοποιήσει την ημέρα γέννησης του μεγάλου καλλιτέχνη , του οποίου φέρει το όνομα δηλαδή στις 6 Μαρτίου. Ακόμα πιο καταστροφικός είναι και ο ιός Win95/CIH. Εκτός του ότι διαγράφει τα πρώτα μεγαμπάιτς (mb) δεδομένων του σκληρού δίσκου, ξαναγράφει μέρος του βασικού συστήματος εισόδου – εξόδου (BIOS) σε ορισμένα chips αναλαμπής της μνήμης ROMS. Το BIOS είναι απαραίτητο για την εκκίνηση του ηλεκτρονικού υπολογιστή έτσι ώστε η επανεκκίνηση του ηλεκτρονικού υπολογιστή με μία εφεδρική δισκέτα να μην απαιτείται. Μία εταιρεία ανέφερε ότι βρήκε τον ιό σε 500 περίπου από τους υπολογιστές της. Ένας «κρυπτοποιός» φέρει φορτίο, το οποίο κρυπτογραφεί με ένα μυστικό κλειδί αρχεία, έχοντας ως συνέπεια να εμποδίζει την πρόσβαση του ιδιοκτήτη σε αυτά. Ένας τέτοιος ιός δεν μπορεί να χρησιμοποιηθεί για εκβιασμό. Εάν ένας ιός δεν εγκαταστήσει τον εαυτό του, τότε θα πρέπει να μολύνει και να αφήσει το φορτίο του σε έναν άλλον υπολογιστή, προτού να αποκτήσει τον έλεγχο του. Από το ένα μηχάνημα στο άλλο, γίνεται η διάδοσή των ιών μέσω δικτύων και δισκετών του υπολογιστή (Dorothy, 2004).

Το 1970 ο GregoryBenford χρησιμοποίησε τον όρο «ιός» προκειμένου να αναφέρει σε ανεπιθύμητο κώδικα ηλεκτρονικού υπολογιστή, όποιος θα μπορούσε να αναπαραγάγει τον εαυτό του κυκλοφορόντας σε υπολογιστές και με τον τρόπο αυτό να εισβάλλει στο APRANEI. Ο DavidGerrold συγγραφέας έργων επιστημονικής φαντασίας, παρουσίασε την ιδέα αυτή σε ένα από τα μυθιστορήματά του με τίτλο «Όταν ο Χάρης ήταν ένας». Ωστόσο, το 1980, όπως γνωρίζουμε και σήμερα οι ιοί ξεκίνησαν να εμφανίζονται και η έννοια τους αποδόθηκε από τον FredCoha, ο οποίος ήταν μεταπτυχιακός φοιτητής του Πανεπιστημίου της Νότιας Καλιφόρνιας (Dorothy, 2004).

Μέχρι τις αρχές του 1998, είχαν ανακαλυφθεί περισσότεροι από 13.000 ιούς στον ηλεκτρονικό υπολογιστή. Εν μέρει, αυτός ο τεράστιος αριθμός εξηγείται από την ευκολία, με την οποία οι πιθανοί δημιουργοί τους μπορούν να βρουν τόσο τα εργαλεία κατασκευής τους όσο και τον πραγματικό ιικό κώδικα, για να εργαστούν , είτε από άλλα κανάλια είτε μέσω του διαδικτύου. Η Ψηφιακή Συμμαχία των Hackers, τον Μάιο του 1997, ανήγγειλε τη διάθεση στο κοινό ενός CD – ROM, ο οποίος περιείχε 10.000 ιούς. Οι ίδιοι προσέφεραν δωρεάν τους πρώτους εκατό πελάτες τους μία συλλογή από 50 εργαλεία κατασκευής ιών (Dorothy, 2004).

Ένας χρήστης μπορεί να «μαζέψει» έναν ιό από διαφορές πηγές, στις οποίες συμπεριλαμβάνονται τα προσαρτώμενα σε μηνύματα ηλεκτρονικά ταχυδρομεία , οι δισκέτες,

τα CD – ROM καθώς επίσης και ιστοσελίδες με ενσωματωμένο κώδικα. Κανονικά ο χρήστης πρέπει να ανοίξει το προσαρτώμενο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου με σκοπό να απελευθερώσει τον ιό (Dorothy, 2004).

Υπάρχουν τρία βασικά είδη ιών, τα οποία είναι του συστήματος εκκίνησης, του προγράμματος και των μακροεντολών τα οποία έχουν πάρει το όνομά τους ανάλογα με τα μέρη του υπολογιστή που μολύνουν. Οι πολυμερείς ιοί συνδυάζουν τα δύο πρώτα από τα είδη αυτά, με αποτέλεσμα να μολύνουν και τα αρχεία του προγράμματος καθώς και τους τομείς εκκίνησης του σκληρού δίσκου (Dorothy, 2004).

2.12.2 Σκουλήκια (Worms)

Ένα σκουλήκι (worm) είναι ένα πρόγραμμα στο οποίο η μετάδοσή του γίνεται από τον έναν υπολογιστή στον άλλον μέσω ενός δικτύου υπολογιστών εισβάλοντας στον υπολογιστή με την ίδια διαδικασία που εισβάλλει και ένας hacker. Αντίθετα, με τους ιούς, αυτά τα προγράμματα δεν παίρνουν καμία βοήθεια από αμελείς χρήστες. Πρέπει να βρουν ένα υπολογιστή στον οποίο να μπορούν να του επιτεθούν , να τον εισβάλλουν και να μετακινήσουν ένα αντίγραφο κώδικά τους σε αυτό, το οποίο θα μπορεί εκεί να εκτελέσει. Στην πραγματικότητα, ο εισβολέας πηδάει από το ένα σύστημα στο άλλο, αυτοματοποιώντας εντελώς το κάθε βήμα που κάνει (Dorothy, 2004).

Από τον ιστορία του internet, το σπουδαιότερο περιστατικό που ξεκίνησε στις 2 Νοεμβρίου το 1998, όταν ο μεταπτυχιακός φοιτητής πληροφορικής του Πανεπιστημίου CornellRobbertTappanMorris, δημιούργησε ένα πρόγραμμα, το οποίο αντίγραφα και τα κυκλοφορούσε σε ολόκληρο το διαδίκτυο. Σε λίγες μόνο ώρες, είχε εισβάλλει σε 2.000 με 6.000 ηλεκτρονικούς υπολογιστές, σε ποσοστό που ανέρχεται μεταξύ 3% έως 10% του συνόλου των ηλεκτρονικών υπολογιστών, που ήταν συνδεδεμένοι τη στιγμή αυτή στο internet. Επιπρόσθετα, αυτό το πρόγραμμα υπερφόρτωνε τα συστήματα που χτυπούσε, δημιουργώντας ουσιαστικά προβλήματα σε κάθε ηλεκτρονικό υπολογιστή, στον οποίο εισέβαλε. Αυτό είχε ως συνέπεια, τα συστήματα αυτά να απενεργοποιηθούν από το δίκτυο ή να σταματήσουν να λειτουργούν εντελώς, για αρκετές μέρες, ενώ οι καθαριστές τους, τα καθάριζαν. Όταν ο Morris αντιλήφθηκε τη ζημιά που είχε προκαλέσει, με την βοήθεια ενός φίλου του έστειλε ένα μήνυμα στο Δίκτυο με οδηγίες για την απενεργοποίηση του Worm, τότε όμως ήταν είδη πολύ αργά για την ζημιά που προκάλεσε. Ο Morris καταδικάστηκε στις 16 Μαΐου το 1990 για παράβαση του νόμου για την Κατάχρηση και την Απάτη σε ηλεκτρονικούς υπολογιστές. Για τις πράξεις του, του επιβλήθηκε πρόστιμο αξίας $10.000 και η ποινή της επιτήρησης για 3 χρόνια καθώς και παροχή εργασίας 400 ωρών στην κοινότητα (Dorothy, 2004).

Σύμφωνα με το Εθνικό Κέντρο Δεδομένων και Εγκλημάτων με ηλεκτρονικό υπολογιστή, ο διαχειριστής και αστρονόμος των συστημάτων CliffStoll, που ανακάλυψε τους hackers του Ανόβερου, έκανε μία εκτίμηση που ξεκινούσε από τα $100.000 και ξεπερνούσε τα $10 εκατομμύρια. Ο πρόεδρος της ομώνυμης εταιρείας JohnMcAfee, ο οποίος διαθέτει προγράμματα κατά των ιών, ανέβασε σχετικό κόστος στα $97 εκατομμύρια (Dorothy, 2004).

Επιστήμονες της πληροφορικής του Ινστιτούτου Τεχνολογίας της Μασαχουσέτης, του Πανεπιστημίου Pordue και άλλοι ενδιαφερόμενοι, κατά την διάρκεια της κρίσης δημιούργησαν μια ομάδα για την επίθεση του worm στους ηλεκτρονικούς υπολογιστές. Οι επιστήμονες αυτοί ανέλυσαν τον κώδικα αυτού του ιού και κυκλοφόρησαν αντίδοτά του. Λιγότερο από έναν μήνα, από την ενέργεια αυτή, το DefenceResearchProjectsAgency ίδρυσε το ComputerEmergencyResponseTeamCoordinationCenter (CEPT/CC) του Πανεπιστημίου

CarnegieMellon με σκοπό να προετοιμάσει την αντιμετώπιση ανάλογων μελλοντικών επιθέσεων. Από την εποχή του worm του internet, καμία άλλη μειωμένη επίθεση δεν κατάφερε να αχρηστεύσει τόσα πολλά συστήματα (Dorothy, 2004).

Μετά την εμφάνιση του worm του internet, περίπου έναν χρόνο μετά, ένα άλλο worm ξεκίνησε τη δράση του μέσω του δικτύου SPAN της NASA. Οι επιστήμονες που έμπαιναν στο κέντρο υπολογιστών της NASAGoddardSpaceFlight στο Greenbelt του Maryland, στις 6 Οκτωβρίου το 1989, έβλεπαν να τους υποδέχεται ένα banner του worm με όνομα WANK (Dorothy, 2004).

Μία επιστήμονας της NASA λάμβανε μηνύματα από τον ηλεκτρονικό υπολογιστή της, τα οποία της έλεγαν πως όλα τα αρχεία της είχαν διαγραφεί κάτι που στην πραγματικότητα δεν συνέβαινε. Επιπλέον, το wormWANK μεταδόθηκε και εκτός του δικτύου της NASA στο Δίκτυο Υψηλής Ενέργειας του Υπουργείου Ενέργειας, το γνωστό στην HEPNET. Οι διαχειριστές αυτού του δικτύου πίστευαν ότι μετά από δυο εβδομάδες, έντονης προσπάθειας, είχαν απαλλαγεί από αυτό, όταν μία νέα και περισσότερο δραστική έκδοσή του εμφανίστηκε. Για να απαλλαγούν από αυτή, χρειάστηκαν δύο ακόμη εβδομάδες. Ο διευθυντής πρωτόκολλων του γραφείου SPAN της NASAJohnMcMahon, υπολόγισε πως αυτό το worm τους κόστισε πάνω από μισό εκατομμύριο δολάρια σε χαμένο χρόνο και πηγές. Η πηγή της επίθεσης αυτής δεν εντοπίστηκε ποτέ, ωστόσο κάποιες ενδείξεις λένε ότι θα μπορούσε να προέρχεται από κάποιους hackers. Η προσπάθεια χρήσης του συστήματος του χρήστη στον κώδικα πρόσβασης για το σπάσιμο ενός λογαριασμού θεωρείται μια απλή στρατηγική επίθεσης του worm (Dorothy, 2004).

2.13 Ξέπλυμα Χρήματος

«Ξέπλυμα χρήματος» ονομάζεται η διαδικασία μέσω των οποίας τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μια σειρά διαδικασιών, οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα) (Λάζος, 2001).

Στον Πίνακα 2.3. παρουσιάζονται τα στάδια διαδικασίας του ξεπλύματος (Χλούπη, 2000).

Πίνακας 2-3 Στάδια Διαδικασίας του Ξεπλύματος.

Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της άδειας χρήσης.	Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης, εφόσον απαιτείται ξεχωριστή άδεια για κάθε ηλεκτρονικό υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα. *Εκδηλώνεται ως εξής:* i. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες. ii. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών των ηλεκτρονικών υπολογιστών. iii. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών. iv. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους. Συχνά οι πωλητές των ηλεκτρονικών 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 εγκατεστημένα προγράμματα.
Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος.	Η παράνομη αναπαραγωγή και η πώληση του λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. 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, καθιστά 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.

(Χλούπη 2000, σελ126).

3. ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΝΟΜΟΘΕΣΙΑΚΗ ΠΡΟΣΕΓΓΙΣΗ

ΕΙΣΑΓΩΓΗ

Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή (Η/Υ) καθώς και της λειτουργίας του Διαδικτύου, αναπτύσσονται αρκετές δυνατότητες τόσο χρήσης όσο και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η διαδικτυακή εγκληματικότητα συνεχώς εμπλουτίζεται με νέες μορφές και είναι σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την αντιμετώπιση της διαδικτυακής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών (Κωστάρας, 2012

3.1 Ελληνική Νομοθεσία

Στην Ελληνική Νομοθεσία δεν υπάρχει κάποιος συγκεκριμένος Νόμος ο οποίος να προσδιορίζει επακριβώς το Διαδικτυακό Έγκλημα. Οι παραβάσεις που διαπιστώνονται για αδικήματα που διαπράττονται μέσω διαδικτύου, τιμωρούνται σύμφωνα με νομοθεσία της κλασσικής μορφής τέλεσης των αδικημάτων αυτών (Παπαντωνίου, 2009). Η συνεργασία της Ελλάδας με τα άλλα κράτη της Ευρωπαϊκής Ένωσης (Ε.Ε.), καθώς και άλλων Διεθνών Οργανισμών, έχει ως κύριο σκοπό την καλύτερη αντιμετώπιση των σχετικών θεμάτων. Σύμφωνα με τη νομοθεσία υπάρχουν δύο απόψεις του Αρείου Πάγου, βάση των οποίων επιτρέπονταν στην ελληνική αστυνομία να ψάχνει και να ελέγχει τα προσωπικά στοιχεία κάποιου, προκειμένου να οδηγηθεί στα ψηφιακά ίχνη του hacker, με σκοπό την σύλληψη του (Σφακιανάκης, 2007).

Συγκεκριμένα, ο νόμος αυτός καλύπτει τις εταιρείες/παρόχους σύνδεσης στο διαδίκτυο (Otenet, Hellasonline, Vodafone, κ.α.) στο να μη δημοσιοποιούν τα προσωπικά στοιχεία του κάθε χρήστη, όπως αυτό της I.P. διεύθυνσης. Έτσι αυτό είχε ως αποτέλεσμα να δημιουργηθεί σύγχυση και το έργο της αστυνομίας να δυσχεραίνεται όλο και περισσότερο. Όπως είναι φανερό κάποιες εταιρείες, για κερδοσκοπικούς λόγους, δεν συνεργάζονται με την αστυνομία εφόσον καλύπτονται και νομικά με την ύπαρξη του νέου νόμου. Η αστυνομία γνωρίζει εξ αρχής ποιες εταιρείες συνεργάζονται μαζί της και έτσι εύχονται το περιστατικό που θα αντιμετωπίσουν να προέρχεται από τους συγκεκριμένους παρόχους (Σφακιανάκης, 2007).

3.2 Διεθνής Νομοθεσία

Όσον αφορά τις νομοθετικές προσεγγίσεις του διαδικτυακού εγκλήματος από τα ποινικά συστήματα των διαφόρων κρατών, η Νομική Επιτροπή της Μ. Βρετανίας (BritishLawCommision) διαπιστώνει την υιοθέτηση τριών βασικών τάσεων που παρουσιάζονται στον Πίνακα 3.1 (Λάζος, 2001).

Πίνακας 3-1 Υιοθέτηση τριών βασικών τάσεων της Νομικής Επιτροπής της Μ. Βρετανίας.

Την εξελικτική, όπου το διαδικτυακό έγκλημα αντιμετωπίζεται με το ισχύον νομοθετικό πλαίσιο, με έννοιες που απλά διευρύνονται κατά περίπτωση για να περιλαμβάνουν και ορισμένες περιπτώσεις διαδικτυακού εγκλήματος.
Νόμοι που θεσπίζονται για την συνολική αντιμετώπιση του διαδικτυακού εγκλήματος.
Νομοθετήματα που σχεδιάζονται ειδικά για τα διαδικτυακά εγκλήματα αλλά εντάσσονται στο ευρύτερο νομοθετικό πλαίσιο.

(Λάζος, 2001, σελ.142).

Αρχικά, οι νομοθεσίες των περισσότερων χωρών όπως οι ΗΠΑ, η Μ. Βρετανία καθώς καιη Αυστραλία αντιμετωπίζουν τον hacker με βάση το υπάρχον νομοθετικό πλαίσιο, συμπεριλαμβάνοντάς το στις γενικότερες κατηγορίες, είτε του οργανωμένου εγκλήματος και της οργανωμένης απάτης (Πολιτεία της Αριζόνα) είτε της πνευματικής ιδιοκτησίας (Φλόριντα) καθώς και του οικονομικού εγκλήματος (Μ. Βρετανία) (Λάζος, 2001).

Κατά την περίοδο της χρονολογίας του 1980 δημιουργήθηκαν διάφορα νομοθετήματα για την κάλυψη των κενών στην αντιμετώπιση του πληροφορικού εγκλήματος. Την χρονολογία του 1986 στο Αμερικάνικο Κογκρέσο θεσπίστηκε ο νόμος για «την Απάτη και Προσβολή των Ηλεκτρονικών Υπολογιστών» (ComputerFraudAndAbuseAct, U.S. PublicLaw, 1986) που προέβλεπε τρία κακουργήματα και τρία πλημμελήματα (Λάζος, 2001).

<u>Τα τρία κακουργήματα αφορούν:</u>

1. Τη σκόπιμη μη εξουσιοδοτημένη ή υπέρβαση εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικούς υπολογιστές με κύριο σκοπό την πρόκληση βλάβη στις ΗΠΑ ή την ωφέλεια ξένης χώρας.
2. Την πρόσβαση σε ηλεκτρονικό υπολογιστή ομοσπονδιακού συμφέροντος με σκοπό την εξαφάνιση των ΗΠΑ καθώς και την απόκτηση αξιών.
3. Τη σκόπιμη, μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικό υπολογιστή, με κύριο σκοπό την αλλαγή, την αλλοίωση ή την καταστροφή πληροφοριών ομοσπονδιακού ενδιαφέροντος ή την παρεμπόδιση της αξιοποίησης αυτών των πληροφοριών (Λάζος, 2001).

Οι ποινές που προβλέπονται για το δράστη κυμαίνονται από χρηματικά πρόστιμα μέχρι δεκαετή φυλάκιση τουλάχιστον τα είκοσι έτη (Λάζος, 2001).

Επίσης, τα δύο πλημμελήματα αφορούν σε ομοσπονδιακά συμφέροντα και το τρίτο με τη παράνομη διακίνηση κωδικών πρόσβασης που επηρεάζει το εμπόριο. Οι ποινές για αυτά δεν ξεπερνούν τη φυλάκιση του ενός έτους.

Η ποινική αντιμετώπιση του διαδικτυακού εγκλήματος στη Μ. Βρετανία παίρνει μορφή με το «Νόμο κακής χρήσης των Ηλεκτρονικών Υπολογιστών» (ComputerMisuseAct) του 1990 (Λάζος, 2001).

<u>Αυτό προβλέπει:</u>

1. **Ένα πρόσωπο είναι ένοχο προσβολής αν:**
    i. Αποκτά πρόσβαση σε τόσο προγράμματα όσο και σε δεδομένα αποθηκευμένα στον ηλεκτρονικό υπολογιστή.
    ii. Η πρόσβαση αυτή είναι χωρίς εξουσιοδότηση, και,
    iii. Είναι σκόπιμη αυτή η πρόσβαση.
2. **Ο σκοπός του προσώπου που διαπράττει την παραπάνω προσβολή δεν είναι απαραίτητο να κατευθύνεται προς:**
    i. Κάποιο ειδικά δεδομένα ή προγράμματα
    ii. Δεδομένα ή προγράμματα ειδικού τύπου
    iii. Δεδομένα ή προγράμματα αποθηκευμένα σε συγκεκριμένο υπολογιστή (Λάζος, 2001).

Έτσι, αυτό είχε ως συνέπεια να δημιουργούνται τρία νέα εγκλήματα εκ των οποίων τα δύο αφορούν τη μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικό υπολογιστή ή δεδομένα και το τρίτο με τη συνειδητή και σκόπιμη αλλαγή του περιεχομένου των δεδομένων ενός ηλεκτρονικού υπολογιστή (Λάζος, 2001).

Την χρονολογία του 1986 ο Γερμανικός Ποινικός Κώδικας προσαρμόστηκε στις νέες μορφές εγκληματικότητας με το «2^{ο} Νόμο για την καταπολέμηση της οικονομικής εγκληματικότητας» που περιλαμβάνει διατάξεις οι οποίες αφορούν άμεσα: (Αργυρόπουλος, 2001).

i. Το haking, τη μετάδοση ιών, τη χωρίς άδεια απόκτηση δεδομένων
ii. Τη παραποίηση δεδομένων
iii. Τη δολιοφθορά ηλεκτρονικού υπολογιστή (Αργυρόπουλος, 2001).

3.3 Διεθνής Προσπάθειες Νομικής Συνεργασίας

Η παγκοσμιοποίηση του διαδικτυακού εγκλήματος απαιτεί συνεργασία καθώς και διακρατικό συντονισμό για την αντιμετώπισή του. Τέτοιες προσπάθειες συνιστούν η Σύμβαση του Συμβουλίου της Ευρώπης για το διαδικτυακό έγκλημα στη Βουδαπέστη το 2001, η Συνθήκη των Ηνωμένων Εθνών ενάντια στο Οργανωμένο Έγκλημα το 2000 στο Παλέρμο, η σύνοδος των G8 για το Διεθνές Οργανωμένο Έγκλημα στο Χάλιφαξ το 1995, η συνθήκη του Μάαστριχτ το 1992, η λειτουργία της Europol και της Interpol κλπ (Broadhurst, 2006).

Για τη διεθνή/νομική συνεργασία στην καταπολέμηση του διαδικτυακού εγκλήματος κάποιοι ειδικοί μελετητές όπως οι Grabosky και Broadhurst πρότειναν τα παρακάτω βασικά στοιχεία (Broadhurst, 2006):

i. Αύξηση της ευαισθητοποίησης και επαγρύπνησης σε θέμα ασφάλειας με παροχή απαραίτητου εξοπλισμού στους ειδικούς για την διασφάλιση των συναλλαγών.
ii. Βελτίωση τόσο του συντονισμού όσο και της συνεργασίας μεταξύ του συστήματος της ποινικής δικαιοσύνης καθώς και των φορέων του δημοσίου και ιδιωτικού τομέα.
iii. Διασφάλιση ότι η τεχνολογία θα έχει τη δυνατότητα να διευκολύνει τη τις αρχές να ερευνούν και να θεσπίζουν τους νόμους για την αντιμετώπιση του εγκλήματος.
iv. Διερεύνηση της ποινικοποίησης των συμπεριφορών.
v. Ενδυνάμωση των διεθνών συμβάσεων για την αναγνώριση των απειλών, του διεθνή χαρακτήρα τους καθώς επίσης και της ανάγκης για εναρμόνιση των νομοθεσιών.
vi. Ανάπτυξη δεξιοτήτων για τα εργαστήρια των εγκλημάτων έτσι ώστε να συνεργάζονται επιχειρησιακά με τις αρχές των διαφόρων κρατών (Broadhurst, 2006).

3.4 Νομική Προσέγγιση του Διαδικτύου

Για την αντιμετώπιση του διαδικτυακού εγκλήματος κυρίαρχο νομικό ζήτημα αποτελεί η νομική ρύθμιση του διαδικτύου. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του διαδικτύου και των υπηρεσιών. Επιπρόσθετα, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών δηλαδή που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του διαδικτυακού «κόσμου» (Ζάννη, 2005).

Τα επιχειρήματα υπέρ της ρύθμισης του διαδικτύου παρουσιάζονται στον Πίνακα 3.2.

Πίνακας 3-2 Επιχειρήματα υπέρ της ρύθμισης του διαδικτύου

Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.
Είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του.
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.

(Βλαχόπουλος, 2007, σελ 96).

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης παρουσιάζονται στον Πίνακα 3.3. (Βλαχόπουλος, 2007).

Πίνακας 3-3 Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης.

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

(Βλαχόπουλος, 2007 σελ. 125).

Σύμφωνα με τις οδηγίες της Ευρωπαϊκής Κοινότητας, η προσαρμογή της Ελληνικής Νομοθεσίας προήλθε, αρχικά, με τον Νόμο 2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Νόμο 2246/94 και στη συνέχεια με τον Νόμο 2867/2000, που ως σήμερα είναι σε ισχύ. Με τον νόμο αυτό, ιδρύθηκε η ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με κύριο στόχο τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους παρόχους τηλεπικοινωνιακών υπηρεσιών καθώς και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης

συγκεκριμένων δικαιωμάτων των χρηστών, όπως είναι η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους (Βλαχόπουλος, 2007).

3.5 Το Πρόβλημα της Δικαιοδοσίας στο Διαδίκτυο

Ιδιαίτερα περίπλοκο είναι το πρόβλημα της δικαιοδοσίας στα διαδικτυακά εγκλήματα εξαιτίας της παγκοσμιότητας τους. Η δικαιοδοσία ονομάζεται 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.

Στον Πίνακα 3.4 παρουσιάζονται οι τέσσερις θεωρίες για τον καθορισμό του τόπου τελέσεως του αδικήματος (Mali, 2008):

Πίνακας 3-4 Θεωρίες για τον καθορισμό του τόπου τελέσεως του αδικήματος

Η θεωρία του τόπου του αποτελέσματος:	Τόπος τελέσεως του αδικήματος θεωρείται ο τόπος που εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
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.
Η μικτή θεωρία:	Τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
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.

3.6 Άρθρα Ποινικού Κώδικα Σχετικά με το Διαδικτυακό Έγκλημα

3.6.1 Άρθρο 13 Γ Ποινικού Κώδικα - Πλαστογραφία σε Ηλεκτρονικό Έγγραφο

Έγγραφο ονομάζεται κάθε γραπτό το οποίο είναι πρόσφορο ή προορίζεται να αποδείξει γεγονός που έχει έννομη σημασία όπως κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. «Έγγραφό επίσης, ονομάζεται και κάθε μέσο στο οποίο χρησιμοποιείται από ηλεκτρονικό υπολογιστή (Η/Υ) ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό, ή ακόμη με άλλο τρόπο, τόσο για τη παραγωγή, την εγγραφή, την αποθήκευση όσο και για την αναπαραγωγή των στοιχείων, τα οποία δεν μπορούν να διαβαστούν άμεσα, καθώς επίσης, και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, ήχος, εικόνα ή σύμβολο αυτοτελώς ή σε συνδυασμό, εφόσον τα υλικά και τα μέσα αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα τα οποία έχουν έννομη σημασία» (Κωστάρας, 2012).

3.6.2 Άρθρο 348Α Ποινικού Κώδικα - Πορνογραφία των Ανηλίκων

Σύμφωνα με το Άρθρο 348 Α Ποινικού Κώδικα, το οποίο θεσπίστηκε με το Νόμο 3064/2002 αναφέρει:

1. Όποιος από κερδοσκοπία αγοράζει, κατέχει, προμηθεύεται, μεταφέρει, παρασκευάζει, διακινεί, πωλεί, διαθέτει ή ακόμη θέτει με οποιονδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό τιμωρείται με φυλάκιση ενός έτους καθώς επίσης και με χρηματική ποινή αξίας δέκα χιλιάδων ευρώ έως εκατό χιλιάδων ευρώ (100.000).
1. Σύμφωνα με την προηγούμενη παραγράφου το πορνογραφικό υλικό συνιστά κάθε περιγραφή πραγματική ή εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου το οποίο αποσκοπεί στη γενετήσια διέγερση, καθώς επίσης και η καταγραφή ή η αποτύπωση σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο.
2. Αν κάποια από τις πράξεις που αναφέρονται στη πρώτη παράγραφο αφορά το πορνογραφικό υλικό το οποίο συνδέεται τόσο με την εκμετάλλευση της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας όσο και με την απειρία ανηλίκου ή με την άσκηση σωματικής βίας κατ' αυτού, επιβάλλεται με κάθειρξη έως δέκα ετών καθώς επίσης και με χρηματική ποινή αξίας πενήντα χιλιάδων ευρώ έως εκατό χιλιάδων ευρώ (50.000 – 100.000). Ωστόσο, αν η πράξη είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται με κάθειρξη τουλάχιστον δέκα ετών καθώς επίσης και με χρηματική ποινή αξίας εκατό χιλιάδων ευρώ έως πεντακοσίων χιλιάδων ευρώ (100.000 – 500.000) (Κωστάρας, 2012).

3.6.3 Άρθρο 370 Α - Η Παραβίαση της Προφορικής Συνομιλίας και του Απορρήτου των Τηλεφωνημάτων

1. Όποιος αθέμιτα παρεμβαίνει σε τηλεφωνική συσκευή ή σύνδεση με σκοπό να μαγνητοφωνήσει ή να πληροφορηθεί το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση. Η χρησιμοποίηση από το δράστη των πληροφοριών ή των μαγνητοταινιών που αποκτήθηκε με τον τρόπο αυτόν θεωρείται ως επιβαρυντική περίπτωση.
2. Όποιος με ειδικά τεχνητά μέσα αθέμιτα μαγνητοφωνεί ή παρακολουθεί μία προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων, τιμωρείται με φυλάκιση. Όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου, τιμωρείται με την ίδια ποινή.
3. Όποιος κάνει χρήση των μαγνητοσκοπήσεων ή των πληροφοριών που αποκτήθηκαν με τους τρόπους που αναφέρονται στις παραγράφου 1 και 2 αυτού του άρθρου, τιμωρείται με φυλάκιση.
4. Η πράξη της παραγράφου 3 δεν είναι άδικη αν και η χρήση έγινε ενώπιον οποιουδήποτε ανακριτικής, δικαστηρίου, ή άλλης δημόσιας αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος το οποίο δε μπορούσε να διαφυλαχθεί διαφορετικά και ιδίως σε ποινικό δικαστήριο για την υπεράσπιση του κατηγορούμενου.
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 του άρθρου αυτού τελεί τις πράξεις αυτές κατά επάγγελμα ή είναι ιδιωτικός αστυνομικός ή απέβλεπε στην είσπραξη αμοιβής επιβάλλεται φυλάκιση τουλάχιστον ενός έτους καθώς επίσης και με χρηματική ποινή.
7. Όποιος διαθέτει στο εμπόριο ή προσφέρει με άλλο τρόπο 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 καθώς επίσης και με χρηματική ποινή (Κωστάρας, 2012).

3.6.4 Άρθρο 370 Β - Παραβίαση Προγραμμάτων ή Στοιχείων των Ηλεκτρονικών Υπολογιστών που Θεωρούνται Απόρρητα

1. Όποιος αθέμιτα χρησιμοποιεί, αντιγράφει, αποτυπώνει, αποκαλύπτει σε οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα ηλεκτρονικών υπολογιστών (Η/Υ), τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του ιδιωτικού ή του δημόσιου τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών.
2. Αν ο δράστης ανήκει στην υπηρεσία του κατόχου των στοιχείων, καθώς επίσης 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 το οποίο αναφέρεται στην ασφάλεια του κράτους, η πράξη τιμωρείται κατά τα άρθρα 146 και 147.
4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση (Κωστάρας, 2012).

3.6.5 Άρθρο 370Γ - Η Αντιγραφή ή η Παράνομη χρήση των προγραμμάτων των ηλεκτρονικών υπολογιστών και η παράνομη πρόσβαση σε δεδομένα των ηλεκτρονικών υπολογιστών

1. Όποιος χωρίς δικαίωμα να αντιγράφει ή ακόμη να χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών, τιμωρείται με φυλάκιση έως έξι μήνες καθώς επίσης και με χρηματική ποινή αξίας διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος αποκτά πρόσβαση σε στοιχεία τα οποία έχουν εισαχθεί σε περιφερειακή μνήμη ηλεκτρονικού υπολογιστή ή σε ηλεκτρονικό υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ ή με φυλάκιση μέχρι τρείς μήνες.
3. Αν ο δράστης ανήκει 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 αρμόδιου υπαλλήλου του.
4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση (Κωστάρας, 2012).

3.6.6 Άρθρο 386Α - Απάτη με Ηλεκτρονικό Υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία του ηλεκτρονικού υπολογιστή τόσο με μη ορθή διαμόρφωση του προγράμματος όσο και με την επέμβαση κατά την εφαρμογή του, με τη χρησιμοποίηση ελλιπών ή μη ορθών στοιχείων τιμωρείται με τις ποινές του άρθρου 370 Γ.Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες αποτελούνται από ένα ή περισσότερα πρόσωπα (Κωστάρας, 2012).

3.6.7 Ελληνική Νομοθεσία

Νόμοι

- ***Ο Νόμος 2225/1994αναφέρει:***
  «Την Προστασία της ελευθερίας της ανταπόκρισης και της επικοινωνίας»
- ***Ο Νόμος 2246/1994 αναφέρει:***
  «Την οργάνωση και τη λειτουργία στο τομέα των τηλεπικοινωνιών»
- ***Ο Νόμος 2472/1997 αναφέρει:***
  «Την προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα»
- ***Ο Νόμος 2672/1998 αναφέρει:***
  «Τη διακίνηση των εγγραφών με ηλεκτρονικά μέσα»
- ***Ο Νόμος 2774/1999 αναφέρει:***
  «Την προστασία των δεδομένων του προσωπικού χαρακτήρα στο τηλεπικοινωνιακό τομέα»
- ***Ο Νόμος 2867/2000 αναφέρει:***
  «Τη λειτουργία και την οργάνωση των τηλεπικοινωνιών»
- ***Ο Νόμος 3115/2003 αναφέρει:***
  «Την αρχή της διασφάλισης του απορρήτου των επικοινωνιών»
- ***Ο Νόμος 3431/2006 αναφέρει:***
  «Τις ηλεκτρικές επικοινωνίες»
- ***Ο Νόμος 3471/2006 αναφέρει:***
  «Την προστασία των δεδομένων του προσωπικού χαρακτήρα» (Κωστάρας, 2012).

3.6.8 Ευρωπαϊκή Νομοθεσία (Οδηγίες της Ευρωπαϊκής Ένωσης (Ε.Ε.)

- ***Η Οδηγία 87/102/ΕΟΚ:***

  Αφορά τη προσέγγιση των διοικητικών των νομοθετικών καθώς και των κανονιστικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
- ***Η Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990:***

  Αφορά τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής του ανοικτού δικτύου *(OpenNetwortProvision – ONP).*
- ***Η Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991:***

  Αφορά τη νομική προστασία των προγραμμάτων των ηλεκτρονικών υπολογιστών.
- ***Η Οδηγία 96/9/ΕΟΚ της 11ης Μαρτίου 1996***:

  Αφορά τη νομική προστασία των βάσεων δεδομένων του ηλεκτρονικού υπολογιστή.
- ***Η Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997:***

  Αφορά τη προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.
- ***Η Οδηγία 1999/93/ΕΚ, της 13ης Δεκεμβρίου 1999:***

  Αφορά το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- ***Η Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000:***
- Αφορά ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, κυρίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.
- ***Η Οδηγία 2000/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002***:

  Αφορά τη πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών καθώς επίσης και τη διασύνδεσή τους.
- ***Η Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002:***

  Αφορά την αδειοδότηση υπηρεσιών και δικτύων των ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).
- **Η Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002**:

  Αφορά το κανονιστικό πλαίσιο για υπηρεσίες και δίκτυα των ηλεκτρονικών επικοινωνιών.
- ***Η Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Μαρτίου 2002***:

  Αφορά τα δικαιώματα και την καθολική υπηρεσία των χρηστών όσον αφορά τις υπηρεσίες και τα δίκτυα των ηλεκτρονικών επικοινωνιών.
- ***Η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002***:

Αφορά την προστασία της ιδιωτικής ζωής καθώς και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

- ***Η Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002***:

  Αφορά τον ανταγωνισμό των υπηρεσιών και των δικτύων των ηλεκτρονικών επικοινωνιών (Κωστάρας, 2012).

3.6.9 Προεδρικά Διατάγματα

- ***Το Προεδρικό Διάταγμα 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».
- ***Το Προεδρικό Διάταγμα 150/2001:*** «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».
- ***Το Προεδρικό Διάταγμα 47/2005:*** «Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών».
- ***Το Προεδρικό Διάταγμα 342/2002:*** «Διακίνηση εγγραφών με ηλεκτρονικό ταχυδρομείο» (Κωστάρας, 2012).

4 ΕΓΚΛΗΜΑΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ-ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

4.1 Το «Πρώτο» Διαδικτυακό Έγκλημα

Γενικά, η εμφάνιση του διαδικτυακού εγκλήματος μπορεί να τοποθετηθεί στην ίδια χρονική περίοδο με αυτή των ηλεκτρονικών υπολογιστών. Οι hackers προσπάθησαν μέσω του ηλεκτρονικού υπολογιστή να αναζητήσουν τρόπους και να εκμεταλλευτούν , προς όφελός τους, τα νέα μέσα που τους προσφέρονταν. Φυσικά, λόγω το ότι η τεχνολογία δεν ήταν τόσο αναπτυγμένη τα πρώτα χρόνια των ηλεκτρονικών υπολογιστών, γεγονός που έκανε τους ηλεκτρονικούς υπολογιστές είδος πολυτελείας. Παρόλα αυτά, το διαδικτυακό έγκλημα δεν είχε σε καμία περίπτωση τις μορφές και τις διαστάσεις που έχει στις μέρες μας (Βλαχόπουλος, 2007).

Η εξέλιξη καθώς επίσης και η εξάπλωση του διαδικτύου, αλλά και η απλοποίηση των χρησιμοποιημένων συστημάτων συνέβαλε στην εξάπλωση του διαδικτυακού εγκλήματος. Ωστόσο, το πρώτο καταγεγραμμένο διαδικτυακό έγκλημα είχε διαπραχθεί πολύ νωρίτερα, όταν ο MarieJacquard, ο οποίος κατασκεύασε τον αργαλειό, στην χρονολογία του 1820. Αυτή η συσκευή επέτρεπε την επανάληψη μιας συγκριμένης ακολουθίας βημάτων, όπως γινόταν και στην διαδικασία της ύφανσης, κάτι το οποίο προκάλεσε έντονη ανησυχία στους υπαλλήλους του MarieJacquard, οι οποίοι ένιωσαν ότι απειλούνταν ο παραδοσιακός τρόπος εργασίας με αποτέλεσμα να προκαλούσαν δολιοφθορές στον αργαλειό, για να αποθαρρύνουν τη χρήση της νέας τεχνολογίας. Συγκεφαλαιώνοντας, το παραπάνω έγκλημα, αν και δεν συμπεριλαμβάνει την χρήση του ηλεκτρονικού υπολογιστή, κατατάσσεται ως το πρώτο διαδικτυακό έγκλημα, λόγω της χρήσης μίας νέας τεχνολογίας (Βλαχόπουλος, 2007).

4.2 Περιπτώσεις Διαδικτυακού Εκφοβισμού / Θυματοποίησης

Τα Μέσα Μαζικής Ενημέρωσης και η Διεθνής Βιβλιογραφία προσφέρουν αρκετά παραδείγματα χρήσης του διαδικτύου για εκφοβιστικούς σκοπούς μεταξύ συνομηλίκων, τα οποία πολλές φορές χαρακτηρίζονται από ιδιαίτερη σκληρότητα. Παρακάτω θα αναφερθούν μερικές από τις πιο χαρακτηριστικές περιπτώσεις του διαδικτυακού εκφοβισμού.

Οι HindujaandPatchin 2009, διηγούνται τη μαρτυρία ενός δωδεκάχρονου κοριτσιού από την περιοχή του Michigan που περιγράφει πώς «ένα κορίτσι μου είπε ότι θα ερχόταν κάποια στιγμή να σκοτώσει εμένα την ίδια και τους γονείς μου. Με έκανε να κλάψω τόσο πολύ που έκανα εμετό. Έτσι, γνωρίζω πως είναι να παρενοχλείσαι πέρα από κάθε φαντασία».

Ένα δευτερό περιστατικό αναφέρει ο Benfer (2001), ο οποίος διηγείται την περίπτωση προσβλητικών και κακοηθών μηνυμάτων που δημοσιεύτηκαν ανώνυμα μέσω διαδικτύου για ένα κορίτσι στο γυμνάσιο, που υπέφερε από πολλαπλή σκλήρυνση κατά πλάκας και παχυσαρκία. Τα μηνύματα αυτά ήταν κατάλληλα σχεδιασμένα να την υποτιμήσουν και να την ταπεινώσουν. Με το πέρασμα του χρόνου, το μίσος μέσω διαδικτύου προεκτάθηκε και στην καθημερινότητα του κοριτσιού, όταν έξω από το σπίτι του κοριτσιού, οι θύτες έγραψαν υβριστικά μηνύματα, προξένησαν ζημιές στο αυτοκίνητό της και πέταξαν μπουκάλια γεμάτα με οξύ στην μπροστινή της πόρτα.

Ο BillBelsey, Καναδός εκπαιδευτικός και πατέρας, που ερευνά το φαινόμενο του διαδικτυακού εκφοβισμού, περιγράφει το εξής περιστατικό: Μία έφηβη που δημιούργησε ένα διαδικτυακό τόπο για τον εαυτό της και ζητούσε να της υπογράψουν το «λεύκωμα» της, έλαβε αρκετά μηνύματα τα οποία της έλεγαν ότι «όλοι τη μισούν» και ότι «πρέπει να πεθάνει». Έχουν καταγραφεί πολλά παρόμοια γεγονότα, όπως για παράδειγμα ένα περιστατικό ενός νέου ο οποίος υπέφερε από καταθλιπτικά συμπτώματα, αφού είχε γίνει στόχος μίας διαδικτυακής εκφοβιστικής εκστρατείας με διάρκεια τρία χρόνια περίπου. Επιπλέον, ένας δεκαπεντάχρονος, που με τρόμο ανακάλυψε ότι είχε δημιουργηθεί ένας διαδικτυακός τόπος με αποκλειστικό σκοπό να τον προσβάλλει, και να τον απειλήσει, συμπεριλαμβανομένης και της ημερομηνίας θανάτου του.

Με τη σειρά τους, οι εφημερίδες και οι τηλεοράσεις περιγράφουν λεπτομερώς σχετικές εμπειρίες. Ένα κορίτσι στο Γυμνάσιο αποκλείστηκε από τους συνομηλίκους της, λόγω των διαδικτυακών αναφορών ότι είχε τον ιό SARS κατά τη διάρκεια πρόσφατων ταξιδιών. Επίσης, οι φωτογραφίες ενός μαθητή από την Ιαπωνία, που τον έδειχναν να αλλάζει στα αποδυτήρια δημοσιεύτηκαν στο διαδίκτυο. Γνωστή είναι η περίπτωση ενός διαδικτυακό τόπου ο οποίος δημιουργήθηκε από συμμαθητές για να χλευαστεί ένας μαθητής που επί χρόνια είχε υπάρξει θύμα εκφοβισμού στο σχολείο. Ο διαδικτυακός τόπος που δημιούργησαν, ανέφερε τα εξής: «Καλώς ήρθατε στο διαδικτυακό τόπο που κοροϊδεύει τον (το όνομα του παιδιού)», τον περιέγραφε ως ένα παιδόφιλο που χρησιμοποιούσε το χάπι βιασμού σε αγοράκια. Επί επτά μήνες τα παρακάλια των γονιών και οι μηνύσεις από δικηγόρο τελικά είχαν ως συνέπεια την αφαίρεση του διαδικτυακού τόπου από το παγκόσμιο ιστό.

Ένα από τα πιο πολυσυζητημένα περιστατικά του διαδικτυακού εκφοβισμού αφορούσε έναν έφηβο από τον Καναδά που δυσφημίστηκε ως το «Παιδί του StarWars», με αποτέλεσμα εκατομμύρια άνθρωποι κατέβασαν ένα βίντεο που ένας από τους συμμαθητές του είχε μοντάρει και δημοσιεύσει στο διαδίκτυο. Το βίντεο τον έδειχνε να αναπαριστάνει μια σκηνή από την δημοφιλή ταινία. Το βίντεο αυτό πάρθηκε, όταν το παιδί, είχε τραβήξει στο σπίτι του, τον εαυτό του, να κουνάει ένα μπαστούνι του γκολφ αντί για σπαθί με φως, έχοντας ως

συνέπεια να γίνει ο περίγελος των συμμαθητών του και σύμφωνα με τις ειδήσεις, εγκατέλειψε το σχολείο και δέχτηκε ψυχιατρική βοήθεια.

Τον Ιούνιο του 2006, σε εφημερίδα δημοσιεύθηκε ένα άρθρο για τις βίαιες απειλές που έγιναν σε έναν γνωστό διαδικτυακό τόπο κοινωνικής δικτύωσης σε μία ομάδα μαθητών περιγραφόμενων ως «Goths» λόγω των σκούρων ρούχων τους και το έντονο μακιγιάρισμα τους. Η διεύθυνση του σχολείου κινήθηκε νομικά και μερικοί γονείς κράτησαν τα παιδιά τους μακριά από το σχολείο από ανησυχία για την ασφάλειά τους.

Ένα άλλο περιστατικό του διαδικτυακού εκφοβισμού, στην Αυστραλία, ένα κορίτσι στην ηλικία των εννιά ετών, δεχόταν επανειλημμένα μηνύματα ηλεκτρονικού ταχυδρομείου, πορνογραφικού περιεχομένου. Οι γονείς του κοριτσιού υπέθεταν ότι ο δράστης ήταν ενήλικας. Όμως, η αλήθεια ήταν διαφορετική από ότι πίστευαν οι γονείς, αφού η δίωξη του ηλεκτρονικού εγκλήματος αποκάλυψε ότι πρόκειται για ένα επίσης ανήλικο συμμαθητή του κοριτσιού.

Αλησμόνητη έχει μείνει η, γνωστή περίπτωση της MeganMeier, από τα Μέσα Μαζικής Ενημέρωσης, η οποία αφού είχε δημιουργήσει σχέση μέσω διαδικτύου με ένα άγνωστό της αγόρι, εκείνο άρχισε να την παρενοχλεί και να την προσβάλλει. Αυτή η συμπεριφορά του ήταν τόσο ανυπόφορη για εκείνη ώστε τελικά να οδηγηθεί στην αυτοκτονία. Η είδηση πως το αγόρι αυτό δεν υπήρξε ποτέ προκάλεσε σοκ. Στην πραγματικότητα, ήταν ένα δημιούργημα της μητέρας της κολλητής του κοριτσιού, η οποία μέσω διαδικτύου επεδίωκε να μάθει τι δημοσίευε η Megan για την κόρη της.

Σε ορισμένες περιπτώσεις, το διαδίκτυο έχει χρησιμοποιηθεί από έφηβους ως μέσο απειλής και προειδοποίησης για επερχόμενη εγκληματική συμπεριφορά. Ένας από το δολοφόνους του περιβόητου μακελειού στο Γυμνάσιο Columbine, ο Eric Harris, δημιούργησε ένα διαδικτυακό τόπο όπου συζητούσε τη δολοφονία των μαθητών, παρόλο που εκείνη την περίοδο, δεν λήφθηκε κανένα μέτρο εναντίον του από τις αρχές.

Επιπλέον, στη χώρα μας έχουν κάνει την εμφάνισή τους περιστατικά που υπογραμμίζουν την επικίνδυνη επέκταση του φαινομένου και στον Ελλαδικό χώρο. Στα τέλη Σεπτεμβρίου του 2010, σύμφωνα με μία διαδικτυακή ειδησεογραφική πηγή, κοντά στο σχολικό συγκρότημα της Γκράβας στην περιοχή της Καλλιθέα, κατά τη διάρκεια τσακωμού μίας μαθήτριας με συμμαθήτρια, μαχαιρώθηκε 17χρονη που προσπάθησε να τις χωρίσει. Σύμφωνα με πληροφορίες, αιτία της διαμάχης στάθηκε ένα υβριστικό σχόλιο στην ιστοσελίδα της στο Facebook. Ο καβγάς των συμμαθητριών ξεκίνησε εντός του σχολικού συγκροτήματος της Γκράβας και συνεχίστηκε έξω από το σπίτι του κοριτσιού. Η μαθήτρια ανέβηκε στο σπίτι της και αφού πρώτα πήρε ένα μαχαίρι, στη συνέχεια κατέβηκε στο δρόμο για να συνεχίσει τον καβγά. Το θύμα προσπάθησε να χωρίσει τις δύο συμμαθήτριές της, με αποτέλεσμα να δεχτεί μαχαιριά από μία από τα κορίτσια. Η δράστης συνελήφθη και οδηγήθηκε στο τμήμα ανηλίκων της Ασφάλειας Αττικής.

Ένα άλλο εξίσου ακραίο παράδειγμα, σε συνδυασμό με αυτοκτονία, είναι η περίπτωση του μαθητή του ΟΑΕΔ, ο οποίος πυροβόλησε τρία άτομα και στη συνέχεια αυτοκτόνησε, μία πράξη για την οποία είχε προειδοποιήσει προηγουμένως στην προσωπική του ιστοσελίδα.

Από τις παραπάνω ιστορίες που αναφέρθηκαν, είναι έκδηλη τόσο η τάση των εφήβων να καταφεύγουν στο διαδίκτυο, έχοντας μία επιθετική διάθεση προς του συνομηλίκους τους, όσο και η ενδεχόμενη διάσταση των πιθανών συνεπειών, που κυμαίνονται από την πρόκληση αναστάτωσης και ενόχλησης σε ένα παιδί, μέχρι και απώλεια της ανθρώπινης ζωής (http://psychografimata.com).

5. ΕΡΕΥΝΗΤΙΚΟ ΣΗΜΕΙΩΜΑ

5.1 ΕΡΕΥΝΑ ΜΕ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Εισαγωγή

Η έρευνα που πραγματοποιήθηκε στην παρούσα πτυχιακή εργασία επικεντρώνεται στο κατά πόσο ο κόσμος γνωρίζει τι είναι διαδικτυακό έγκλημα και κατά πόσο ξέρει που να απευθυνθεί εάν του συμβεί κάτι παρόμοιο.

Το ερωτηματολόγιο απευθύνθηκε στα κατάλληλα άτομα σε διάφορες ηλικίες . Σε αυτό το κεφάλαιο θα δούμε το ερωτηματολόγιο και τα αποτελέσματα που προκύπτουν μέσα από την ανάλυση του.

Καθορισμός των Ερευνητικών στόχων

Στόχοι της έρευνας για το διαδικτυακό έγκλημα είναι:

Η διερεύνηση του τι είναι για τον κόσμο διαδικτυακό έγκλημα. Επίσης να προσδιοριστεί κατά πόσο ο κόσμος χρησιμοποιεί το διαδίκτυο

Και κατά πόσο γνωρίζει τη νομοθεσία και τι κάνει σε περίπτωση που πέσει σε διαδίκτυα έγκλημα

Έρευνα με ερωτηματολόγιο

Η μέθοδος του ερωτηματολογίου ήταν η πιο κατάλληλη μέθοδος για αυτήν την έρευνα δεδομένου ότι επιτρέπει την διανομή και την ανάκτηση των πληροφοριών σε σύντομο χρονικό διάστημα.

Σχεδιασμός του ερωτηματολογίου

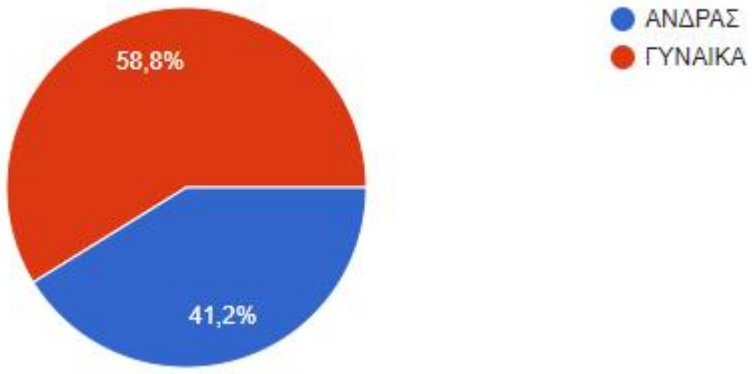
Το ερωτηματολόγιο απευθύνθηκε σε όλες τις ηλικίες όλων των επίπεδων μόρφωσης ώστε να κατανοηθεί κατά πόσο παίζει ρολό η γνώση ανάλογα με το επίπεδο μορφωσης,κατά πόσο ο κόσμος πλέον χρησιμοποίει το διαδίκτυο για ενημέρωση..

5.2 ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

Στοιχεία Ερωτηματολογίου

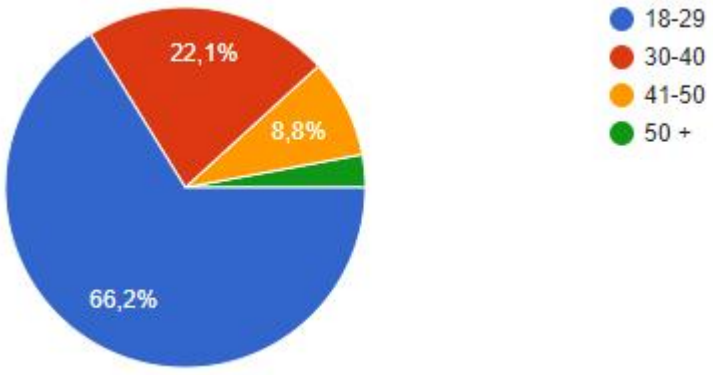
Ξεκίνησα με τα στοιχειά που πήρα τις πληροφορίες μου και τα παρουσιάζω ακολούθως:

1.ΦΥΛΛΟ



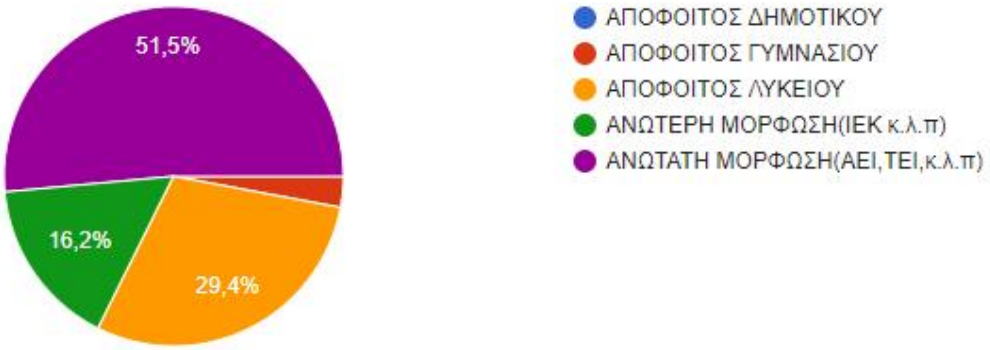
Εδώ βλέπουμε ότι τις περισσότερεςαπαντήσειςέδωσανγυναίκες

2.ΗΛΙΚΙΑ



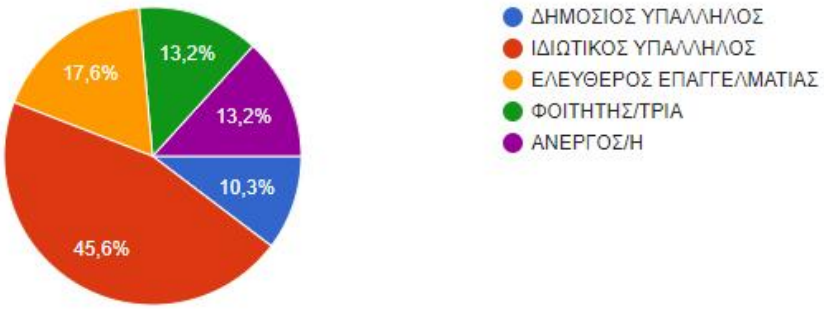
Εδώ όσοναφορά την ηλικίαβλέπουμε ότι 66,2% που απάντησανήταν 18-29 το 22,1% ήταν 30-40 το 8,8% ήταν 41-50, και τέλος ένα 2,9% από 50 και πανω.Αρα οι μικρότεροι σε ηλικίαδείχνει ότι ασχολούνταιπερισσότερομε το διαδίκτυο

3.ΜΟΡΦΩΤΙΚΟ ΕΠΙΠΕΔΟ



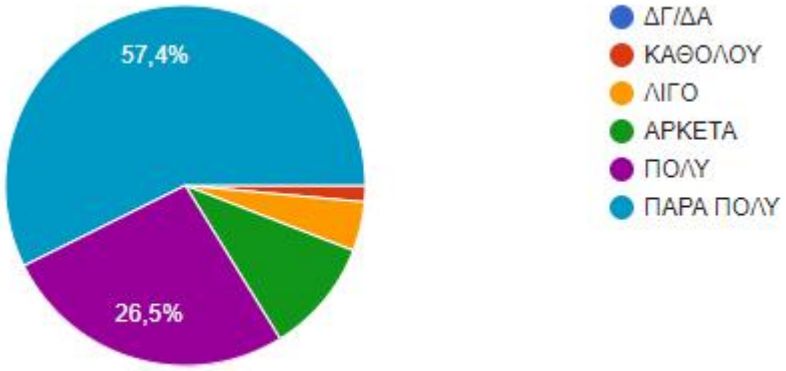
Εδώ το γράφημα αυτό μας δείχνει το μορφωτικόεπίπεδο των χρηστών που απάντησαν και βλέπουμε πως το μεγαλύτεροποσοστόκαλύπτει η ανωτάτημόρφωση(ΑΕΙ,ΤΕΙ) με 51,5%, ακολουθει με 29,4% οι απόφοιτοιλυκείου, ενώ με 16,2% απόφοιτοιανώτερημόρφωση(ΙΕΚκλπ), ενώ με 2,9% απόφοιτοιγυμνασίου..

4.ΕΠΑΓΓΕΛΜΑ



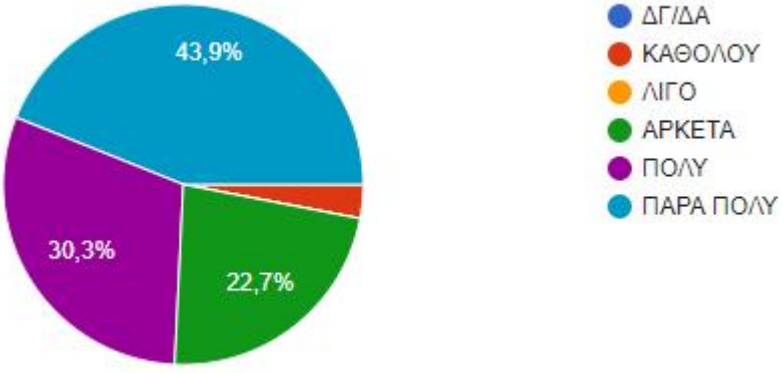
Στο σχήμα αυτό βλέπουμε πως με βάση τον αριθμό των απαντήσεων που δόθηκαν το μεγαλύτεροποσοστόέχει ο ιδιωτικόςυπάλληλος με 45,6%, εν συνεχεία ο ελεύθεροςεπαγγελματίας με 17,6%,ισοψηφουν οι φοιτητές και οι άνεργοι με 13,2% και τέλοςμόλις 10,3% έχουν οι δημόσιοιυπάλληλοι

5.ΠΟΣΟ ΣΥΧΝΑ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΤΟ ΔΙΑΔΙΚΤΥΟ;



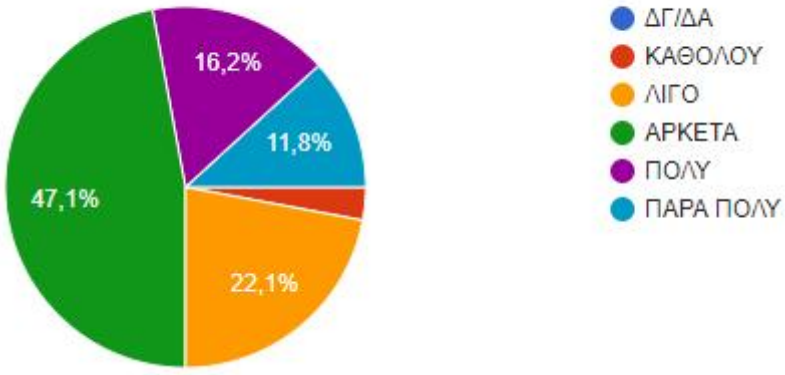
Εδώ βλέπουμε πως το μεγαλύτεροποσοστόχρηστών με 57,4% χρησιμοποιεί το διαδίκτυοπάραπολύ. Στησυνέχεια το 26,5% πολύ ενώ ακολουθούν με 10,3% αρκετά, με 4,4% λίγο και μόλις 1,5% καθόλου..

6.ΠΟΣΟ ΧΡΗΣΙΜΟ ΣΑΣ ΦΑΙΝΕΤΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ;



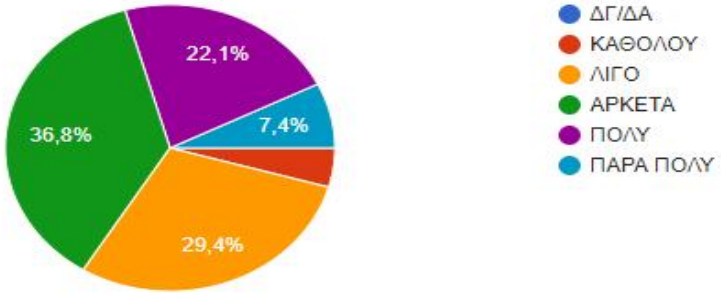
Εδώ το 43,9% του φαίνεταιχρήσιμο το διαδίκτυο ,το 30,3% πολύ χρήσιμο , το 22,7% αρκετά, ενώ το 3% καθόλου..

7.ΠΟΣΟ ΑΞΙΟΠΙΣΤΟ ΣΑΣ ΦΑΙΝΕΤΑΙ;



Στην ερώτηση στο πόσο αξιόπιστο φαίνεται το διαδίκτυο βλέπουμε πόσο το πάρα πολύ καλύπτει ένα μικρό ποσοστό της τάξεως του 11,8%, ένα μεγάλο ποσοστό το αρκετά με 47,1%,το 22,1% λίγο, το 16,2% πολύ , ενώ με μόλις το 2,9% απάντησε πως το διαδίκτυο δεν είναι καθόλου αξιόπιστο..

8. ΠΟΣΟ ΣΥΧΝΑ ΕΝΗΜΕΡΩΝΕΣΤΕ ΓΙΑ ΚΑΠΟΙΟ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ;



Στην ερώτηση για το πόσο συχνά ενημερώνονται οι χρήστες για κάποιο διαδικτυακό έγκλημα το 36,8% απάντησε αρκετά, το 29,4% απάντησε λίγο, το 22,1% είπε πολύ, το 7,4% πάρα πολύ δηλαδή σχεδόν κάθε μέρα, ενώ μόλις το 4,4% απάντησε καθόλου.

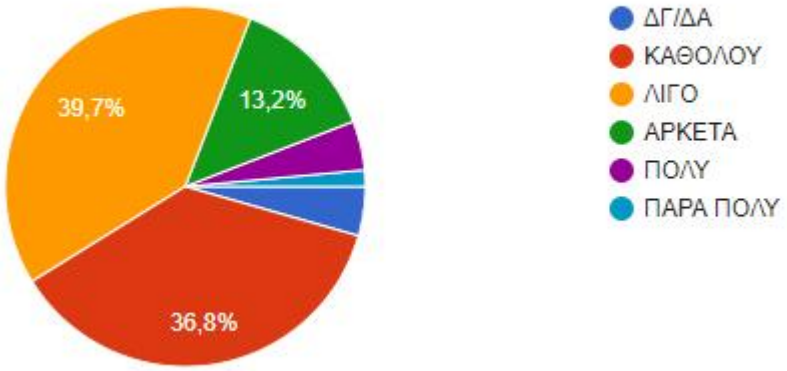
9. ΤΙ ΕΙΝΑΙ ΓΙΑ ΕΣΑΣ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ;

1) ΤΑ ΠΑΝΤΑ
2) Απατη
3) ΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
4) *ΕΓΚΛΗΜΑ ΟΠΩΣ ΤΑ ΑΛΛΑ*
5) ΤΙΠΟΤΑ
6) Μια παράνομη κατάσταση η οποία εξελίσσετε μέσα από το χώρο αυτο
7) Παραβίαση προσωπικών δεδομένων
8) Παραβίαση προσωπικού απορρήτου
9) Υποκλοπές σε προσωπικό και εταιρικό επίπεδο κυρίως
10) Παιδικη πορνογραφία
11) Απατη, cyberbullying
12) Cyberbullying
13) Η οποιαδήποτε μορφής παρενόχληση ενός ατόμου μέσω του διαδικτύου
14) Κακουργημα
15) Το φαινόμενο της παιδικής πορνογραφίας
16) Πλαστοπροσωπια , μαστροπια κ.α.
17) Η παραβίαση προσωπικών δεδομένων
18) Υποκλοπή προσωπικών δεδομένων εν αγνοία του "θύματος". Επίσης, κάθε κακόβουλη πράξη που βασίστηκε σε υπηρεσίες διαδικτύου.
19) ΑΠΑΤΕΣ, ΥΠΟΚΛΟΠΕΣ
20) Παραβίαση προσωπικων δεδομένων
21) Ναι
22) ΚΑΤΑΠΑΤΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
23) ΧΑΚΑΡΙΣΜΑ
24) Η δημοσίευση προσωπικών δεδομένων χωρίς την συγκατάθεση μου, ο εκβιασμός μέσω διαδικτύου, το bullying.
25) Παραβίαση προσωπικών δεδομένων
26) Ενοχλητική αλληλογραφία, ιοί, ανακατεύθυνση σε ψεύτικες ιστοσελίδες, λεκτική ή σεξουαλική παρενόχληση, κλπ
27) Είναι διάφορες οι κατηγορίες των διαδικτυακών εγκλημάτων... Από απόσπαση χρημάτων μέσω ψεύτικων αγοραπωλησιών μέχρι ακόμα και πρόκληση αυτοκτονίας λόγω "μπούλινγκ"...
28) Κλοπη δεδομενων, απατη προιοντων, χρηση προσωπικων δεδομένων απο τριτους, πλαστοπροσωπια, προβολη σκηνων και ρητορικης μίσους
29) Οτιδήποτε έχει σχέση με αποπλάνηση ανηλίκων,με εκβιασμούς ανηλίκων και ενηλίκων,με διαφημίσεις προϊόντων επικίνδυνα για την υγεία μας,με αγορές μέσω διαδικτύου με κάρτες χρεωστικές ή πιστωτικές με αποτέλεσμα κάποιοι να χακαρουν προσωπικά δεδομένα.
30) Δημοσίευση προσωπικών στοιχείων, καταπάτηση προσωπικής ζωής
31) Όταν κάποιος εκμεταλλεύεται την άγνοια της τεχνολογίας και την ανωνυμία για να κάνει κάτι που με την κοινή λογική ή τον νόμο είναι έγκλημα
32) Κλοπη φωτογραφιων για κακο σκοπο
33) ΚΛΟΠΗ ΣΤΟΙΧΕΙΩΝ ΚΑΙ ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΟΥΣ
34) Εξαπάτηση
35) Οτιδήποτε μορφη απατης η εξαπάτησης
36) Οικονομικη εκμεταλευση
37) ΟΙΚΟΝΟΜΙΚΗ ΕΚΜΕΤΑΛΕΥΣΗ

38) ΑΠΑΤΗ
39) Είναι να προσπαθείς να πλησιασεις με κακό σκοπο τον άλλον,να τον εξαπατησεις, κλπ
40) Να μου χακαρουν καποιον ηλεκτρονικό λογαριασμό
41) Εγκλημα που σαν κυρια μορφή επικοινωνίας του εχει το διαδυκτιο
42) Η πορνογραφία γιατί μπαίνουν και ανηληκ
43) Είναι το χακάρισμα λογαριασμών... εισβολή σε προσωπικά δεδομένα ή μηνύματα...bullying μέσω ίντερνετ...κ.α
44) Οικονομικη απατη
45) Όταν κάποιος εισχωρεί στα προσωπικά δεδομένα κάποιου και τα χρησιμοποιεί είτε για να τον βλάψει είτε για να βγαλει κέρδος γενικά για όποιονδιποτε λογο
46) Παραβιαση προσωπικων δεδομενων
47) Παραβιαση δεδομενων
48) Παραπληροφορηση,εξαπατηση,παραβιαση
49) Η οικονομικηεξαπατηση, η διακίνηση παράνομων ουσιών, η παράνομη πορνογραφία
50) ΑΝΕΠΙΤΡΕΠΤΟ
51) Πορνογραφια
52) δεν ξερω

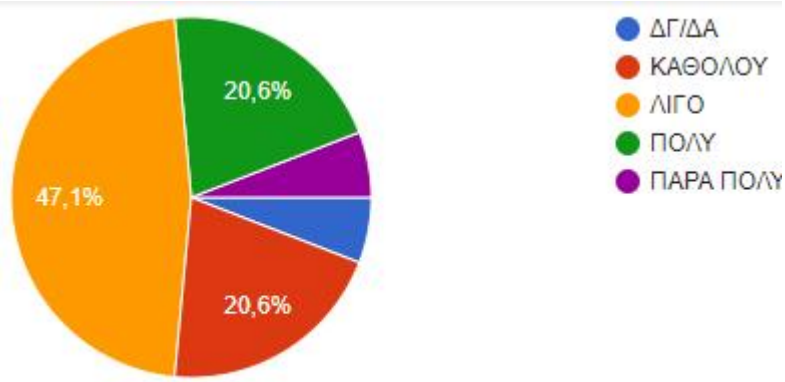
Εδώ βλέπουμε τις απαντήσεις που μας έδωσαν διάφοροι χρήστες στην ερώτηση το τι είναι κατά τη γνώμη τους διαδικτυακό έγκλημα

10.ΠΟΣΟ ΚΑΛΑ ΓΝΩΡΙΖΕΤΕ ΤΗ ΝΟΜΟΘΕΣΙΑ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ;



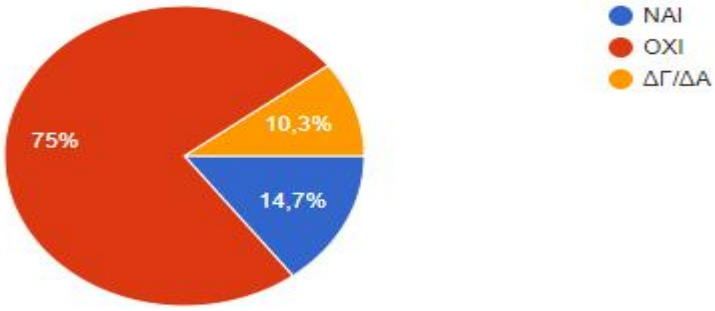
Στην ερώτηση κατά πόσο οι χρήστες γνωρίζουν τη νομοθεσία βλέπουμε πως το μεγαλύτερο ποσοστό γνωρίζει λίγο (με 39,7%) έως καθόλου(με 36,8%) τη νομοθεσία γύρω από το διαδικτυακό έγκλημα , το 13,2% γνωρίζει αρκετά,ενώ με ποσοστό 4,4% δηλώνουν ότι γνωρίζουν πολύ τη νομοθεσία η με επίσης 4,4% δεν γνωρίζουν/δεν απαντούν και μόλις το 1,5% γνωρίζει τη γίνεται γύρω από τους νόμους του διαδικτύου.

11. ΓΝΩΡΙΖΕΤΕ ΤΙ ΠΡΕΠΕΙ ΝΑ ΚΑΝΕΤΕ ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΟΥ ΠΕΣΕΤΕ ΘΥΜΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ;



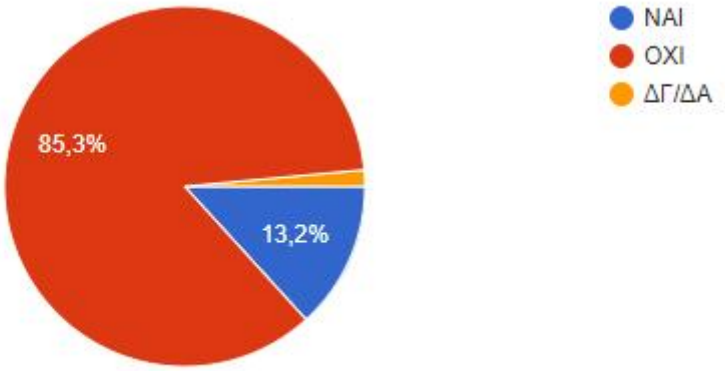
Στην ερώτηση αν γνωρίζουν τι πρέπει να κάνουν εάν πέσουνθύμαδιαδικτυακούεγκλήματοςμόλις το 5,9% γνωρίζειπάρα πολύ καλά να το αντιμετωπίσει, το 20,6% δηλώνει ότι γνωρίζει πολύ, το 47,1% γνωρίζειελάχιστα, ενώ ένα ακόμα 20,6% δηλώνεικαθόλου , τελειώνοντας με ένα 5,9% που δήλωσε δεν γνωρίζω/δεν απαντώ..

12. ΕΧΕΤΕ ΠΕΣΕΙ ΠΟΤΕ ΘΥΜΑ "ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΙΑ"(HAKER);



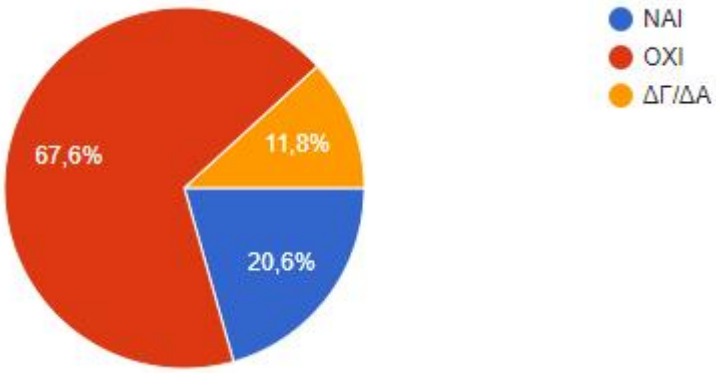
Στην ερώτηση εάν έχουνπέσειθύμαHaker το μεγαλύτεροποσοστόδήλωσε όχι με 75%, το 14,7% απάντησε πως ναι έχειπέσειθύμα, ενώ βλέπουμε πως ένα 10,3% δήλωσε πως δεν θέλει να απαντήσει με το δεν γνωρίζω/δεν απαντώ.

13. ΕΧΕΤΕ ΠΕΣΕΙ ΠΟΤΕ ΘΥΜΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΚΦΟΒΙΣΜΟΥ(CYBERBULLYING);



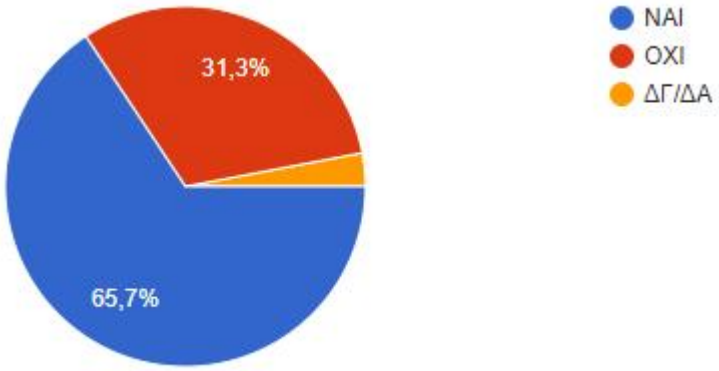
Στην ερώτηση ενός cyberbullying οι χρήστεςαπάντησαν με υψηλόποσοστό της τάξεως 85,3% όχι, με 13,2% είπαν ναι, ενώ μόλις ένα 1,5% δήλωσε δεν γνωρίζω/δεν απαντώ.

14. ΕΧΟΥΝ ΠΑΡΑΒΙΑΣΕΙ ΠΟΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΣΑΣ ΔΕΔΟΜΕΝΑ;



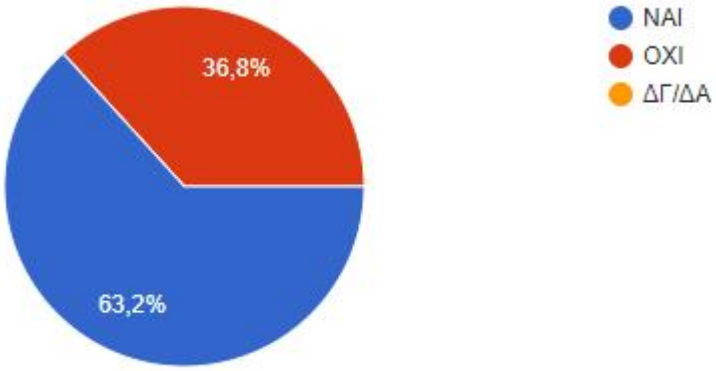
Από την παραπάνωερώτηση εάν έχουνπαραβιάσει τα προσωπικά τους δεδομένα οι χρήστεςαπάντησαν με 67,6% πως όχι δεν έχουνπαραβιαστεί, το 20,6% απάντησε ναι ,ενώ το μόλις 11,8% απάντησε δεν γνωρίζω/δεν απαντώ

15. ΕΧΕΤΕ ΛΑΒΕΙ ΠΟΤΕ ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ(SPAMMING);



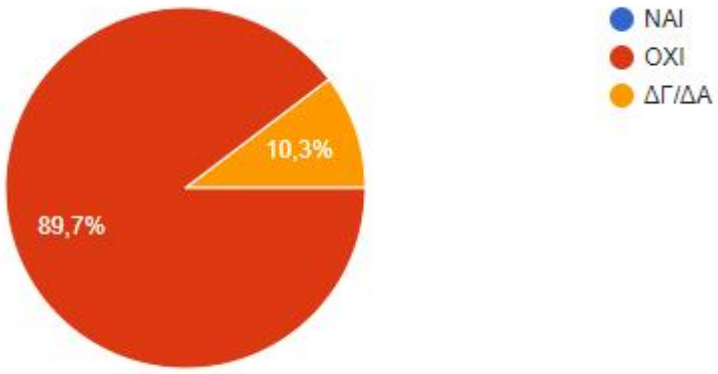
Στην ερώτηση με την ανεπιθύμητηαλληλογραφίαβλέπουμε πως το μεγαλύτεροποσοστό με 65,7% είπε ναι, το 31,8% όχι,ενώ το 3% απάντησε δεν γνωρίζω/δεν απαντώ

16. ΕΧΕΙ ΠΡΟΣΒΛΗΘΕΙ ΠΟΤΕ Ο ΥΠΟΛΟΓΙΣΤΗΣ ΣΑΣ ΑΠΟ ΙΟ;



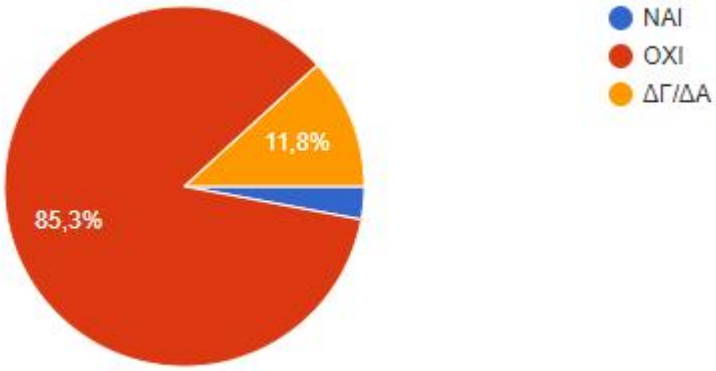
Στην ερώτηση στους χρήστες εάν ο υπολογιστής τους έχειπροσβληθεί από ιό το 63,2% απάντησεναι,και το 36,8% όχι..

17. ΕΧΕΤΕ ΕΜΠΛΑΚΕΙ ΠΟΤΕ ΣΕ ΠΟΡΝΟΓΡΑΦΙΑ ΧΩΡΙΣ ΝΑ ΤΟ ΓΝΩΡΙΖΕΤΕ;



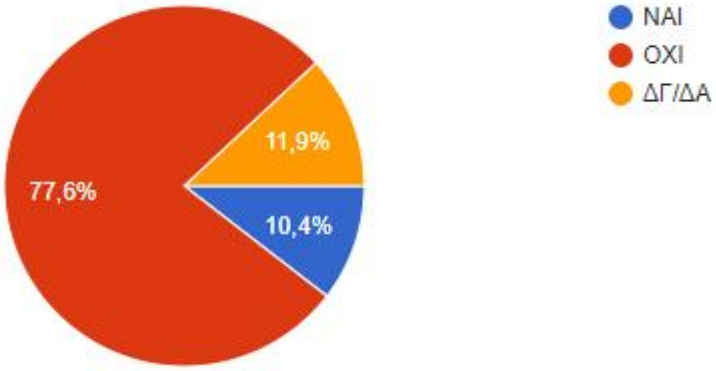
Στην ερώτηση εάν έχουνεμπλακείποτέ σε πορνογραφίαδίχως την γνώμη τους το μεγαλύτεροποσοστόαπάντησε όχι με 89,7%, ενώ το 10,3% δεν έδωσεξεκάθαρηαπάντηση και είπε δεν γνωρίζω/δεν απαντώ

18. ΕΧΟΥΝ ΠΑΡΑΒΙΑΣΕΙ ΠΟΤΕ ΤΙΣ ΠΡΟΣΩΠΙΚΕΣ ΣΑΣ ΣΥΖΗΤΗΣΕΙΣ ΜΕΣΩ ΛΟΓΑΡΙΣΜΩΝ ΣΤΑ SOCIALMEDIA(facebook,instagram,twitter κ.λ.π);



Στην ερώτηση εδώ βλέπουμε πως το μεγαλύτεροποσοστό των χρηστών με 85,3% απάντησε με όχι πως δεν έχουνπαραβιαστεί οι λογαριασμοί τους στα socialmedia , το 2,9% απάντησε πως ναι έχουνπαραβιάσει τις προσωπικέςσυζητήσεις και το 11,8% είπε δεν γνωρίζω/δεν απαντώ

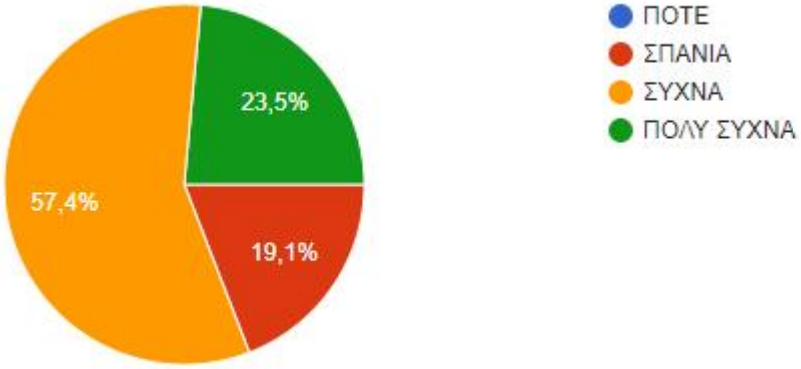
19. ΣΑΣ ΕΧΟΥΝ ΚΑΝΕΙ ΠΟΤΕ ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ;



Στην ερώτηση προς τους χρήστες εάν τους έχειγίνειποτέηλεκτρονικόψάρεμα το 77,6% είπε όχι, το 10,4% απάντησε με ναι , ενώ το 11,9% απάντησε

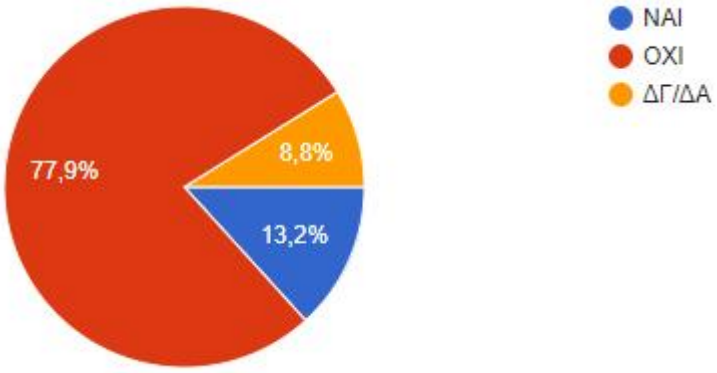
δεν γνωρίζω/δεν απαντώ

20. ΠΟΣΟ ΣΥΧΝΑ ΠΙΣΤΕΥΕΤΕ ΟΤΙ ΓΙΝΕΤΑΙ ΔΙΑΚΙΝΗΣΗ ΝΑΡΚΩΤΙΚΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ;



Στην ερώτηση ένα πιστεύουν ότι γίνεταιδιακίνησηναρκωτικώνμέσω ιντερνετ το μεγαλύτεροποσοστό με 57,4% απάντησεσυχνά, το 23,5% απάντησε πολύ συχνά, ενώ το 19,1% είπεσπάνια

21. ΕΧΕΤΕ ΕΞΑΠΑΤΗΘΕΙ ΠΟΤΕ ΜΕΣΩ ONLINE ΑΓΟΡΩΝ;



Στην ερώτηση εάν έχουνεξαπατηθείποτέμέσωonlineαγορών το μεγαλύτεροποσοστόαπάντησε όχι με 77,9%, το 13,2% είπε ναι, ενώ το 8,8% είπε όχι.

5.3ΣΥΜΠΕΡΑΣΜΑΤΑ ΜΕ ΒΑΣΗ ΤΟ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΤΗΣ ΕΡΕΥΝΑΣ

Τα συμπεράσματα της πιλοτικής μας έρευνας έδειξαν ότι το μεγαλύτερο ποσοστό που απάντησαν ήταν γυναίκες, σε σχέση με τους άντρες. Επίσης το μεγαλύτερο ποσοστό ήταν νεαρής ηλικίας από 18-29 που απάντησαν στο ερωτηματολόγιο. Βλέπουμε ότι οι ποιο νέοι ασχολούνται με το διαδίκτυο , ενώ υπάρχει και ένα μικρό ποσοστό ηλικίας 50 και άνω που ασχολήθηκε..

Το μεγαλύτερο ποσοστό ήταν απόφοιτοι ανώτατης εκπαίδευση (ΑΕΙ,ΤΕΙ), ενώ υπήρχε και ένα μικρό ποσοστό απόφοιτοι γυμνάσιου που ασχολούνται με διαδικτυο,ενώ οι ιδιωτικοί υπάλληλοι ήταν περισσότεροι σε σχέση με τους δημοσίους υπάλληλους..

Βλέπουμε ότι το μεγαλύτερο ποσοστό χρηστών χρησιμοποιεί στην καθημερινή του βάση το ίντερνετ,αρα συμπεραίνουμε πως τους φαίνεται αρκετά χρήσιμο και αξιόπιστο για ενημερώνονται για κάποιο διαδικτυακό έγκλημα από το ιντερνετ και όχι από κάποιο άλλο είδος μετάδοσης ειδήσεων.

Ωστόσο στην ερώτηση προς τους χρήστες τι είναι για αυτούς διαδικτυακό έγκλημα είδαμε πως πήραμε διαφορετικές απαντήσεις , συμπεραίνοντας πως το διαδικτυακό έγκλημα με μεγαλύτερο ποσοστό να πιστεύει ότι είναι ένας είδος απάτης η εξαπάτησης καθώς κάθε είδους οικονομικής εκμετάλλευσης.

Παρόλαυτα το μεγαλύτερο ποσοστό ανθρώπων δεν γνωρίζει τη νομοθεσία και το τι πρέπει να κάνει εάν πέσει θύμα ηλεκτρονικού εγκλήματος η ηλεκτρονικού εγκληματία.

Εν συνεχεία το μεγαλύτερο ποσοστό χρηστών προσέχει σχετικά με το διαδίκτυο και είναι ενήμερο γύρω από την ασφάλεια και των προσωπικών του λογαριασμών στα socialmedia αλλά και ηλεκτρονικού εκφοβισμού.

Ενώ ένα μεγάλο ποσοστό καλύπτει πως οι σημερινοί νέοι δεν γνωρίζουν πώς να διαφυλάξουν τον υπολογιστή τους από κάποιον ιό η να λάβουν spamming στο email τους.

Τέλος βλέπουμε πως το 57,4% πιστεύει ότι γίνεται συχνά διακίνηση ναρκωτικών έναντι του 19,1% που πιστεύει σπάνια, καθώς επίσης υπάρχει ένα μεγάλο ποσοστό χρηστών που δεν έχει εξαπατηθεί ποτέ μέσω online αγορών..

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τόσο η πληροφορία όσο και το έγκλημα δεν γνωρίζει σύνορα πια. Από την πιο απλή χρήση του διαδικτύου οι κίνδυνοι που ελλοχεύουν είναι αρκετοί και πολλαπλασιάζονται έχοντας ως αποτέλεσμα ο χρήστης να είναι περισσότερο ευάλωτος από οποιονδήποτε άλλον και να θυματοποιεί. Οι hackers εκμεταλλεύονται την ανωνυμία που προσφέρει το διαδίκτυο με αποτέλεσμα να έχουν την δυνατότητα να μπορούν να τελέσουν ακόμα και εγκλήματα που με τον παραδοσιακό τρόπο που δε θα τολμούσαν καν να σκεφτούν.

Είναι φανερό ότι η Διαδικτυακή Εγκληματικότητα στις μέρες μας διογκώνεται και αποτελεί την ουσία της ασφάλειας των πληροφοριακών συστημάτων της σύγχρονης ψηφιακής κοινωνίας. Η αυξανόμενη χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου καθώς και οι γενικότερες αλλαγές που επέφεραν οι καινοτόμες τεχνολογίες, έχουν δώσει νέες διαστάσεις στη συμβατική εγκληματικότητα καθιστώντας την αρκετά απειλητική και επικίνδυνη τόσο στους μέσους όσο και στους ενημερωμένους χρήστες του ηλεκτρονικού υπολογιστή.

Αυτή η ραγδαία εξελισσόμενη πραγματικότητα όπως επίσης, και η υπερεθνική διάσταση που παίρνουν κάποια από τα διαδικτυακά εγκλήματα είναι οι βασικότεροι αιτιολογικοί παράγοντες που δυσχεραίνουν το έργο του νομοθέτη σχετικά με την ποινική αντιμετώπιση καθώς και τη δίωξη των διαφόρων περιστατικών. Από τη χρησιμοποίηση της τεχνολογίας εξελιγμένων συστημάτων και υψηλής τεχνογνωσίας χαρακτηρίζονται οι σύγχρονες εγκληματικές απειλές. Η αντιμετώπιση για κάθε οργανισμό που θα πρέπει να μεριμνά συνεχώς για την πρόληψη εκδήλωσης επιθέσεων, την ανίχνευσή τους αλλά και την άμεση αντίδραση προς αποκατάσταση της προκληθείσης ζημιάς όταν αυτή συμβεί αποτελεί ζήτημα καίριας σημασίας.

Η όλη πολιτική ασφάλεια επιβάλλει τον συνδυασμό τεχνολογικών μέτρων και συνεχούς εκπαίδευσης και επιμόρφωσης του προσωπικού όπως και των απλών οικιακών χρηστών σε θέματα ασφάλειας. Συγκεφαλαιώνοντας, όσον αφορά το έργο των αρμόδιων διωκτικών αρχών, χρειάζεται εκσυγχρονισμός των υφιστάμενων υπηρεσιών της δίωξης ηλεκτρονικού εγκλήματος καθώς και η εκπαίδευση του προσωπικού των υπηρεσιών στη μεθοδολογία διεύρυνσης εγκλημάτων στα οποία χρησιμεύει με οποιονδήποτε τρόπο η ψηφιακή τεχνολογία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

- Αργυρόπουλος Α. (2001). *Ηλεκτρονική Εγκληματικότητα.Εκδόσεις* Σάκκουλα. Αθήνα – Κομοτηνή.
- Βλαχόπουλος Κ. (2007). *Ηλεκτρονικό Έγκλημα*. Νομική Βιβλιοθήκη.
- Γουλτίδης Χρ. (2014). *Γονείς, Παιδιά και Διαδίκτυο. Εκδόσεις* Κλειδάριθμος. Αθήνα.
- Ελαφρός Γ. (2006). *Το διαδίκτυο αλλάζει άρδην την ζωή μας*. Εφημερίδα «Η Καθημερινή».
- Ζάννη Αν. (2005). *Το διαδικτυακό έγκλημα*. Αθήνα.
- Καπατζιά Αν. (2008). *Ηλεκτρονικός Εκφοβισμός*. Θεσσαλονίκη.
- Κωστάρας Α. Ποινικό Δίκαιο. (2012). Αθήνα.
- Λάζος Γρ. (2001). *Πληροφορική και έγκλημα*. Νομική βιβλιοθήκη.
- Μανωλεδάκης Ι. (2005). *Ποινικό Δίκαιο*. Ζ' έκδοση. Αθήνα.
- Παπαντωνίου Α., και Σερκετζής Ν. (2007). *Το έγκλημα παραμένει έγκλημα ακόμα και όταν πραγματοποιείται ηλεκτρονικά.*Αθήνα.
- Πιπερόπουλος Γ. (1998). *Κοινωνικά Προβλήματα. Εκδόσεις* Ελληνικά Γράμματα. Αθήνα.
- Σφακιανάκης, Ε. (2007). *Πόσο ασφαλής είναι ο νέος ασύρματος και κινητός κόσμος;* Αθήνα.
- Σφακιανάκη Εμμ., Σιώμου Κ., Φλώρου Γ. (2012). *Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου. Εκδόσεις*. Α.Α. Λιβάνη. Αθήνα.
- Τσουραμάνης Χρήστος. (2005). *Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου. Εκδόσεις* Κατσαρού Β.Ν. Αθήνα.
- Χλούπη Γ. (2000). *Νομιμοποίηση εσόδων από παράνομες δραστηριότητες: Περιγραφή του φαινομένου και τρόπου αντιμετώπισης*.Ποινικό Δίκαιο. Αθήνα.

Ξενόγλωσση Βιβλιογραφία

- BloomBecker B. (1997). *Computer Crime and Abuse, στο Hollinger Richard C.* Aldershot Hants, England, Dartmouth.
- Bigelow R. (1985). *The challenges of computer law.* Western New England Law Review.
- Broadhurst R. (2006). *Developments in the global law enforcement of cyber – crime.* Policing: An International Journal of Police Strategies and Management.
- Edwards O. (1995). *Hackers from hell.* Forbes 9.
- Hinduja S., & Patchin J. W. (2007). *Offline consequences of online victimization: School violence and delinquency.* Journal of School Violence.
- Hollinger R. (1997). *Hackers: Computer Heroes or Electronic Highwaymen.* Aldershot Hants, England, Dartmouth.
- Mali, P. (2008). *A textbook of cybercrimes and penalties.*
- Newman R. (2004). *Identity Theft.* US Department of Justice.
- Shinder D.L., & TIttel Ed. (2002). *Scene of cybercrime Computer Forensics Handbook.* Syngress Publishing.

- Thomas P.(1983). *Hughes, Networks οι Power: Electrification in Western Society Baltimore:* John Hopkins University Press.

Ξενόγλωσση Βιβλιογραφία Μεταφρασμένη στα Ελληνικά

- DorothyE. Denning (2004). *Πληροφοριακός & Ασφάλεια Πληροφοριών των Επιχειρήσεων*. Επιμέλεια: Τσουραμάνης Χρήστος. *Εκδόσεις* ΙΩΝ, Αθήνα.
- StevenF. (2006). «*Κυβερνοέγκλημα, καταστρέφοντας την κοινωνία της πληροφορίας*». μτφρ: Μηλιώνη Φωτεινή. *Εκδόσεις* Παπαζήση. Αθήνα.

Διαδικτυακές Πηγές

- http://psychografimata.com