Α Ρ Ι Σ Τ Ο Τ Ε Λ Ε Ι Ο Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο
Θ Ε Σ Σ Α Λ Ο Ν Ι Κ Η Σ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Π Τ Υ Χ Ι Α Κ Η / Δ Ι Π Λ Ω Μ Α Τ Ι Κ Η
Ε Ρ Γ Α Σ Ι Α

«ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ»

(E-crime)

«ΣΟΛΔΑΤΟΥ ΕΛΕΝΗ»

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΓΕΩΡΓΙΟΣ ΠΑΠΑΔΗΜΗΤΡΙΟΥ, ΚΑΘΗΓΗΤΗΣ
ΑΝΔΡΕΑΣ ΠΟΜΠΟΡΤΣΗΣ, ΚΑΘΗΓΗΤΗΣ

ΘΕΣΣΑΛΟΝΙΚΗ 2013

ΠΕΡΙΛΗΨΗ

Στη σημερινή εποχή, που η εξέλιξη της τεχνολογίας είναι ραγδαία, η χρήση των υπολογιστών και του Διαδικτύου είναι πλέον δεδομένη και οι ηλικίες των χρηστών ποικίλουν. Αυτό έχει ως αποτέλεσμα το Διαδίκτυο να ασκεί επιρροή σε πολλούς τομείς της καθημερινότητας μας, όπως στην παραγωγική διαδικασία, στην εκπαίδευση, στις συναλλαγές, στις καθημερινές δραστηριότητες, στη διασκέδαση, ακόμα και στον τρόπο σκέψης του σύγχρονου ανθρώπου.

Έτσι, με την πάροδο του χρόνου έχουν αναπτυχθεί νέες έννοιες όπως:

- Ηλεκτρονικό Εμπόριο (e-commerce)
- Ηλεκτρονικές τραπεζικές συναλλαγές (e-banking)
- Ηλεκτρονικό επιχειρείν (e-business)
- Ηλεκτρονική διακυβέρνηση (e-government)
- Ηλεκτρονική υγεία (e-health)
- Ηλεκτρονική μάθηση (e-learning)

Μαζί όμως με τις αλλαγές αυτές εμφανίζονται και νέες παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό έγκλημα (e-crime)». Δηλαδή μιλάμε για τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή και συστημάτων επεξεργασίας δεδομένων.

Αντικείμενο της παρούσας εργασίας είναι το ηλεκτρονικό έγκλημα.

Επειδή λοιπόν το ηλεκτρονικό έγκλημα βρίσκεται σε αυξητική τάση, δημιουργείται το ερώτημα: «Τί ακριβώς είναι το ηλεκτρονικό έγκλημα και πως μπορεί κανείς να προστατεύσει το εαυτό του και άλλους από το να γίνει θύμα μιας τέτοιας κατάστασης;».

Η παρούσα εργασία προσδοκεί να απαντήσει σε αυτά τα ερωτήματα και σε άλλα που μπορεί να προκύψουν κατά την ανάγνωση, οπως για παράδειγμα «Ποιά είναι η Νομοθεσία που ισχύει σε περιπτώσεις ηλεκτρονικών εγλημάτων;». Ο αναγνώστης έχει την ευκαιρία να διαβάσει τους ορισμούς που δίνονται για το ηλεκτρονικό έγκλημα, να ενημερωθεί για τις μορφές του και στη συνέχεια να δει αναλυτικά κάποιες από αυτές.

Σχετικά με το Νομοθετικό πλαίσιο παρατίθενται τα άρθρα του ελληνικού ποινικού κώδικα που σχετίζονται με το ηλεκτρονικό έγκλημα, καθώς 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.

Τέλος, υπάρχουν συμβουλές για την ασφάλεια του χρήστη υπολογιστή κατά την περιήγησή του στον κόσμο του Διαδικτύου.

ABSTRACT

Nowadays that technological development is rapid, the use of computers and the Internet are popular. This fact makes the internet an influence on many areas of our everyday life, such as the production process, education, the banking area, daily activities, entertainment, and even the way of thinking of the modern people.

So, new concepts have been developed such as:

- E-commerce
- E -banking
- E -business
- E -government
- E -health
- E -learning

But along with these changes, new parameters occur that help the development of new forms of crime. These new forms of crime are enacted by the term “E-crime”. So, we are talking about criminal offenses committed by using computers and data processing systems.

Object of this thesis is the e-crime.

So, because of the increasing trend of cybercrime, a question arises: “What exactly is cyber crime and how one can protect himself and others from becoming a victim of such a situation?”.

This thesis hopes to answer these questions and others that may arise during reading it, such as "What is the law that applies in the case of cybercrimes?". The reader has the opportunity to read the definitions given for cybercrime, to be informed of the forms of cybercrime and then see some details about them.

The thesis lists the articles of the Greek Penal Code related to cybercrime, as in Greek law there are no laws that refer exclusively to internet issues regulating the behavior of internet users in terms of criminal law.

Finally, there are safety tips for the computer user while browsing in the internet world.

ΕΥΧΑΡΙΣΤΙΕΣ

Πριν την παρουσίαση των αποτελεσμάτων της παρούσας εργασίας, αισθάνομαι την υποχρέωση να ευχαριστήσω ορισμένους από τους ανθρώπους που γνώρισα, συνεργάστηκα μαζί τους και έπαιξαν πολύ σημαντικό ρόλο στην πραγματοποίησή της.

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον Καθηγητή Γεώργιο Παπαδημητρίου και στον αποβιώσαντα Καθηγητή Ανδρέα Πομπόρτση. Οι σημαντικές υποδείξεις και συμβουλές τους με κατεύθυναν σ' ένα σωστό τρόπο σκέψης και μου προσέφεραν σημαντικά εφόδια για την μετέπειτα ζωή μου.

Τέλος, θέλω να εκφράσω ένα τεράστιο ευχαριστώ στην οικογένεια μου, για την στήριξη και την εμπιστοσύνη που μου έδειξε όλα αυτά τα χρόνια των σπουδών μου.

19/10/2013

Σολδάτου Ελένη

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

ΕΙΣΑΓΩΓΗ

Αντικείμενο της παρούσας εργασίας είναι το «Ηλεκτρονικό έγκλημα».

Η εργασία δομείται σε κεφάλαια ως εξής:

- Στο Κεφάλαιο 2, Γενικές πληροφορίες και ορισμοί σχετικά με το ηλεκτρονικό έγκλημα. Στην υποενότητα 2, παρατίθεται ταξινόμηση των ηλεκτρονικών εγκλημάτων. Στην υπονότητα 3, βλέπουμε τα χαρακτηριστικά του εγκλήματος στο Διαδίκτυο
- 37. Στο Κεφάλαιο 3, Μορφές ηλεκτρονικού εγκλήματος και περαιτέρω πληροφορίες σχετικά με το κακόβουλο λογισμικό, τα spam
- 38, τους χάκερ 40, τα adware)42, riskware, pornware) 43 και spyware 71, τις απάτες στο Διαδίκτυο 73 και τα cookies. Στη συνέχεια βλέπουμε κάποια στατιστικά 74 στοιχεία, καθώς και κάποια παραδείγματα ηλεκτρονικών εγκλημάτων. Στο Κεφάλαιο 4, Νομοθετικό πλαίσιο στην Ελλάδα. Στην υποενότητα 2, υπάρχουν παραδείγματα νομοθεσίας σχετικής με το ηλεκτρονικό έγκλημα στο εξωτερικό. Στην υποενότητα 3, αναφέρονται πληροφορίες σχετικά με τα πνευματικά δικαιώματα.
- Στο Κεφάλαιο 5, Συμβουλές ασφαλείας. Στις υποενότητες 1 και 2, παρατίθενται συμβουλές για την προστασία κατά την περιήγηση στο Διαδίκτυο και για ασφαλείς οικονομικές συναλλαγές. Στις υποενότητες 3, 4 και 5, από spam, κακόβουλο λογισμικό και παρενοχλήσεις. Τέλος, στις υποενότητες 6 και 7, θα βρει κανείς πληροφορίες για τα λογισμικά φίλτρα και τα λογισμικά antivirus.
- Στο Παράρτημα Ι παρουσιάζονται η βιβλιογραφία και οι δικτυακοί τόποι από τους οποίους αντλήθηκαν πληροφορίες που αναφέρονται στην εργασία.
- Στο Παράρτημα ΙΙ παρουσιάζονται τα ακρωνύμια τα οποία χρησιμοποιούνται σε αυτή την εργασία για την διευκόλυνση του αναγνώστη.
- Στο Παράρτημα ΙΙΙ παρουσιάζεται το γλωσσάριο όρων οι οποίοι χρησιμοποιούνται σε αυτή την εργασία για την διευκόλυνση του αναγνώστη.
- Στο Παράρτημα IV παρουσιάζεται το ευρετήριο των όρων οι οποίοι χρησιμοποιούνται σε αυτή την εργασία για την διευκόλυνση του αναγνώστη.

Εικόνα 1: Cyber attack

ΚΕΦΑΛΑΙΟ 2: ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ-ΟΡΙΣΜΟΙ

ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ - ΟΡΙΣΜΟΙ

Στο κεφάλαιο αυτό θα δούμε, τους επικρατέστερους ορισμούς που δίνονται για τον όρο «Ηλεκτρονικό έγκλημα». Στη συνέχεια τα ηλεκτρονικά εγκλήματα ταξινομούνται σε κατηγορίες ανάλογα με το αν είναι βίαια ή όχι και τα χαρακτηριστικά του εγκλήματος στον κυβερνοχώρο.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: *e-crime, cybercrime, computer-crime, internet related crime και hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα, δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

2.1 ΟΡΙΣΜΟΙ ΤΟΥ ΟΡΟΥ «ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ»

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα.

Ένας ορισμός που δόθηκε από τους T. Forester and P. Morrison [1] προσδιόρισε το ηλεκτρονικό έγκλημα ως *«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της»*.

Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε [6]. Υιοθετώντας μια τριπλή προσέγγιση που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- Μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- Μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ΄ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής

Σύμφωνα με τους Debarati Halder και Dr. K. Jaishankar [2], ως εγκλήματα στον κυβερνοχώρο ορίζονται εγκλήματα που διαπράττονται εις βάρος ατόμων ή ομάδων ατόμων με κίνητρο να βλάψουν σκόπιμα τη φήμη του θύματος ή να προκαλέσουν σωματική ή ψυχική βλάβη στο θύμα, άμεσα ή έμμεσα, με τη χρήση σύγχρονων τηλεπικοινωνιακών δικτύων, όπως το Διαδίκτυο (chat rooms, e-mail, πίνακες ανακοινώσεων και ομάδες) και κινητών τηλεφώνων (SMS / MMS). Τα εγκλήματα αυτά μπορούν ακόμα να απειλήσουν την ασφάλεια ενός έθνους και την οικονομική υγεία.

Ο ορισμός που δίνεται από την Ελληνική Αστυνομία είναι ο εξής:

Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, 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. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου [7].

Συνοπτικά, ένα ηλεκτρονικό έγκλημα λαμβάνει χώρα όταν τα δίκτυα ή οι υπολογιστές είναι:

1. Εργαλεία του εγκλήματος
2. Στόχοι του εγκλήματος
3. Μέσα αποθήκευσης & καταγραφής στοιχείων που αφορούν το έγκλημα

2.2 ΤΑΞΙΝΟΜΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Η ταξινόμηση των ηλεκτρονικών εγκλημάτων τα κατατάσσει σε δύο κατηγορίες. Αυτά που δεν εμπεριέχουν τη χρήση βίας ή μπορεί ένα βίαιο επεισόδιο να λάβει χώρα ως επιπλοκή και αυτά που εμπεριέχουν τη χρήση βίας [3].

Μη βίαια ηλεκτρονικά εγκλήματα:

- Παρακολούθηση δικτυακών πόρων (cybertresspassing) : Προσπέλαση ηλεκτρονικών δεδομένων χωρίς τροποποίηση, χωρίς υστεροβουλία (πειραματικό hacking) ή με σκοπό την παρακολούθηση και συγκέντρωση πληροφοριών από πρόσβαση σε προσωπικά δεδομένα που δε διαμοιράζονται με πρωτοβουλία του ιδιοκτήτη τους.
- Διαδικτυακή απάτη: Δημιουργία διαδικτυακών τόπων πλαστών επενδύσεων και παρακίνηση των χρηστών για συμμετοχή σε αυτούς με παραπλάνηση και ψευδή στοιχεία.
- Διαδικτυακή κλοπή: Κλοπή πνευματικής ιδιοκτησίας, κλοπή ταυτότητας, αντιγραφή κειμένων χωρίς αναφορά, κατάχρηση χρηματικών πόρων τρίτων, κατάχρηση DNS με σκοπό την ανακατεύθυνση διαδικτυακής κίνησης.
- Καταστροφή υπολογιστικών πόρων: Παρέμβαση και καταστροφή ή αλλαγή διαδικτυακής και υπολογιστικής υποδομής που ανήκει σε τρίτους. Hacking, SQL injections, αποστολή malware όπως Trojan horses και worms.
- Παράνομος τζόγος
- Εμπόριο ναρκωτικών ουσιών
- Διαφήμιση πορνογραφικού υλικού

Βίαια ή δυνητικά βίαια ηλεκτρονικά εγκλήματα:

- Τρομοκρατία στον κυβερνοχώρο: Αφορά τρομοκρατικές ενέργειες που διαπράττονται, σχεδιάζονται ή συντονίζονται μέσω του ίντερνετ. Εμπεριέχει την

αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου για συνεννόηση των μελών μιας οργάνωσης και τη χρήση ιστοσελίδων ή ηλεκτρονικών ομάδων για τη στρατολόγηση νέων μελών. Κλασικά παραδείγματα μπορούν να θεωρηθούν η πρόκληση βλάβης στο υπολογιστικό σύστημα ελέγχου εναέριας κυκλοφορίας με σκοπό την πρόκληση σύγχυσης ή τη σύγκρουση αεροσκαφών και η παραποίηση μιας βάσης δεδομένων ενός νοσοκομείου.

- Επίθεση με απειλή: Αφορά την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την απειλή κατά της ζωής του παραλήπτη, αλλά και απειλές για τοποθέτηση βόμβας ή σαμποτάζ σε επιχειρήσεις και γραφεία.
- Κατασκοπία μέσω διαδικτύου (cyberstalking) : Πρόκειται για μορφή ηλεκτρονικής παρενόχλησης, που συχνά περιέχει άμεσες ή έμμεσες σωματικές απειλές που προκαλούν φόβο στο θύμα και θα μπορεί να κλιμακωθούν σε πραγματική παρακολούθηση και βίαιη συμπεριφορά.
- Παιδική πορνογραφία: Περικλείει μια πληθώρα συμμετεχόντων στα συμβάντα. Ανθρώπους που δημιουργούν το υλικό χρησιμοποιώντας μικρά παιδιά, ανθρώπους που ασχολούνται με τη διανομή του υλικού και ανθρώπους που αποκτούν πρόσβαση σε αυτό.
- Παραδοσιακό έγκλημα με ηλεκτρονική υπόσταση: Οποιαδήποτε εγκληματική πράξη (φόνος, ηθική αυτουργία σε αυτοκτονία, κακοποίηση), μέρος της οποίας έχει λάβει χώρα με τη χρήση ηλεκτρονικών υπολογιστών και δικτύων.

2.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Σε αυτή την ενότητα παρατίθενται τα χαρακτηριστικά του εγκλήματος στον κυβερνοχώρο, μαζί με μια σύντομη περιγραφή.

Τα χαρακτηριστικά του εγκλήματος στον κυβερνοχώρο είναι τα εξής:

- Είναι γρήγορο, δηλαδή διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στη διάπραξή του, μιλώντας φυσικά για όσους γνωρίζουν τον τρόπο να το διαπράξουν.
- Για την τέλεσή του δεν απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς τη φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σε όσους έχουν ροπή ή τάση στην παιδοφιλία ή τη χρήση υλικού παιδικής πορνογραφίας να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζήτησης.
- Χαρακτηρίζεται ως έγκλημα «χωρίς πατρίδα», παρόλο που τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους.

- Είναι κατά κανόνα, πολύ δύσκολο να προσδιοριστεί ο πραγματικός τόπος τέλεσής του. Κατά τεκμήριο για τη διερεύνησή του απαιτείται συνεργασία δυο τουλάχιστον κρατών, δηλαδή του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία. Οι περιπτώσεις που το έγκλημα στον κυβερνοχώρο περιορίζεται στα όρια ενός μόνο κράτους είναι ελάχιστες και σπάνιες.
- Δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον ελληνικό, αλλά και στον διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται. Αυτό συμβαίνει για να μην αμφισβητείται η αξιοπιστία των παθόντων, οι οποίοι κατά κανόνα είναι εταιρείες. Συνεπώς, ο «σκοτεινός αριθμός» της εγκληματικότητας στο χώρο του διαδικτύου είναι «ακόμα πιο σκοτεινός», από ότι στον κοινό εγκληματικό χώρο.
- Η αστυνομική διερεύνησή του είναι πολύ δύσκολη και απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Επίσης απαιτούνται και όσοι άλλοι ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (εισαγγελείς, δικαστές, δικηγόρους) να έχουν κι εκείνοι εξειδικευμένες γνώσεις[8].

Όσον αφορά αποκλειστικά το ηλεκτρονικό έγκλημα, βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ένας ηλεκτρονικός υπολογιστής, ένα κινητό τηλέφωνο,ένα palmtop, notepad κλπ.

Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί [5]:

- **Να αποτελεί τον στόχο κάποιας επίθεσης**. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.
- **Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης**, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).
- **Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος**, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες[3],[5].

Εικόνα 2: Joseph-Marie Jacquard

Το πρώτο "Ηλεκτρονικό Έγκλημα"

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό.

Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία [6].

ΚΕΦΑΛΑΙΟ 3: ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στο κεφάλαιο αυτό θα δούμε τις μορφές του ηλεκτρονικού εγκλήματος περιγράφοντας συνοπτικά την καθεμία και ύστερα θα αναλύσουμε παραπέρα κάποιες πτυχές τους.

Τέλος, θα δουμε κάποια στατιστικά στοιχεία για το 2011 και 2012, καθώς και παραδείγματα ηλεκτρονικών εγκλημάτων που έχουν διαπραχθεί στην Ελλάδα και στο εξωτερικό.

3.1 ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Μπορούμε να τις χωρίσουμε στις παρακάτω κατηγορίες[6],[8]:

- **Κακόβουλες εισβολές σε δίκτυα (Hacking και cracking)**

  Κακόβουλη εισβολή σε δίκτυα υπολογιστών ονομάζεται η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει κάποιου είδους ζημιά ή να αποκομίσει οικονομικό όφελος και είναι κακόβουλος, τότε αναφέρεται ως cracker,ενώ σε αντίθετη περίπτωση ως hacker.

- **Επιθέσεις Άρνησης Εξυπηρέτησης**

  Στόχος των επιθέσεων άρνησης εξυπηρέτησης είναι η εξάντληση των πόρων ενός υπολογιστή ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με τη διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό.

- **Κακόβουλο λογισμικό**

  Το κακόβουλο λογισμικό περιλαμβάνει προγράμματα που δημιουργούνται με σκοπό να προκαλέσουν ζημιά σε Η/Υ ή να εισχωρήσουν σε έναν Η/Υ για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τέσσερις βασικές κατηφορίες: Ιούς, (viruses), σκουλήκια (worms), Δούρειους ίππους (Trojan Horses) και Rootkits. Περισσότερες λεπτομέρειες για τη λειτουργία των παραπάνω κακόβουλων θα δούμε σε επόμενη ενότητα αναλυτικά.

- **Ανεπιθύμητη Αλληλογραφία (Spamming)**

  Ο όρος αναφέρεται κυρίως στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο. Επίσης, χρησιμοποιείται, για να καταδείξει την

αποστολή οποιοδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό, από αυτόν που το λαμβάνει.

- **Επιθέσεις σε δικτυακούς τόπους (websites)**

  Αυτού του είδους οι επιθέσεις αποσκοπούν στην αλλοίωση τον περιεχομένου ενός δικτυακού τόπου, κατά τρόπο χιουμουριστικό, προπαγανδιστικό και μερικές φορές περιλεμβάνουν προσβλητικό περιεχόμενο.

- **Ηλεκτρονικό ψάρεμα (Phising)**

  Με το phising ή αλλιώς "ηλεκτρονικό ψάρεμα" επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως για παράδειγμα ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κλπ. προκειμένου να χρησιμοποιηθούν σε άλλες παράνομες δραστηριότητες. Οι επιθέσεις αυτές στηρίζονται στην εξαπάτηση του θύματος με διάφορους τρόπους και μεθόδους όπως π.χ., την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο.

- **Πειρατεία λογισμικού**

  Πειρατεία λογισμικού ονομάζεται η παράνομη χρήση, αντιγραφή ή διάδοση λογισμικού, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.

- **Πειρατεία ψηφιακών δεδομένων**

  Ψηφιακή πειρατεία ονομάζεται η πρακτική της παράνομης αντιγραφής και πώλησης ψηφιακών δεδομένων όπως μουσικής, βίντεο κλπ, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους [9].

- **Απάτη στο Διαδίκτυο**

  Αποτελεί την ηλεκτρονική έκφανση της συμβατικής μορφής της οικονομικής απάτης. Μπορεί να συντελεστεί με διάφορους τρόπους και μεθόδους. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλλοντας επιστολές ή ενημερώσεις, όπως θα δούμε και παρακάτω.

Εικόνα 3: Internet fraud

- **Κλοπή ταυτότητας**

  Η υποκλοπή στοιχείων ταυτότητας ανυποψίαστων ατόμων και η χρήση τους για παράνομες δραστηριότητες.

- **Ξέπλυμα χρήματος**

  Η προσπάθεια εξαφάνισης χρήματος που προέρχεται από παράνομες δραστηριότητες . Χαρακτηριστικό παράδειγμα αποτελεί η αγορά μέσω του Διαδικτύου ασυνίθιστα μεγάλων ποσοτήτων αγαθών.

- **Διακίνηση παιδικού πορνογραφικού υλικού**

  Αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων.

- **Διαδικτυακή τρομοκρατία**

  Αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μιας τρομοκρατικής επίθεσης.

- **Επιθέσεις παρενόχλησης (cyberbulling)**

  Είναι μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.α.

Εικόνα 4: Κάποιες μορφές ηλεκτρονικού εγκλήματος

3.2 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Όπως αναφέρθηκε και παραπάνω το κακόβουλο λογισμικό διακρίνεται σε τέσσερις βασικές κατηφορίες: Ιούς, (viruses), σκουλήκια (worms), Δούρειους ίππους (Trojan Horses) και Rootkits. Ας δούμε την κάθε περίπτωση αναλυτικά.

3.2.1 Ιός (virus)

Ένας ιός υπολογιστή είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς την παρέμβαση του χρήστη και να μολύνει τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση.

Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, π.χ. από ένα χρήστη που στέλνει τον ιό μέσω τοπικού δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB.

Οι ιοί μπορούν επίσης να εκμεταλλευθούν υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές φορές δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημιά, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές χιουμοριστικών. Όμως, ακόμα και αυτοί οι ιοί μπορούν να δημιουργήσουν προβλήματα στον υπολογιστή του χρήστη με τον εξής τρόπο: καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash).

Επιπλέον, πολλοί ιοί είναι γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

Αξίζει να σημειωθεί οτι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα σκουλήκια υπολογιστών (worms) και τους δούρειους ίππους (trojan horses).

Ιστορία

Ο πρώτος ιός ανιχνεύθηκε στο ARPANET, τον πρόδρομο του Διαδικτύου στις αρχές της δεκαετίας του '70. Διαδόθηκε μέσω του λειτουργικού συστήματος TENEX, που χρησιμοποιούσε τότε το ARPANET και θα μπορούσε να χρησιμοποιήσει όποια σύνδεση γινόταν με το δίκτυο για να μολύνει τους συνδεδεμένους υπολογιστές. Μετά τη μόλυνση εμφάνιζε το κείμενο: "I’ m the Creeper! Catch me if you can". Σε

σύντομο χρονικό διάστημα, ωστόσο, εμφανίστηκε ένα πρόγραμμα, το οποίο ονομαζόταν "Reaper", ανώνυμου δημιουργού, το οποίο ανίχνευε τον Creeper στους υπολογιστές που είχε μολύνει και τον διέγραφε.

Ο πρώτος ιός που αναφέρεται ως εξαπλούμενος εκτός του συστήματος μέσα στο οποίο δημιουργήθηκε (ο σχετικός όρος είναι "in the wild") υπήρξε ο "Elk Cloner". Τον δημιούργησε το 1982 ο δεκαπεντάχρονος, τότε, Ρίτσαρντ Σκρέντα (Richard Skrenta) για υπολογιστές Apple II με λειτουργικό σύστημα το Apple DOS 3.3. Τον αποθήκευσε σε μια δισκέτα και την έδωσε σε φίλους και γνωστούς του. Οι περισσότεροι υπολογιστές, εκείνη την εποχή, δε διέθεταν σκληρό δίσκο κι έτσι οι ανταλλαγές δισκετών ήταν πολύ συχνές. Όταν ο υπολογιστής εκκινούσε από τη μολυσμένη δισκέτα αντιγραφόταν μόνος του σε όποια άλλη δισκέτα είχε εκείνη τη στιγμή πρόσβαση ο υπολογιστής. Ο Cloner δεν είχε καταστροφικές προθέσεις και δημιουργήθηκε από τον έφηβο Σκρέντα ως αστείο. Ωστόσο διαδόθηκε στους υπολογιστές πολλών συμμαθητών του και του καθηγητή του των μαθηματικών, εξασφαλίζοντάς του έτσι μια θέση στην ιστορία των ιών.

Ο πρώτος ιός που εμφανίστηκε στους προσωπικούς υπολογιστές ήταν ο ιός Brain, που δημιουργήθηκε στο Πακιστάν το 1986 από τους αδελφούς Basit και Amjad Farooq Alvi και προσέβαλε τον τομέα εκκίνησης (boot sector) του σκληρού δίσκου.

Από τότε έως σήμερα έχουν δημιουργηθεί και κυκλοφορήσει χιλιάδες ιοί, αρκετοί από τους οποίους είναι πολύ επικίνδυνοι, όταν προσβάλουν κάποιο υπολογιστικό σύστημα ή δίκτυο. Εκτιμάται ότι το έτος 2000 υπήρχαν περίπου 50.000 γνωστοί ιοί, ενώ σήμερα ο αριθμός τους έχει υπερβεί τις 60.000.

Οι περισσότεροι είναι γραμμένοι για υπολογιστές με λειτουργικά συστήματα MS-DOS και/ή Windows. Αυτό πιστεύεται ότι οφείλεται είτε στην αυξημένη διάδοση των συστημάτων αυτών, είτε στα κενά ασφάλειας που παρουσιάζουν και κάνουν ευκολότερη τη μόλυνση του συστήματος και τη διάδοσή τους [10].

Εικόνα 5: Computer virus

Τύποι ιών

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

- Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:
  - Τομείς σκληρού δίσκου συστήματος (system sectors)

- Αρχεία
- Ιοί μακροεντολών (Macro Viruses)
- Ιοί πηγαίου κώδικα (Source Code Viruses)
- Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters)

- Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:
  - Πολυμορφικοί ιοί
  - Αόρατοι ιοί (Stealth Viruses)
  - Θωρακισμένοι ιοί (Armored Viruses)
  - Πολυτμηματικοί ιοί (Multipartite Viruses)
  - Ιοί πλήρωσης κενών (Spacefiller Viruses)
  - Ιοί παραλλαγής (Camouflage Viruses)

Ας δούμε αναλυτικά κάποιους τύπους ιών:

Ιοί μακροεντολών (macro viruses):

Macro viruses είναι οι ιοί αυτοί που βρίσκονται σε αρχεία προγράμματος. Η διάδοσή τους γίνεται μέσω διαδικτύου χωρίς να χρειάζεται να επισυνάπτονται σε κάποιο αρχείο. Μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία ενός υπολογιστή και στη συνέχεια να στέλνουν αντίγραφα του εαυτού τους σε υποψήφια θύματα. .

Για την προστασία του χρηστή από τους ιούς, οι εταιρείες αντιβιοτικού λογισμικού προσφέρουν το αντίστοιχο λογισμικό για την αντιμετώπιση τους. Ωστόσο, οι αόρατοι ιοί (stealth) προβλέποντας αυτές τις κινήσεις, παραμένουν ενεργοί, κάνοντας τις καταστροφικές λειτουργίες τους χωρίς να μπορούν να εντοπιστούν από το εκάστοτε αντιβιοτικό λογισμικό.

Πολυμορφικοί ιοί:

Οι πολυμορφικοί ιοί (Polymorphic, self-mutating) παράγουν αντίγραφα του εαυτού τους, διαφορετικά μεταξύ τους αλλά το ίδιο καταστροφικά. Τα αντίγραφα δημιουργούν ένα «θόρυβο» με αποτέλεσμα να μην εντοπίζονται από τα antivirus [11].

Ιοί περιοχής εκκίνησης
Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα και ήταν οι πρώτοι ιοί που εμφανίστηκαν.

Ιοί αρχείων

Σ’ αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία, που προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα αυτών των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του

κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

3.2.2 Σκουλήκι (worm)

Τα σκουλήκια είναι και αυτά κακόβουλα προγράμματα με συμπεριφορά παρόμοια με τους ιούς. Διαφέρουν όμως σε μερικά σημαντικά σημεία:

Αρχικά, είναι κατασκευασμένα για να μεταδοθούν μέσα από το δίκτυο και όχι τόσο μέσα από φυσικά μέσα (δισκέτες και CD). Επίσης σπάνια απαιτείται η αλληλεπίδραση με τον χρήστη. Είναι προγραμματισμένα έτσι ώστε να μολύνουν έναν υπολογιστή αυτόματα και αθόρυβα. Συνήθως χρησιμοποιούν κάποιο κενό ασφαλείας του λειτουργικού συστήματος και βασισμένα σε αυτό καταφέρνουν να κερδίσουν την πρόσβαση στον υπολογιστή που δέχεται επίθεση. Αυτό σημαίνει ότι απλά και μόνο συνδέοντας τον υπολογιστή σας στο δίκτυο κινδυνεύετε από σκουλήκια, σε αντίθεση με τους ιούς όπου συνήθως απαιτείται η παρέμβαση του χρήστη (π.χ. εκτέλεση ενός προγράμματος, αντιγραφή δισκέτας κ.ά.).

Ένα σκουλήκι σπάνια έχει σκοπό την ολοκληρωτική καταστροφή του υπολογιστή που μολύνει. Συνήθως ο υπολογιστής μετατρέπεται σε ένα πλήρως ελεγχόμενο από μακριά σύστημα που θα χρησιμοποιηθεί για την επίθεση του σκουληκιού σε άλλους υπολογιστές ή και για εντελώς διαφορετικές επιθέσεις. Πολύ συχνά επίσης χρησιμοποιείται και για άλλους σκοπούς που εξυπηρετούν τους κακόβουλους δημιουργούς του σκουληκιού.

Τέλος, ένα σκουλήκι είναι πλήρως αυτοματοποιημένο και δεν χρειάζεται καμία ανθρώπινη παρέμβαση από τον δημιουργό του μετά την κατασκευή του. Αρχικά σαρώνει ένα μέρος του διαδικτύου και ψάχνει για ευάλωτους υπολογιστές. Μολύνει όσους μπορεί και μεταφέρει ένα αντίγραφο του εαυτού του σε καθέναν. Κατόπιν τα ίδια τα αντίγραφα σαρώνουν από ένα μικρό, αλλά διαφορετικό μέρος του διαδικτύου και προσπαθούν να μολύνουν και αυτά άλλους υπολογιστές οι οποίοι με την σειρά τους θα προσπαθήσουν να κάνουν το ίδιο.

Το τελικό αποτέλεσμα είναι ότι ένας μολυσμένος υπολογιστής δεν παρουσιάζει κάποιο εμφανές πρόβλημα όσο λειτουργεί. Με εξαίρεση μια μικρή καθυστέρηση στο δίκτυο που δύσκολα γίνεται αντιληπτή από μη ειδικούς χρήστες ο υπολογιστής φαίνεται να λειτουργεί φυσιολογικά και είναι μολυσμένος χωρίς να το ξέρει ο χρήστης του.

Από τα πιο καταστροφικά σκουλήκια ήταν το Code Red II που μόλυνε σε 14 ώρες 359.000 υπολογιστές προκαλώντας ζημία που ξεπερνούσε τα δύο δις. δολάρια.

Εικόνα 6: Computer worm

Ιστορία

Ο όρος "σκουλήκι"(worm) χρησιμοποιήθηκε για πρώτη φορά στο μυθιστόρημα του John Brunner, το 1975, με τίτλο "The Shockwave Rider". Σε αυτό το μυθιστόρημα ο Nichlas Halfinger σχεδίασε και εξαπέλυσε ένα σκουλήκι συλλογής δεδομένων σε μία πράξη εκδίκησης εναντίον κάποιων ισχυρών ανθρώπων οι οποίοι λειτουργούσαν έναν εθνικό ηλεκτρονικό ιστό πληροφοριών που παρακινούσε τη συμμόρφωση μάζας.

Στις 2 Νοεμβρίου του 1988, ο Robert Tappan Morris, μεταπτυχιακός φοιτητής της επιστήμης υπολογιστών του πανεπιστημίου Κορνέλ, εξαπέλυσε ένα σκουλήκι που έγινε γνωστό ως "σκουλήκι Morris", διαταράσσοντας ίσως και το 10% των υπολογιστών του Διαδικτύου τότε. Το 1989 ο Morris ήταν ο πρώτος άνθρωπος που κατηγορήθηκε με βάση νόμο των ΗΠΑ περί Ηλεκτρονικής Απάτης και Κατάχρησης [12].

3.2.3 Δούρειος Ίππος (Trojan Horse)

Ο δούρειος ίππος (trojan horse ή απλά trojan) είναι και αυτό ένα κακόβουλο πρόγραμμα υπολογιστή. Το όνομά του προκύπτει από την Ιλιάδα του Ομήρου, όπου αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στο εσωτερικό του οποίου κρύβονταν Αχαιοί πολεμιστές. Με τον τρόπο αυτό ξεγέλασε τους κάτοικους της Τροίας, εισήγαγε τον στρατό των Αχαιών μέσα στην πόλη και την κυρίευσε. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, οπότε πήραν και αυτήν την ονομασία.

Πιο συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου.

Εικόνα 7: Δούρειος ίππος

Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία και δεν είναι σε θέση να αυτοαναπαράγονται [13].

Τα trojans μπορούν να ταξινομηθούν ανάλογα με το είδος των ενεργειών που μπορούν να εκτελέσουν στον υπολογιστή του χρήστη [14]:

- Backdoor Trojan

Ένα Backdoor Trojan επιτρέπει σε κακόβουλους χρήστες να έχουν απομακρυσμένο έλεγχο των μολυσμένων υπολογιστών. Δίνουν τη δυνατότητα στο δημιουργό να κάνει ό, τι επιθυμεί στο μολυσμένο υπολογιστή - συμπεριλαμβανομένων την αποστολή, τη λήψη, την έναρξη και τη διαγραφή αρχείων, εμφάνιση των δεδομένων και την επανεκκίνηση του υπολογιστή. Ένα Backdoor Trojan συχνά χρησιμοποιείται για να ενώσει μια ομάδα υπολογιστών των θυμάτων σχηματίζοντας έτσι ένα δίκτυο που μπορεί να χρησιμοποιηθεί για εγκληματικούς σκοπούς.

- Exploit Trojan

Τα Exploit Trojans είναι είναι προγράμματα που περιέχουν δεδομένα ή κώδικα που εκμεταλλεύεται τα τρωτά σημεία στο λογισμικό εφαρμογών που τρέχει στον υπολογιστή του χρήστη.

- Rootkit Trojan

Τα Rootkit Trojans είναι σχεδιασμένα να αποκρύπτουν ορισμένες δραστηριότητες στον υπολογιστή του χρήστη. Συχνά ο κύριος σκοπός τους είναι να εμποδίζουν τον εντοπισμό κακόβουλων προγραμμάτων, προκειμένου να παραταθεί η περίοδος κατά την οποία τα προγράμματα τρέχουν σε ένα μολυσμένο υπολογιστή.

- Trojan-Banker

Τα Trojan-Banker είναι προγράμματα που έχουν σχεδιαστεί για να κλέβουν τα στοιχεία του λογαριασμού που χρησιμοποιεί ο χρήστης για online τραπεζικά

συστήματα, συστήματα ηλεκτρονικών πληρωμών και πιστωτικές ή χρεωστικές κάρτες.

- Trojan-DdoS

Τα προγράμματα αυτά διεξάγουν DoS επιθέσεις (Denial of Service- άρνηση εξυπηρέτησης) κατά μια στοχευμένη διαδικτυακή διεύθυνση. Με την αποστολή πολλαπλών αιτήσεων, από τον υπολογιστή του χρήστη και πολλών άλλων μολυσμένων υπολογιστών, η επίθεση μπορεί να κατακλύσει τη διεύθυνση στόχου, οδηγώντας έτσι σε άρνηση εξυπηρέτησης.

- Trojan-Downloader

Τα Trojan-Downloader μπορούν να κατεβάσουν και να εγκαταστήσουν νέες εκδόσεις των κακόβουλων προγραμμάτων στον υπολογιστή του χρήστη.

- Trojan-Dropper

Αυτά τα προγράμματα που χρησιμοποιούνται από χάκερ είτε για να εγκαθιστούν Trojans ή / και ιούς, είτε για να αποφευχθεί η ανίχνευση κακόβουλων προγραμμάτων. Δεν είναι όλα τα προγράμματα προστασίας από ιούς ικανά να σαρώνουν όλα τα συστατικά στο εσωτερικό αυτού του τύπου Trojan.

- Trojan-GameThief

Αυτός ο τύπος προγράμματος κλέβει τις πληροφορίες λογαριασμού χρήστη από online gamers.

- Trojan-IM

Τα Trojan-IM προγράμματα κλέβουν στοιχεία και κωδικούς πρόσβασης των χρηστών για τα προγράμματα ανταλλαγής άμεσων μηνυμάτων - όπως το ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype και πολλά άλλα.

- Trojan-Ransom

Τα Trojan-Ransom μπορούν να τροποποιήσουν τα δεδομένα στον υπολογιστή του χρήστη, έτσι ώστε ο υπολογιστής να μη λειτουργεί σωστά ή να μη μπορεί πλέον να χρησιμοποιήσει συγκεκριμένα δεδομένα.

- Trojan-SMS

Τα προγράμματα αυτά μπορεί να κοστίσουν χρήματα στον χρήστη, με την αποστολή μηνυμάτων κειμένου από το κινητό του σε τηλέφωνικούς αριθμούς που χρεώνουν για υπηρεσίες.

- Trojan-Spy

Τα Trojan-Spy προγράμματα μπορούν να κατασκοπεύσουν τον τρόπο που χρησιμοποιεί ένας χρήστης τον υπολογιστή του, πχ με την παρακολούθηση των δεδομένων που εισάγει μέσω του πληκτρολογίου του, δημιουργώντας screen shots, δηλαδή αρχεία εικόνας με την απεικόνιση της οθόνης του υπολογιστή, ή λαμβάνοντας μια λίστα με τις εφαρμογές που τρέχουν.

- Trojan-Mailfinder

Τα προγράμματα αυτά μπορούν να συλλέγουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τον υπολογιστή του χρήστη.

- Άλλοι τύποι των Trojans είναι και οι εξής:

- Trojan-ArcBomb
- Trojan-Clicker
- Trojan-Notifier
- Trojan-Proxy
- Trojan-PSW

3.2.4 Rootkit

Το rootkit είναι λογισμικό το οποίο μπορεί να ανήκει πολύ εύκολα σε οποιαδήποτε από τις παραπάνω κατηγορίες. Αυτό το λογισμικό έχει την ιδιαιτερότητα να κρύβει κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας και να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών. Κάποιες φορές λειτουργούν προστατευτικά για τους χάκερ διαγράφοντας τις πληροφορίες του εισβολέα. Η ανίχνευση ενός rootkit είναι δύσκολη επειδή μπορεί να είναι σε θέση να αλλάξει ακόμα και το λογισμικό που προορίζεται για την εύρεσή του.

Ο όρος αναφερόταν αρχικά σε κακόβουλα προγράμματα τα οποία αντικαθιστούσαν βασικά διαχειριστικά εργαλεία για λειτουργικά συστήματα τύπου Unix. Αν κάποιος κατάφερνε να αντικαταστήσει κάποιο από αυτά σε έναν υπολογιστή αποκτούσε τον πλήρη έλεγχο αλλά, παράλληλα, έχοντας δικαιώματα υπερχρήστη μπορούσε να κρύβει και τα ίχνη του. Το πρώτο γνωστό rootkit για προσωπικούς υπολογιστές που έχει αναλυθεί ήταν ο ιός Brain [15].

Μόνιμα Rootkits:

Ένα μόνιμο rootkit σχετίζεται με ένα κακόβουλο πρόγραμμα που ενεργοποιείται κάθε φορά που ο υπολογιστής ξεκινά. Προκειμένου να ενεργοποιείται αυτόματα ο κώδικας του rootkit, πρέπει να αποθηκεύεται σε ένα μόνιμο σημείο, όπως το Μητρώο Εκκίνησης ή το σύστημα αρχείων και να βρει έναν τρόπο ενεργοποίησης χωρίς την παρέμβαση του χρήστη.

Rootkits βασιζόμενα στη Μνήμη:

Τα rootkits που βασίζονται στη Μνήμη είναι κακόβουλα προγράμματα που δεν έχουν μόνιμο κώδικα και γι’ αυτό δεν ενεργοποιούνται μετά από επανεκκινηση του υπολογιστή.

Rootkits σε επίπεδο χρήστη:

Υπάρχουν πολλοί τρόποι με τους οποίους τα rootkits προσπαθούν να αποφύγουν την ανίχνευση. Για παράδειγμα, ένα rootkit σε επίπεδο χρήστη μπορεί να ανιχνεύει όλες τις κλήσεις στα APIs των Windows FindFirstFile/FindNextFile, τα οποία χρησιμοποιούνται από λειτουργίες διαχείρησης των αρχείων συστήματος, όπως ο Internet Explorer και η γραμμή εντολών. Όταν μια εφαρμογή εκτελεί μια καταλογογράφηση φακέλου που θα επέστρεφε τα αποτελέσματα που θα περιείχαν αρχεία σχετιζόμενα με το rootkit, το rootkit παρεμβαίνει και τροποποιεί τα αποτελέσματα της καταλογογράφησης ώστε να μη φαίνονται τα αρχεία αυτά.

Rootkits σε επίπεδο Κελύφους:

Τα rootkits σε επίπεδο κελύφους είναι ακόμα πιο ισχυρά κάθως όχι μόνο παρεμβάλλονται στα native API του επιπέδου κελύφους, αλλά μπορούν απευθείας να χειρίζονται δομές δεδομένων σε επίπεδο κελύφους. Μια συνηθισμένη τεχνική για να κρύβεται η παρουσία ενός κακόβουλου προγράμματος/διεργασίας είναι η αφαίρεση της διεργασίας από τις ενεργές διεργασίες στη λίστα του κελύφους. Αφού τα APIs που χειρίζονται διεργασίες βασίζονται στα περιεχόμενα αυτής της λίστας, η κακόβουλη διεργασία δε θα φαίνεται σε εργαλεία διαχείρισης εργασιώμ όπως το Task Manager ή το Process Explorer[16], [17].

3.3 ΑΝΕΠΙΘΥΜΗΤΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ – SPAM

Η αζήτητη ηλεκτρονική επικοινωνία, δηλαδή κάθε ηλεκτρονικό μήνυμα που αποστέλλεται με σκοπό την εμπορική προώθηση προϊόντων ή υπηρεσιών ή και κάθε άλλο διαφημιστικό σκοπό χωρίς ο παραλήπτης να έχει δώσει τη συγκατάθεσή του γι' αυτό, αναφέρεται διεθνώς με τον όρο "spam". Τα μηνύματα spam μπορεί να αποσκοπούν σε οποιονδήποτε διαφημιστικό σκοπό, π.χ. να προωθούν δράσεις φιλανθρωπικών ιδρυμάτων ή πολιτικών κομμάτων. Η πρακτική του "spamming" μπορεί να απαντηθεί σε πολλές περιπτώσεις ηλεκτρονικής επικοινωνίας, όπως:

- σε μηνύματα ηλεκτρονικού ταχυδρομείου
- στις υπηρεσίες μηνυμάτων με χρήση κινητής τηλεφωνίας (SMS, MMS)
- στις υπηρεσίες φαξ
- στις υπηρεσίες στιγμιαίων μηνυμάτων (instant messaging), π.χ. MSN, Yahoo Messenger, Google chat, κ.ά.
- στις υπηρεσίες ηλεκτρονικής ανταλλαγής μηνυμάτων, όπως σελίδες κοινωνικής δικτύωσης, π.χ. Facebook, Twitter, Myspace κ.ά.

Οι αποστολείς μηνυμάτων spam είναι γνωστοί και ως spammers.

Σε όλη την Ευρωπαϊκή Ένωση, για την αποστολή διαφημίσεων με αυτοματοποιημένα μέσα, ισχύει το λεγόμενο σύστημα "opt-in", δηλαδή η αποστολή τους επιτρέπεται μόνο κατόπιν ρητής συγκατάθεσης του παραλήπτη, με ελάχιστες εξαιρέσεις. Στα μέσα αυτά, με τα οποία η επικοινωνία πραγματοποιείται χωρίς ανθρώπινη παρέμβαση, συμπεριλαμβάνονται τα μηνύματα ηλεκτρονικού ταχυδρομείου στο διαδίκτυο, τα μηνύματα σε δίκτυα κινητής τηλεφωνίας (SMS, MMS), τα φαξ κ.λπ.

Εξαίρεση στον κανόνα αυτόν αποτελεί η περίπτωση στην οποία τα στοιχεία επικοινωνίας του παραλήπτη αποκτήθηκαν από τον αποστολέα στο πλαίσιο παρόμοιας, προηγούμενης συναλλαγής, κυρίως πώλησης παρόμοιων προϊόντων ή υπηρεσιών. Επιπλέον, σε κάθε μήνυμα, ακόμα και σε αυτά που στέλνονται με συγκατάθεση, πρέπει να αναγράφεται η ταυτότητα του αποστολέα και να παρέχεται ένας έγκυρος τρόπος τερματισμού της περαιτέρω αποστολής τέτοιων μηνυμάτων[18],[19].

Συνοψίζοντας τα σημαντικά σημεία για τα ανεπιθύμητα μηνύματα/SPAM είναι τα εξής:

- *Δεν* αποτελούν κίνδυνο για τον υπολογιστή του χρήστη. Αν ένα email είναι επικίνδυνο τότε πέφτει στην κατηγορία των ιών.
- Καταναλώνουν απλά χώρο στην ηλεκτρονική θυρίδα του χρήστη.

- Τα μηνύματα αυτά δεν στέλνονται προσωπικά. Έτυχε απλά η ηλεκτρονική διεθύνση του χρήστη να βρίσκεται μέσα σε μία λίστα με άπειρες άλλες ηλεκτρονικές θυρίδες που χρησιμοποίησε μια εταιρία.
- Για κανένα λόγο δεν πρέπει να απαντηθεί ένα τέτοιο μήνυμα. Σε περίπτωση ααπάντησης ο χρήστης θα αποκαλύψει στην εταιρία που έστειλε το μήνυμα ότι η ηλεκτρονική του διεύθυνση είναι πράγματι ενεργή.

3.4 ΧΑΚΕΡ (HACKERS)

Χάκερ(Hacker):

Είναι το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται. Ένας χάκερ έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι χάκερ είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες αποκαλούνται κράκερ(cracker).

Κράκερ(cracker):

Ένας κράκερ δηλαδή, είναι εκείνος που διεισδύει ή παραβιάζει την ακεραιότητα συστημάτων απομακρυσμένων μηχανημάτων, με κακή πρόθεση. Έχοντας αποκτήσει παράνομη πρόσβαση, οι κράκερς καταστρέφουν σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν σοβαρά προβλήματα στα θύματά τους.

Τα τελευταία χρόνια, οι χάκερ είναι ευρέως γνωστοί ως οι κακοί του κυβερνοχώρου και έχουν χαρακτηριστεί από την κοινωνία μας, ως εγκληματίες. Είναι γνωστοί επίσης ως crackers ή black hats. Ο όρος κράκερ χρησιμοποιήθηκε για να διακρίνει όσους αποκτούν πρόσβαση σε υπολογιστικά συστήματα, προκαλώντας όμως σ' αυτά και σοβαρές ζημιές.

Οι όροι black / white / gray hats αφορούν ομάδες των hacker ανάλογα με τις ηθικές τους αρχές. Ο όρος black hats χαρακτηρίζει τα άτομα εκείνα που έχουν υψηλή ειδίκευση στους υπολογιστές και χρησιμοποιούν τις δεξιότητές τους με μη ηθικούς τρόπους.

Οι χάκερ δεν είναι όλοι κακόβουλοι, αλλά υπάρχουν και άνθρωποι της hacking κοινότητας που εισβάλλουν σε κάποιο σύστημα στα πλαίσια των ηθικών αρχών για να αναγνωρίσουν ποια είναι τα τρωτά σημεία, οι οποίοι είναι γνωστοί και ως white hat hackers. Ένα παράδειγμα white hat hackers είναι οι υπάλληλοι εταιρειών, οι οποίοι έχουν άδεια να επιτίθενται στα δίκτυο και τα συστήματα της εταιρείας στην οποία εργάζονται για τον καθορισμό των αδυναμιών τους. Επίσης ένα παράδειγμα white hats, είναι και οι πράκτορες μιας μυστικής υπηρεσίας που χρησιμοποιούν τις ικανότητές τους στο όνομα της εθνικής ασφάλειας ή για τη διερεύνηση και την επίλυση διάφορων εγκλημάτων. Έχουν, δηλαδή, καθήκον να χρησιμοποιούν τις γνώσεις τους με τέτοιο τρόπο, ώστε να επωφεληθούν άλλοι άνθρωποι ή υπηρεσίες.

Στο μέσο των white hats και black hats βρίσκονται οι gray hats. Οι Gray hat hackers, περιλαμβάνουν τους εθελοντές hacker, δηλαδή, τα άτομα αυτά που χρησιμοποιούν τους υπολογιστές για τη διερεύνηση και την προσπάθεια να τιμωρήσουν τους υποτιθέμενους εγκληματίες του κυβερνοχώρου. Επίσης, χαρακτηρίστηκαν και ως «hacktιβιστές (hacktivists)», δηλαδή τα άτομα που χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να μεταφέρουν πολιτικά μηνύματα[20].

3.5 ADWARE

"Adware" είναι το όνομα που δίνεται σε προγράμματα που έχουν σχεδιαστεί για να εμφανίζουν διαφημίσεις στον υπολογιστή του χρήστη, να κατευθύνουν τις αιτήσεις αναζήτησης σε ιστοσελίδες διαφήμισης και μάρκετινγκ, και να συλλέγουν δεδομένα για τον χρήστη. Οι διαφημίσεις που παράγονται από adware έχουν συνήθως τη μορφή pop-up παραθύρων. Τα προγράμματα adware δεν πρέπει να συγχέονται με τα προγράμματα κατασκοπείας λογισμικού Trojan που συλλέγουν πληροφορίες χωρίς την άδειά του χρήστη. Αν το adware δεν ενημερώνει ότι συλλέγει πληροφορίες, θεωρείται ως κακόβουλο.

Πέρα από την εμφάνιση διαφημίσεων και τη συλλογή δεδομένων, τα adware δεν κάνουν γενικά γνωστή την παρουσία τους. Συνήθως, δεν υπάρχουν σημάδια του προγράμματος στο δίσκο του συστήματος του υπολογιστή του χρήστη και καμία ένδειξη στο μενού προγραμμάτων του, ότι έχουν εγκατασταθεί κάποια αρχεία στον υπολογιστή του.

Υπάρχουν δύο βασικοί τρόποι με τους οποίους τα adware μπορεί να εισβάλλουν σε έναν υπολογιστή:

- Μπορούν να συμπεριληφθούν σε ορισμένα freeware ή shareware προγράμματα (δηλαδή το λογισμικό εκείνο που είναι διαθέσιμο στους χρήστες χωρίς κόστος ή λογισμικό με άδεια δοκιμής-μια περιορισμένη έκδοση λογισμικού, η οποία διατίθεται δωρεάν προς δοκιμή για ένα συγκεκριμένο χρονικό διάστημα), ως νόμιμος τρόπος παραγωγής διαφημιστικών εσόδων που βοηθούν να χρηματοδοτήσει την ανάπτυξη και τη διανομή των freeware ή shareware προγραμμάτων.
- Μια επίσκεψη σε μια μολυσμένη ιστοσελίδα μπορεί επίσης να οδηγήσει σε παράνομη εγκατάσταση adware στον υπολογιστή του χρήστη. Συχνά χρησιμοποιείται η τεχνολογία των χάκερ. Για παράδειγμα, ένας υπολογιστής μπορεί να μολυνθεί λόγω ευπάθειας του προγράμματος περιήγησης, και μπορεί να χρησιμοποιηθούν Trojans που έχουν σχεδιαστεί για κρυφή εγκατάσταση. Τα προγράμματα adware που λειτουργούν με αυτόν τον τρόπο συχνά χαρακτηρίζονται Browser Hijackers «πειρατές του προγράμματος περιήγησης».

3.6 RISKWARE

Riskware είναι το όνομα που δίνεται σε νόμιμα προγράμματα που μπορούν να προκαλέσουν βλάβη εάν γίνονται αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες, προκειμένου να διαγράψουν, να εμποδίσουν, να τροποποιήσουν ή να αντιγράψουν τα δεδομένα, και να διαταράξουν τη λειτουργία των υπολογιστών ή των δικτύων υπολογιστών. Τα Riskware μπορεί να περιλαμβάνουν τους ακόλουθους τύπους προγραμμάτων που χρησιμοποιούνται συνήθως για νόμιμους σκοπούς:

- Απομακρυσμένα εργαλεία διαχείρισης
- IRC clients (υπηρεσίες συνδιάλεξης σε πραγματικό χρόνο μέσω Διαδικτύου)
- Dialer programs (προγράμματα που δημιουργούν σύνδεση στο Διαδίκτυο)
- Downloaders αρχείων
- Λογισμικό για την παρακολούθηση της δραστηριότητας του υπολογιστή
- Εργαλεία διαχείρησης κωδικών πρόσβασης
- Υπηρεσίες διακομιστή Internet

Τα προγράμματα αυτά δεν έχουν σχεδιαστεί για να είναι κακόβουλα, αλλά έχουν λειτουργίες που μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς. Ένα παράδειγμα αποτελούν τα προγράμματα απομακρυσμένης διαχείρισης που χρησιμοποιούνται συχνά από τους διαχειριστές συστημάτων και διαχειριστές των γραφείων υποστήριξης για τη διάγνωση και την επίλυση προβλημάτων που προκύπτουν στον υπολογιστή ενός χρήστη. Εάν όμως ένα τέτοιο πρόγραμμα έχει εγκατασταθεί στον υπολογιστή από κακόβουλο χρήστη, χωρίς τη γνώση του χρήστη, τότε ο κακόβουλος χρήστης θα έχει απομακρυσμένη πρόσβαση στον υπολογιστή του. Με πλήρη έλεγχο στο μηχάνημά του, ο κακόβουλος χρήστης θα είναι σε θέση να χρησιμοποιήσει τον υπολογιστή με σχεδόν οποιοδήποτε τρόπο επιθυμεί[21].

3.7 PORNWARE

Pornware είναι το όνομα που δίνεται σε μια κατηγορία προγραμμάτων που εμφανίζουν πορνογραφικό υλικό σε μια συσκευή. Εκτός από τα προγράμματα που ορισμένοι χρήστες μπορεί σκόπιμα να εγκαταστήσουν στους υπολογιστές τους και στις φορητές συσκευές τους για να αναζητήσουν και να εμφανίσουν πορνογραφικό υλικό, το pornware περιλαμβάνει επίσης τα προγράμματα εκείνα που έχουν εγκατασταθεί κακόβουλα, χωρίς ο χρήστης να έχει καμία γνώση της παρουσίας τους. Συχνά, ο σκοπός του ανεπιθύμητου pornware είναι να διαφημίσει με αμοιβή πορνογραφικές ιστοσελίδες και υπηρεσίες.

Οι προγραμματιστές κακόβουλου λογισμικού μπορούν να εκμεταλλευτούν τρωτά σημεία σε εφαρμογές που χρησιμοποιούνται συχνότερα ή στο λειτουργικό σύστημα, για την εγκατάσταση πορνογραφικού περιεχομένου στον υπολογιστή, στο tablet ή στο smartphone ενός χρήστη. Επιπλέον, κάποια Trojans, όπως πχ τα Trojan-Downloader και Trojan-Dropper μπορούν να χρησιμοποιηθούν για να μολύνουν μια συσκευή με πορνογραφικό περιεχόμενο. Ας δούμε κάποια παραδείγματα pornware[22]:

- Porn-Dialer
  Αυτό το είδος προγραμμάτων καλούν υπηρεσίες τηλεφωνίας με «περιεχόμενο για ενήλικες» και αριθμούς τηλεφώνου. Σε αντίθεση με άλλα κακόβουλα προγράμματα, τα Porn-Dialer ενημερώνουν τον χρήστη για τις ενέργειές τους.
- Porn-Downloader
  Αυτά τα προγράμματα κατεβάζουν πορνογραφικά αρχεία πολυμέσων στον υπολογιστή του χρήστη από το Internet. Και πάλι σε αντίθεση με άλλα κακόβουλα προγράμματα, τα Porn-Downloaders ειδοποιούν το χρήστη για τις ενέργειές τους.
- Porn-Tool
  Τα Porn-Tool προγράμματα αναζητούν και εμφανίζουν πορνογραφικό υλικό στον υπολογιστή του χρήστη. Για παράδειγμα εμφανίζουν ειδικές γραμμές

εργαλείων για τα προγράμματα περιήγησης στο Διαδίκτυο και ειδικά εργαλεία αναπαραγωγής βίντεο.

3.8 ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ (SPYWARE)

Με τον όρο Spyware (Λογισμικό Κατασκοπίας) αναφερόμαστε σε ένα είδος κακόβουλου λογισμικό το οποίο βοηθά στη συλλογή πληροφοριών σχετικά με ένα πρόσωπο ή οργανισμό χωρίς τη γνώση του και μπορεί να στείλει τις πληροφορίες αυτές σε άλλο φορέα χωρίς τη συγκατάθεση του χρήστη. Το Spyware φορτώνεται κρυφά και με ύπουλο τρόπο σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο εκτελώντας διάφορες ενέργειες χωρίς την γνώση και έγκριση του χρήστη.

Τα Spyware προγράμματα συνήθως κατατάσσονται σε τέσσερις τύπους: system monitors, trojans, adware, και εντοπισμού των cookies. Το κατασκοπευτικό λογισμικό είναι ως επί το πλείστον χρησιμοποιείται για τους σκοπούς, όπως η παρακολούθηση και αποθήκευση των κινήσεων των χρηστών του διαδικτύου στο διαδίκτυο. Το Spyware κρύβεται ώστε να μην μπορεί το θύμα να το εντοπίσει εύκολα και συγκεντρώνει στοιχεία σχετικά με το χρήστη (ιστοσελίδες που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πρόσβασης πιστωτικών καρτών). Μερικά spyware μπορούν να αλλάξουν τις ρυθμίσεις του υπολογιστή. Οι αλλαγές αυτές μπορούν να οδηγήσουν σε αργή ταχύτητα σύνδεσης στο Internet, μη εξουσιοδοτημένες αλλαγές στις ρυθμίσεις του προγράμματος περιήγησης, ή αλλαγές στις ρυθμίσεις του λογισμικού[23].

Εικόνα 8: «Κλοπή» κωδικού πρόσβασης

Η εξάπλωση του spyware λογισμικού γίνεται με τρεις τρόπους:

- Με την εγκατάσταση προγραμμάτων: Συνήθως με προγράμματα ανταλλαγής αρχείων (peer-to-peer π.χ. το Kazaa)
- Με την εγκατάσταση πρόσθετων (Add-ons): Τα Add-ons είναι προγράμματα που ενισχύουν το πρόγραμμα περιήγησης. Μπορεί να είναι γραμμές εργαλείων, κουμπιά αναζήτησης, κινούμενες εικόνες κλπ.
- Με την επίσκεψη σε δικτυακούς τόπους: Μερικοί δικτυακοί τόποι μπορούν να κατεβάσουν και να εγκαταστήσουν αυτόματα στον υπολογιστή σας spyware.

Συνοπτικά οι διεργασίες που πραγματοποιεί το Spyware είναι οι εξής:

1. Αλλαγή της αρχικής σελίδας του προγράμματος περιήγησης
2. Τροποποίηση της λίστας αγαπημένων (σελιδοδεικτών) του browser
3. Προσθήκη νέων γραμμών εργαλείων στον browser
4. Εμφανίζουν συνεχώς παράθυρα με ανεπιθύμητες διαφημίσεις
5. Ξεκινάνε μαζί με τον υπολογιστή κατά την εκκίνηση του και πιάνουν μνήμη και υπολογιστική ισχύ.
6. Το spyware κάποιες φορές απενεργοποιεί το firewall, αφαιρεί ανταγωνιστικό λογισμικό κατασκοπίας και εκτελεί άλλες κακόβουλες ενέργειες.

Τα πρώτα τρία στοιχεία αλλάζουν τη συμπεριφορά του browser, με τέτοιο τρόπο ώστε ακόμη κ η επανεκκίνηση του συστήματος δεν επαναφέρει τις προηγούμενες τιμές. Η επίθεση αυτή είναι γνωστή ως πειρατεία φυλλομετρητή (browser hijacking) [24].

3.9 ΕΠΙΘΕΣΕΙΣ ΠΑΡΕΝΟΧΛΗΣΗΣ (CYBERBULLYING)

Ο κόσμος του διαδικτύου έχει μετατραπεί τελευταία, για χιλιάδες ανήλικους, σε έναν εικονικό τόπο "μαρτυρίου", που προκαλεί αισθήματα φόβου, ντροπής και αμηχανίας σε παιδιά και εφήβους, καθώς έχει λάβει εφιαλτικές διαστάσεις ένα φαινόμενο το οποίο στη «γλώσσα» του ίντερνετ ονομάζεται Cyber Bullying.

Ο εκφοβισμός μέσω του Διαδικτύου είναι οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που θεσπίζεται και πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών επικοινωνίας, συγκεκριμένα του Διαδικτύου και των κινητών τηλεφώνων και η οποία επαναλαμβάνεται ανά τακτά ή άτακτα χρονικά διαστήματα.

Ο όρος cyberbullying δημιουργήθηκε από τον Καναδό Bill Belsey που είναι ο πρόεδρος του bullying.org και ο δημιουργός της πρώτης διαδικτυακής σελίδας που ασχολείται με αυτού του είδους τις παρενοχλήσεις και έχει τις ρίζες του στον παραδοσιακό σωματικό ή ψυχολογικό εκφοβισμό όπου ο στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του.

Αξίζει να σημειωθεί ότι δεν είναι όλες οι μορφές ηλεκτρονικού εκφοβισμού εξίσου ανησυχητικές ή επικίνδυνες. Η αλληλεπίδραση με κάποιον ο οποίος δεν εμφανίζεται πουθενά, ούτε μπορεί να ακουστεί στην άλλη άκρη της τηλεφωνικής γραμμής, επιτρέπει την έκφραση ιδεών και σκέψεων χωρίς τύψεις και χωρίς την πλήρη κατανόηση των αρνητικών επιπτώσεων των λέξεων ή των πράξεων. Σε όλες αυτές τις περιπτώσεις, το άτομο που συμπεριφέρεται κατ' αυτόν τον τρόπο δεν βλέπει το στόχο ούτε και ο ίδιος ο στόχος τον δράστη που δεν είναι φανερός, κάτι που αυξάνει τον κίνδυνο που ενυπάρχει στις συγκεκριμένες συμπεριφορές.

Αιτίες:

Συχνά οι νέοι οδηγούνται στον διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων όπως θυμός, απόγνωση είτε και εκδίκηση, που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργικότητας που παρουσιάζει το άτομο. Σε μερικές περιπτώσεις ο Διαδικτυακός εκφοβισμός αποτελεί μορφή

ψυχαγωγίας στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποίηση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου. Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου.

Μορφές ηλεκτρονικού εκφοβισμού:

Ας δούμε τις διάφορες μορφές που μπορεί να έχει ο ηλεκτρονικός εκφοβισμός:

- Ανάφλεξη (flaming): διαδικτυακοί διαπληκτισμοί, με τη χρήση βίαιης, χυδαίας και αγενούς γλώσσας.
- Παρενόχληση (harassment): προσβλητικά μηνύματα, μοιάζει με τον έμμεσο εκφοβισμό.
- Δυσφήμιση (denigration): αποστολή ή δημοσίευση σκληρών κουτσομπολιών ή φημών σχετικά με ένα άτομο, με σκοπό να τραυματιστεί η φήμη του.
- Αποκλεισμός (exclusion): αποκλεισμός από μία ομάδα στο Διαδίκτυο.
- Πλαστοπροσωπία (impersonation): το να παριστάνει κανείς ότι είναι κάποιος άλλος, θέτοντας αυτόν σε κίνδυνο ή τραυματίζοντας τη φήμη του.
- Ξεμπρόστιασμα (outing): η γνωστοποίηση στο Διαδίκτυο μυστικών, κουτσομπολιών ή άλλων προσωπικών πληροφοριών.
- Εξαπάτηση (trickery): όταν κάποιος εξαπατά κάποιον στο Διαδίκτυο και να του αποσπά επιβαρυντικές για αυτόν πληροφορίες, τις οποίες διαδίδει στη συνέχεια.
- Διαδικτυακή καταδίωξη (cyberstalking): ψυχαναγκαστική και συνεχής παρακολούθηση και κατασκοπεία σε διαδικτυακό επίπεδο.
- Διαδικτυακές απειλές (cyberthreats): αποτελούν είτε απευθείας απειλές ή «ενοχλητικό υλικό», δηλαδή σχόλια τα οποία υποδηλώνουν ότι ο συντάκτης τους είναι συναισθηματικά ταραγμένος και ότι μπορεί να σκέφτεται να βλάψει κάποιον άλλον ή τον εαυτό του ή και να αποπειραθεί να αυτοκτονήσει.
- Sexting: είναι ένας συνδυασμός των δύο όρων «sex» (σεξουαλικός) και «text» (κείμενο). Ο όρος αυτός βρίσκει εφαρμογή σε καταστάσεις όπου αποστέλλονται φτιαχτές γυμνές ή ημίγυμνες και σεξουαλικά προκλητικές εικόνες ή σεξουαλικά προκλητικό κείμενο. Ο όρος εστιάζεται περισσότερο στην αποστολή γυμνών φωτογραφιών, επειδή αυτές είναι πιο πιθανό να έχουν ευρύτερη διάδοση, η οποία μπορεί να θέσει τα νεαρά άτομα σε μεγαλύτερο κίνδυνο.

Σύμφωνα με Αμερικανούς ερευνητές, ο εκφοβισμός στον κυβερνοχώρο μπορεί να είναι πιο σκληρός για τα θύματά του από ότι η σωματική επίθεση ή οι βρισιές[25],[26].

3.10 ΑΠΑΤΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET FRAUD)

Όταν μιλάμε για απάτη στο Διαδίκτυο, εννοούμε την χρήση των υπηρεσιών του Διαδικτύου ή του λογισμικού με πρόσβαση στο Διαδίκτυο. Σκοπός των κακόβουλων χρηστών είναι να εξαπατήσουν τα θύματα ή να επωφεληθούν από αυτές τις απάτες, για παράδειγμα με την κλοπή προσωπικών πληροφοριών, που μπορεί ακόμη και να οδηγήσει σε κλοπή ταυτότητας. Μια πολύ συνηθισμένη μορφή απάτης στο Διαδίκτυο είναι το παραπλανητικό λογισμικό ασφαλείας που εξαπατά ή παραπλανά τους χρήστες να πληρώνουν χρήματα, για πλαστά προγράμματα ή προσομοιώσεις προγραμμάτων για απομάκρυνση κακόβουλου λογισμικού.

Εικόνα 9: Απάτη στο Διαδίκτυο

Οι απάτες στο Διαδίκτυο, μπορεί να συμβούν σε chat rooms, e-mail, πίνακες μηνυμάτων ή σε ιστοσελίδες.

Παρακάτων αναλύονται κάποια είδη απάτης στο Διαδίκτυο[27],[28].

Απάτες συναλλαγών:

Κάποιες από τις απάτες στο Διαδίκτυο συμβαίνουν όταν ένας εγκληματίας πλησιάζει έναν έμπορο, προτείνει μια επιχειρηματική συναλλαγή, και στη συνέχεια χρησιμοποιεί δόλια μέσα να πληρώσει για αυτήν, όπως με κλεμμένες ή πλαστές πιστωτικές κάρτες. Αυτό έχει ως αποτέλεσμα, οι έμποροι να μην πληρώνονται για την πώληση.

Οι έμποροι που δέχονται τις πλαστές ή και κλεμμένες πιστωτικές κάρτες μπορεί να χρεωθούν κιόλας για τη συναλλαγή και τελικά να χάσουν και χρήματα.

Απάτες με πλαστές ταχυδρομικές επιταγές:

Τα τελευταία χρόνια έχει παρατηρηθεί αύξηση στην ποσότητα και βελτίωση στην ποιότητα των πλαστών ταχυδρομικών επιταγών. Θύματα αυτής της απάτης είναι κυρίως μικροί έμποροι του Διαδικτύου, διαφημιστές και άτομα που έρχονται σε επαφή με τους απατεώνες διαδικτυακά.

Απάτες με πωλήσεις αυτοκινήτων στο Διαδίκτυο:

Αρχικά, ο απατεώνας δημοσιεύει προς πώληση ένα ανύπαρκτο όχημα σε μια ιστοσελίδα πώλησης αυτοκινήτων. Το όχημα αυτό είναι συνήθως ένα πολυτελές ή σπορ αυτοκίνητο, το οποίο διαφημίζει πως πουλάει σε τιμή πολύ κατώτερη της αγοραίας του αξίας.

Ο ενδιαφερόμενος αγοραστής, που ελπίζει σε μια συμφωνία, στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου. Ο απατεώνας τότε απαντά λέγοντας ότι το αυτοκίνητο είναι ακόμα διαθέσιμο, αλλά βρίσκεται στο εξωτερικό ή ότι ο ίδιος βρίσκεται στο εξωτερικό και στη συνέχεια ζητά από τον ενδιαφερόμενο να πληρώσει μέσω εμβάσματος κάποια προκαταβολή ή και ολόκληρο το ποσό προκειμένου να ξεκινήσει η διαδικασία φόρτωσης και αποστολής του αυτοκινήτου.

Για να φανεί πιο αληθοφανής και νόμιμη η συναλλαγή, ο απατεώνας ζητάει από τον αγοραστή να στείλει τα χρήματα σε ένα ψεύτικο παράγοντα που προσφέρει προστασία στη συναλλαγή. Τα ανυποψίαστα θύματα στέλνουν τα χρήματα και στη συνέχεια ανακαλύπτουν ότι έχουν εξαπατηθεί.

Απάτες με δημοπρασίες στο διαδίκτυο:

Σε ένα online σύστημα δημοπράτησης, ένας απατεώνας ξεκινάει μια δημοπρασία με πολύ χαμηλές τιμές και χωρίς ελάχιστη τιμή, ιδιαίτερα για τα τυπικά ακριβά αντικείμενα, όπως ρολόγια, υπολογιστές, ή συλλεκτικά αντικείμενα υψηλής αξίας. Ο απατεώνας δέχεται πληρωμές από τον νικητή στη δημοπρασία, αλλά είτε δεν παραδίδει τα αγαθά που έχει υποσχεθεί, ή παραδίδει ένα αντικείμενο που έχει πολύ μικρότερη αξία από εκείνο που προσφέρεται, για παράδειγμα, ένα πλαστό, χαλασμένο, ή χρησιμοποιημένο αντικείμενο.

Σύμφωνα με τα στοιχεία που έχουν συλλέξει οργανώσεις προστασίας των καταναλωτών, οι απάτες που εμφανίζονται σε ιστοσελίδες δημοπρασιών στο Διαδίκτυο είναι μια από τις πιο συχνά αναφερόμενες μορφές μαζικής απάτης.

Απάτες μεταφοράς χρημάτων:

Αρχικά, το υποψήφιο θύμα λαμβάνει ένα email στο οποίο ο απατεώνας προσφέρει στο υποψήφιο θύμα απασχόληση-εργασία, κατά την οποία το θύμα θα εργάζεται για τη μεταφορά χρημάτων σε ξένες εταιρείες, επειδή υποθετικά κοστίζει πάρα πολύ για να το κάνει κανείς μέσω άλλων μεθόδων. Οι απατεώνες στη συνέχεια στελνουν πλαστές ταχυδρομικές επιταγές, με την ελπίδα ότι τα θύματα θα εισπράξουν τα πλαστά χρηματικά μέσα και θα στείλουν χρήματα στους απατεώνες πριν να αποκαλυφθεί η απάτη. Εναλλακτικά, μπορεί επίσης να είναι μια περίπτωση όπου οι απατεώνες θέλουν να ξεπλύνουν χρήματα από κλοπή.

Απάτες μέσω ιστοσελίδων γνωριμιών:

Με αυτού του είδους τις απάτες, συχνά ο απατεώνας αναπτύσσει μια σχέση με το θύμα του μέσω μιας ιστοσελίδας γνωριμιών και πείθει το θύμα να του στείλει χρήματα. Οι αιτήσεις για χρήματα μπορεί να είναι ένα μεμονωμένο, ή κατ' επανάληψη γεγονός κατά τη διάρκεια μιας εκτεταμένης χρονικής περιόδου.

Απάτες με πρόφαση τη φιλανθρωπία:

Ο απατεώνας εμφανίζεται ως φιλανθρωπική οργάνωση και προσελκύει τα υποψήφια θύματα να προσφέρουν δωρεές για να βοηθήσουν τα θύματα μιας φυσικής καταστροφής, τρομοκρατικής επίθεσης ή επιδημιών. Τα θύματα μέσω της δωρεάς που προσφέρουν, πιστεύουν ότι βοηθούν ανθρώπους που βρίσκονται σε ανάγκη. Μόλις όμως αποσταλούν τα χρήματα, τότε κιόλας εξαφανίζεται και ο απατεώνας.

3.11 HTTP COOKIES

Ένα cookie, επίσης γνωστό ως HTTP cookie, web cookie, ή browser cookie, είναι ένα μικρό κομμάτι δεδομένων που αποστέλλονται από μια ιστοσελίδα και αποθηκεύονται στον browser του χρήστη, ενώ ο χρήστης περιηγείται στην ιστοσελίδα. Κάθε φορά που ο χρήστης φορτώνει την ιστοσελίδα, ο browser στέλνει το cookie πίσω στο server για να ειδοποιήσει τον ιστοχώρο για την προηγούμενη δραστηριότητα του χρήστη.

Τα cookies έχουν σχεδιαστεί για να είναι ένας αξιόπιστος μηχανισμός για τους ιστοχώρους να θυμούνται πληροφορίες (όπως αντικείμενα σε ένα καλάθι αγορών), ή

να καταγράφουν την περιηγητική δραστηριότητα του χρήστη (κλικ σε συγκεκριμένα κουμπιά, σύνδεση ή εγγραφή σε σελίδες που επισκέφτηκε ο χρήστης), μήνες ή και χρόνια πριν.

Τα cookies μπορούν επίσης να αποθηκεύουν κωδικούς πρόσβασης και άλλα στοιχεία που ένας χρήστης έχει εισάγει, όπως έναν αριθμό πιστωτικής κάρτας ή μια διεύθυνση. Όταν ένας χρήστης αποκτά πρόσβαση σε μια ιστοσελίδα, ένα cookie στέλνεται από τον server στον browser και αποθηκεύεται μαζί με το πρόγραμμα περιήγησης στον υπολογιστή. Αργότερα, όταν ο χρήστης πηγαίνει πίσω στην ίδια ιστοσελίδα, η ιστοσελίδα θα αναγνωρίσει το χρήστη, λόγω του αποθηκευμένου cookie με τις πληροφορίες του χρήστη.

Υπάρχουν πολλά ήδη cookies, τα οποία λειτουργούν με διαφορετικό τρόπο και έχουν διαφορετική «αποστολή». Ας δούμε κάποια από αυτά:

Authentication cookies:

Ίσως τα σημαντικότερα cookies είναι τα cookies ελέγχου ταυτότητας, που είναι η πιο κοινή μέθοδος που χρησιμοποιείται από τους διακομιστές web για να γνωρίζουν αν ο χρήστης είναι συνδεδεμένος ή όχι, και με ποιό λογαριασμό είναι συνδεδεμένος. Χωρίς έναν τέτοιο μηχανισμό, η ιστοσελίδα δεν θα ήξερε αν πρέπει να στείλει μια σελίδα που περιέχει ευαίσθητες πληροφορίες, ή να απαιτήσουν από το χρήστη να επικυρώσει τον εαυτό του κάνοντας σύνδεση με το λογαριασμό του.

Η ασφάλεια ενός cookie ελέγχου ταυτότητας εξαρτάται γενικά από την ασφάλεια της ιστοσελίδας την οποία αφορά και του browser του χρήστη, καθώς και με το εάν τα δεδομένα του cookie είναι κρυπτογραφημένα.

Session cookies:

Τα session cookies (επίσης γνωστά ως in-memory cookies ή transient cookies) για μια ιστοσελίδα υπάρχουν στην προσωρινή μνήμη μόνο όσο ο χρήστης διαβάζει και περιηγείται στην ιστοσελίδα. Όταν μια ημερομηνία λήξης ή ημερομηνία διαστήματος ισχύος δεν έχει ρυθμιστεί κατά το χρόνο δημιουργίας του, τότε δημιουργείται ένα cookie συνεδρίας. Τα προγράμματα περιήγησης στο Web διαγραφή κανονικά cookies περιόδου, όταν ο χρήστης κλείσει το πρόγραμμα περιήγησης. Τα προγράμματα περιήγησης στο web κανονικά διαγράφουν τα session cookies, όταν ο χρήστης κλείσει το browser.

Persistent cookies:

Ένα persistent cookie (μόνιμο cookie) ξεπερνάει σε διάρκεια ένα session cookie. Εάν ένα persistent cookie έχει μέγιστη ηλικία σύνολο έως 1 έτος (για παράδειγμα), κατά τη διάρκεια του ίδιου έτους, η αρχική τιμή που καθορίζεται στο εν λόγω cookie στέλνεται πίσω στο διακομιστή κάθε φορά που ο χρήστης επισκέφτεται το διακομιστή αυτό. Ο τρόπος αυτός θα μπορούσε να χρησιμοποιηθεί για να καταγράψει ένα ζωτικό κομμάτι των πληροφοριών, όπως το πώς ο χρήστης αρχικά ήρθε σε αυτή την ιστοσελίδα. Για το λόγο αυτό, τα persistent cookies ονομάζονται επίσης και tracking cookies (cookies παρακολούθησης).

Secure cookies:

Ένα secure cookie έχει ενεργοποιημένο το χαρακτηριστικό να είναι ασφαλές και χρησιμοποιείται μόνο μέσω HTTPS, διασφαλίζοντας ότι το cookie είναι πάντα

κρυπτογραφημένο κατά τη διαβίβαση από τον client στον server. Αυτό καθιστά το secure cookie λιγότερο πιθανό να εκτεθεί σε κλοπή μέσω υποκλοπής.

HttpOnly cookies:

Το χαρακτηριστικό HttpOnly υποστηρίζεται από τα περισσότερα σύγχρονα προγράμματα περιήγησης. Σε ένα υποστηριζόμενο πρόγραμμα περιήγησης, ένα HttpOnly session cookie θα πρέπει να χρησιμοποιείται μόνο κατά τη διαβίβαση HTTP (ή HTTPS) αιτημάτων, περιορίζοντας έτσι την πρόσβαση από άλλους, μη-HTTP APIs (όπως JavaScript). Ο περιορισμός αυτός μετριάζει, αλλά δεν εξαλείφει την απειλή της κλοπής session cookie μέσω cross-site scripting (βλ. Γλωσσάριο). Αυτή η λειτουργία ισχύει μόνο για session-management cookies, και όχι για άλλα cookies του προγράμματος περιήγησης.

Άλλα cookies είναι τα third-party cookies, τα supercookies και τα zombie cookies.

Οι ευπάθειες στην ασφάλεια μπορεί να επιτρέψουν σε έναν χάκερ ή κράκερ να διαβάσει τα δεδομένα ένος cookie και να τα χρησιμοποιήσει:

- Είτε για να αποκτήσει πρόσβαση στα δεδομένα των χρηστών, ή
- Είτε για να αποκτήσει πρόσβαση στην ιστοσελίδα στην οποία το cookie ανήκει με τα διαπιστευτήρια του χρήστη[29].

3.12 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ

Κύριες μορφές κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος:

1. Απάτες μέσω Διαδικτύου
2. Παιδική πορνογραφία
3. Cracking και hacking
4. Διακίνηση-πειρατία λογισμικού
5. Πιστωτικές κάρτες
6. Διακίνηση ναρκωτικών
7. Έγκλημα στα chat rooms

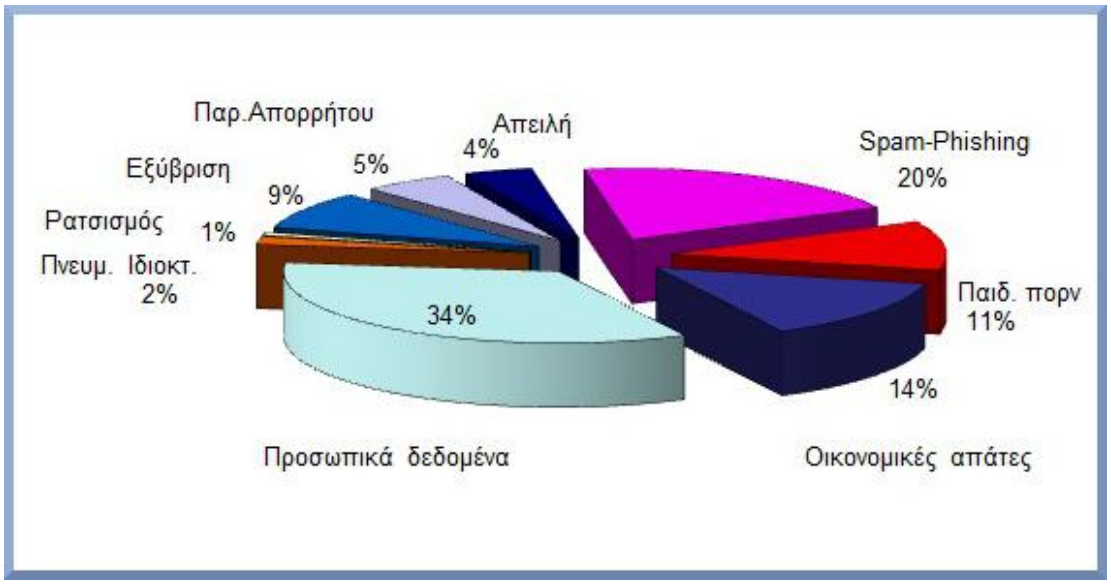
Η Ελληνική Ανοικτή γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο, η SafeLine, για το 2012 έλαβε 2598 καταγγελίες για παράνομο περιεχόμενο στο Διαδίκτυο.

Από τα τελευταία στατιστικά στοιχεία, φαίνεται πως οι καταγγελίες που λαμβάνει η SafeLine γίνονται όλο και πιο στοχευμένες και πιο ποιοτικές συγκριτικά με τα προηγούμενα έτη.

Το μεγαλύτερο ποσοστό καταγγελιών ανήκει στην κατηγορία των Προσωπικών δεδομένων (34%). Είναι προφανές από το ποσοστό αυτό ότι πάνω από το ένα τρίτο των περιπτώσεων των αναφορών είχαν να κάνουν με την έλλειψη σεβασμού της διαδικτυακής ταυτότητας καθώς και της ιδιωτικής ζωής των χρηστών του Διαδικτύου. Το τελευταίο αποδεικνύεται και από τον αριθμό των καταγγελιών που αφορούσαν το Facebook (845 καταγγελίες), οι οποίες περιελάμβαναν περιπτώσεις δημιουργίας ψεύτικων προφίλ, διαδικτυακό εκφοβισμό (cyberbulling)[30].

Οι καταγγελίες που λαμβάνει η SafeLine, των οποίων το περιεχόμενο επιβεβαιώνεται ως παράνομο έχει ως χώρο προέλευσης την Ελλάδα , προωθούνται στη Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, καθώς επίσης και σε άλλες ανεξάρτητες ελληνικές αρχές, όπως είναι η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και η Αρχή Προστασίας Προσωπικών Δεδομένων.

Στις περιπτώσεις που το παράνομο περιεχόμενο εντοπίζεται σε άλλη χώρα του εξωτερικού, τότε οι καταγγελίες αυτές προωθούνται στις αντίστοιχες Ανοικτές Γραμμές του εξωτερικού μέσω της κοινής βάσης του INHOPE. Για τον INHOPE θα δούμε περισσότερες πληροφορίες παρακάτω.



Διάγραμμα 1: Καταγγελίες στην Ελλάδα για παράνομο περιεχόμενο στο Διαδίκτυο το 2012

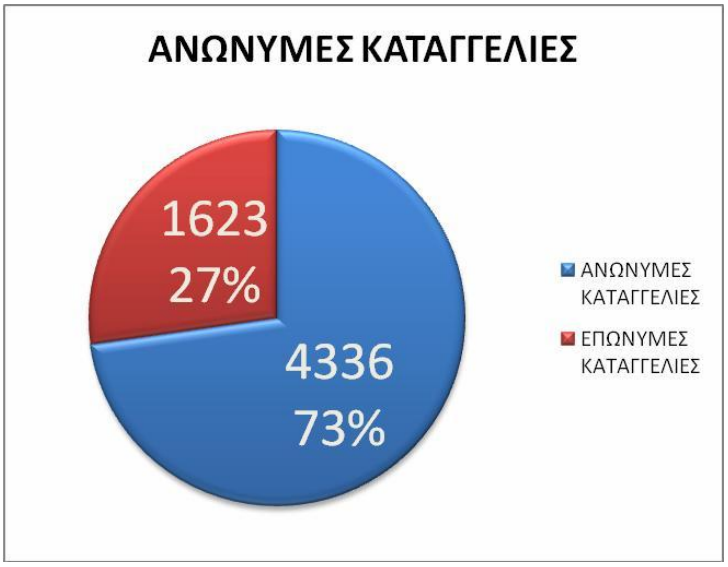
Σύμφωνα με την SafeLine οι αιτίες της ραγδαίας αύξησης του αριθμού των καταγγελιών που έχει καταγραφεί, οι οποίες αφορούν το Facebook, είναι αρκετά δύσκολο να προσδιοριστούν, αλλά σίγουρα μία από αυτές είναι η αύξηση του αριθμού των χρηστών του Διαδικτύου, οι οποίοι έχουν δημιουργήσει προφίλ στο δημοφιλές αυτό κοινωνικό δίκτυο.

Μελετώντας το παραπάνω διάγραμμα, καταγράφεται μια αύξηση στο ποσοστό της κατηγορίας Παιδική πορνογραφία το οποίο είναι 11% (το ποσοστό αυτό ήταν της τάξεως του 6% το 2010).

Σύμφωνα με τη Δίωξη Ηλεκτρονικού Εγκλήματος προκύπτουν τα εξής στοιχεία που αφορούν την Ελλάδα για το 2011:

Από την έναρξη της λειτουργίας της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος το καλοκαίρι του 2011 και μέχρι τα τέλη του επόμενου Φεβρουαρίου, έχει δεχθεί συνολικά 5.959 καταγγελίες, στον ειδικό τηλεφωνικό αριθμό καταγγελιών 11012, από τις οποίες το μεγαλύτερο μέρος αφορά στη μη έκδοση αποδείξεων παροχής υπηρεσιών.

Στη συνέχεια, οι καταγγελίες αυτές ομαδοποιούνται, κατά γεωγραφική περιοχή και είδος παράνομης δραστηριότητας, εξετάζονται από επιτροπές αξιολόγησης και προωθούνται στα Τμήματα της Οικονομικής Αστυνομίας και της Δίωξης Ηλεκτρονικού Εγκλήματος για περαιτέρω αστυνομική έρευνα. Από το σύνολο των καταγγελιών οι 4.336 καταγγελίες έγιναν επώνυμα, ενώ οι 1.623 ανώνυμα.

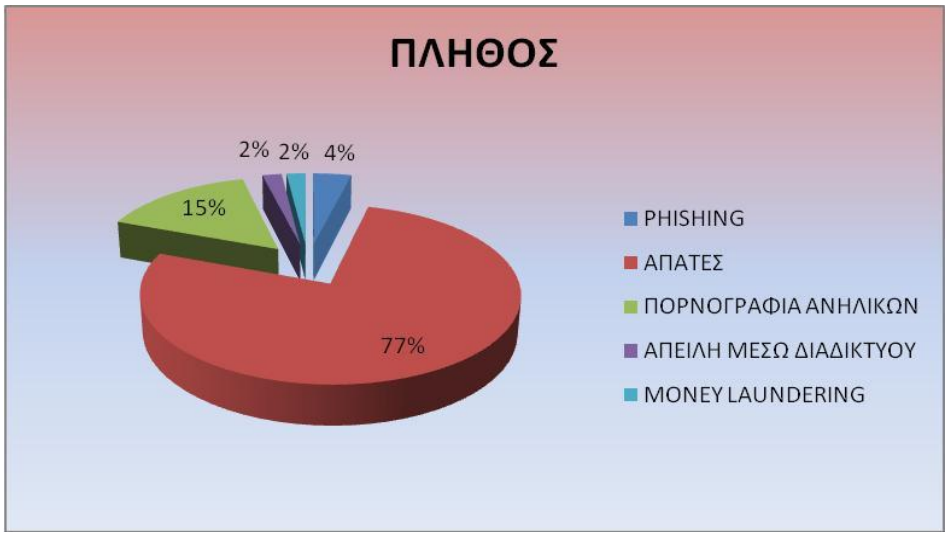


Διάγραμμα 2: Αριθμός επώνυμων και ανώνυμων καταγγελιών για το 2011

Στον τομέα της ηλεκτρονικής μορφής εγκληματικών συμπεριφορών, η Δίωξη Ηλεκτρονικού Εγκλήματος, χειρίστηκε 832 δικογραφίες για πληθώρα διαδικτυακών ή ηλεκτρονικών εγκλημάτων. Έμφαση στη δράσης της δόθηκε σε εκείνες τις ηλεκτρονικές παράνομες και ταυτόχρονα αντικοινωνικές συμπεριφορές που στερούν από την Εθνική Οικονομία αρκετά έσοδα, προκαλούν οικονομικό ρήγμα στις δομές κοινωνικής ασφάλισης, καθώς και σε εκείνες που διαταράσσουν το κλίμα εμπιστοσύνης και υγιούς συναλλαγής μεταξύ των ηλεκτρονικών χρηστών.

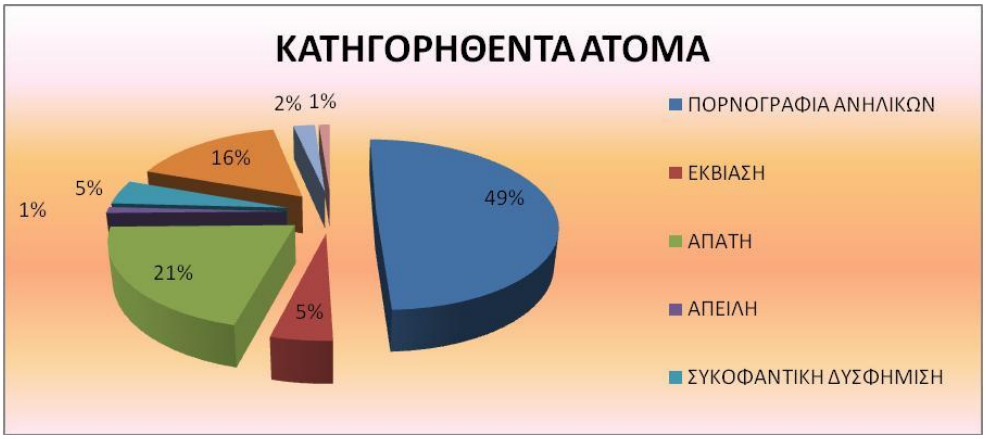
Σε 364 περιπτώσεις, ακολουθήθηκε αστυνομική έρευνα και σχηματίσθηκε δικογραφία, από κλιμάκια της Δίωξης Ηλεκτρονικού Εγκλήματος, ύστερα από καταγγελίες Φορέων Προστασίας Καταναλωτών, Οργανισμών, Χρηματοπιστωτικών Ιδρυμάτων, Εταιρειών Τηλεπικοινωνιών, καθώς και καταστημάτων ηλεκτρονικού εμπορίου (e shops).

Επιπλέον, στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol & Europol), παρασχέθηκε συνδρομή σε 71 περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα, και αφορούσαν στο ηλεκτρονικό εμπόριο, στις διαδικτυακές απάτες, στις υφαρπαγές στοιχειών και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοχώρους ηλεκτρονικών οικονομικών δραστηριοτήτων[31].



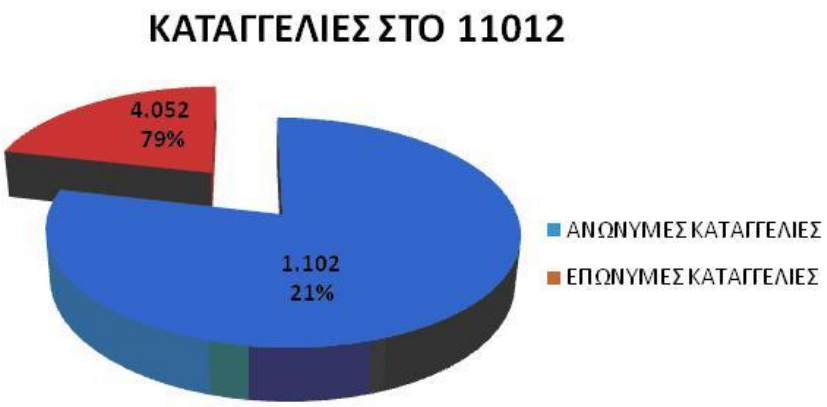
Διάγραμμα 3: Διαδικτυακή μορφή εγκληματικών συμπεριφορών 2011: Πλήθος

Συνολικά έχουν αποδοθεί κατηγορίες για διάφορα αδικήματα σε συνολικά 87 άτομα.

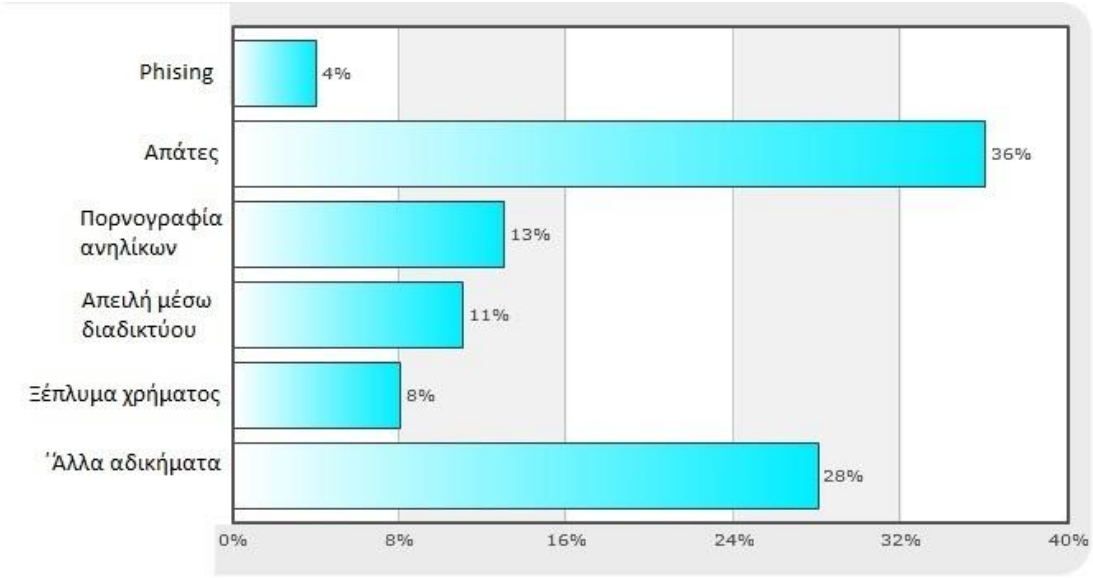


Διάγραμμα 4: Κατηγορηθέντα άτομα για το 2011

Επισημαίνεται ότι το έτος 2012, ο ειδικός τηλεφωνικός αριθμό καταγγελιών 11012 της Οικονομικής Αστυνομίας, δέχτηκε συνολικά 5.154 καταγγελίες. Οι καταγγελίες αυτές ομαδοποιούνται, κατά γεωγραφική περιοχή και είδος παράνομης δραστηριότητας, εξετάζονται από επιτροπές αξιολόγησης και προωθούνται στα Τμήματα της Οικονομικής Αστυνομίας και της Δίωξης Ηλεκτρονικού Εγκλήματος για περαιτέρω αστυνομική έρευνα. Από το σύνολο των καταγγελιών οι 1.102καταγγελίες έγιναν επώνυμα, ενώ οι 4.052 ανώνυμα.



Διάγραμμα 5: Αριθμός επώνυμων και ανώνυμων καταγγελιών για το 2012



Διάγραμμα 6: Διαδικτυακή μορφή εγκληματικών συμπεριφορών 2012: Πλήθος

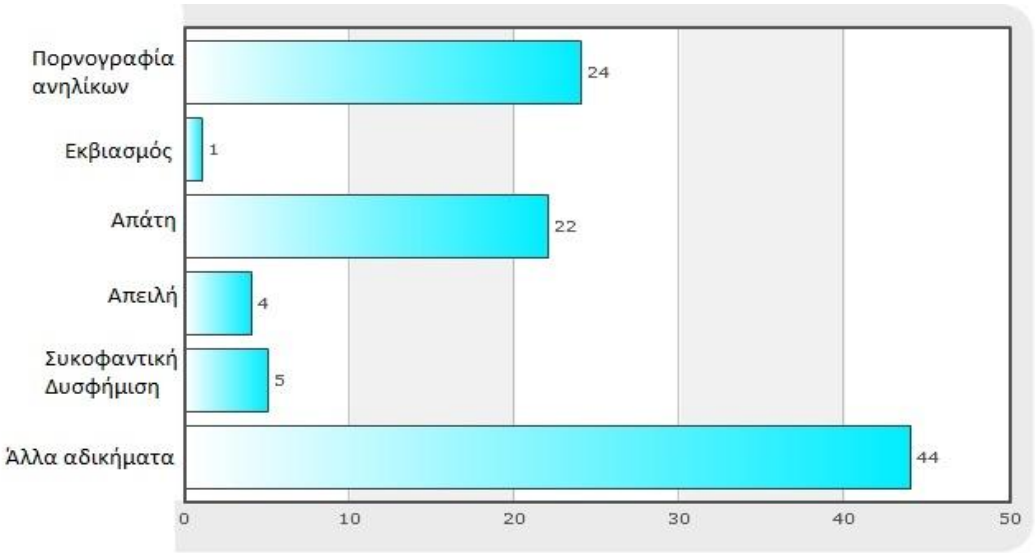
Στον τομέα της ηλεκτρονικής-διαδικτυακής μορφής εγκληματικών συμπεριφορών, η Δίωξη Ηλεκτρονικού Εγκλήματος, χειρίστηκε 3.193 δικογραφίες για πληθώρα διαδικτυακών ή ηλεκτρονικών εγκλημάτων. Έμφαση στη δράση της δόθηκε σε εκείνες τις ηλεκτρονικές παράνομες και ταυτόχρονα αντικοινωνικές συμπεριφορές που στερούν από την Εθνική Οικονομία αρκετά έσοδα, προκαλούν οικονομικό ρήγμα στις δομές κοινωνικής ασφάλισης, καθώς και σε εκείνες που διαταράσσουν το κλίμα εμπιστοσύνης και υγιούς συναλλαγής μεταξύ των ηλεκτρονικών χρηστών.

Σε 115 περιπτώσεις ακολουθήθηκε αστυνομική έρευνα και σχηματίσθηκε δικογραφία από κλιμάκια της Δίωξης Ηλεκτρονικού Εγκλήματος ύστερα από καταγγελίες Φορέων Προστασίας Καταναλωτών, Οργανισμών, Χρηματοπιστωτικών Ιδρυμάτων, Εταιριών Τηλεπικοινωνιών, καθώς και καταστημάτων ηλεκτρονικού εμπορίου (e-shops).

Επιπρόσθετα, στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol και Europol), η Υποδιεύθυνση Δίωξης Ηλεκτρονικού εγκλήματος διαχειρήστηκε 746 αιτήματα συνεργασίας. Τα αιτήματα αφορούν περιπτώσεις διακρατικών αστυνομικών

ερευνών που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικού εγκλήματος, και αφορούσαν στο ηλεκτρονικό εμπόριο, στις διαδικτυακές απάτες, στις υφαρπαγές στοιχείων και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοχώρους ηλεκτρονικών οικονομικών δραστηριοτήτων[32].

Συνολικά έχουν αποδοθεί κατηγορίες σε συνολικά 458 άτομα για διάφορα αδικήματα.

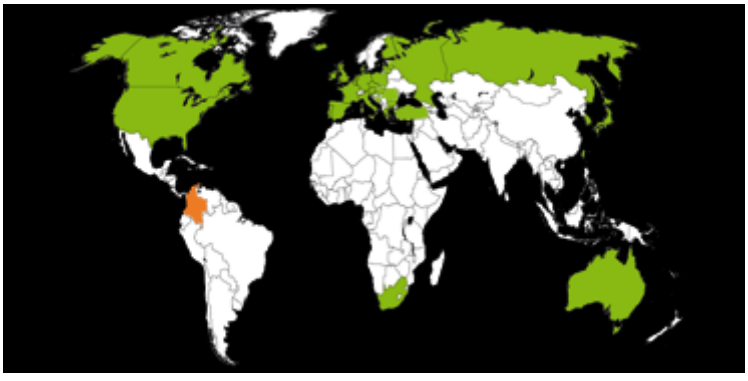


Διάγραμμα 7: Κατηγορηθέντα άτομα για το 2012

Στατιστικές από τον INHOPE:

Οι ανοικτές γραμμές επικοινωνίας INHOPE προσφέρουν στο κοινό έναν τρόπο ανώνυμης αναφοράς υλικού στο Διαδίκτυο που περιλαμβάνει υλικό σεξουαλικής κακοποίησης παιδιών, το οποίο υποπτεύονται ότι είναι παράνομο. Η Γραμμή διασφαλίζει ότι το θέμα διερευνάται και εφόσον διαπιστωθεί ότι είναι παράνομη η πληροφορία θα πρέπει να περάσει στην αρμόδια Υπηρεσία επιβολής του νόμου. Στην ιστοσελίδα του INHOPE μπορεί κανείς να βρει ανάλογα με την χώρα στην οποία βρίσκεται, την τοπικής ανοιχτής γραμμής στην χώρα στην οποία βρίσκεται. Δηλαδή, ο χρήστης ανακατευθύνεται σε ιστοσελίδες χωρών εντός και εκτός Ευρώπης όπως: η Ελλάδα, η Γερμανία, η Ρουμανία, η Ρωσία, η Αυστραλία, οι ΗΠΑ, η Τουρκία, η Ιαπωνία και η Νότια Αφρική.

Με λίγα λόγια ο INHOPE αντιπροσωπεύει και υποστηρίζει τις ανοικτές γραμμές επικοινωνίας, σε ολόκληρο τον κόσμο.

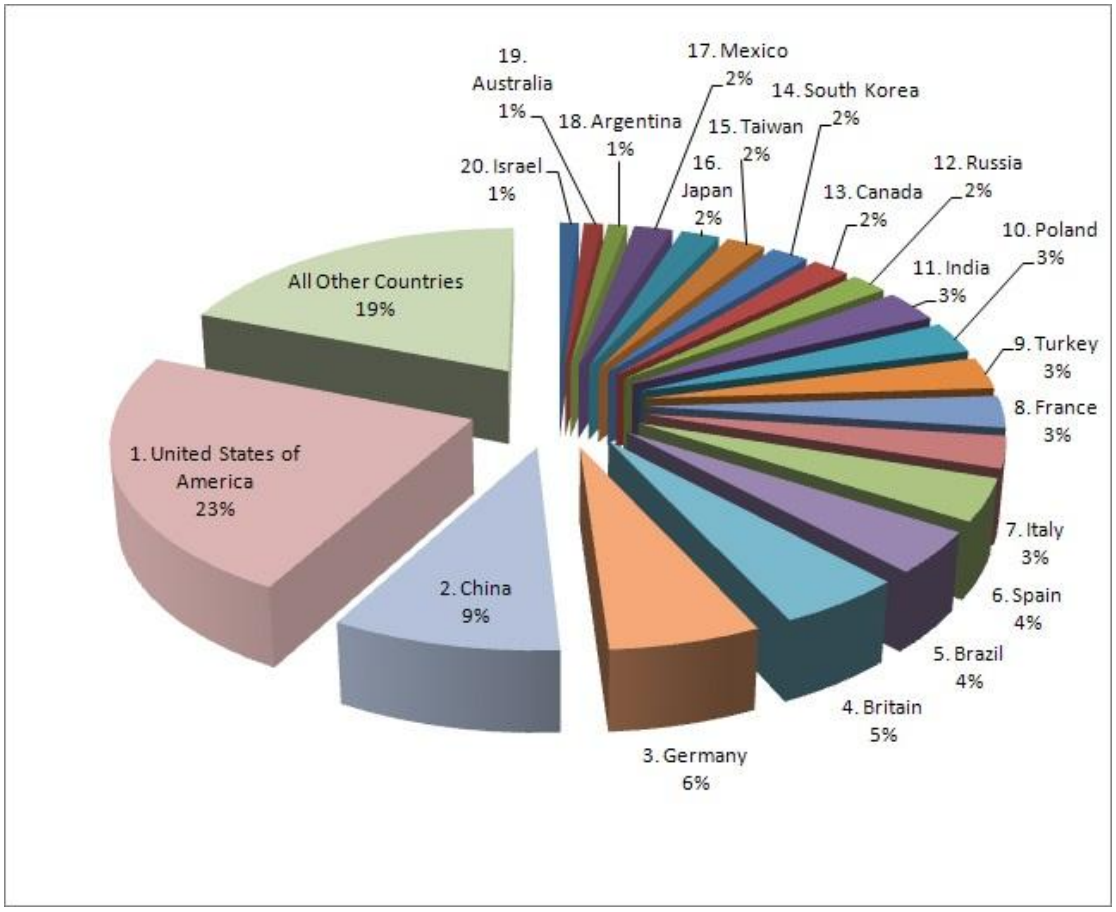


Εικόνα 10: Χώρες τις οποίες στηρίζει ο INHOPE

Ο οργανισμός INHOPE έδωσε στη δημοσιότητα κάποια στατιστικά στοιχεία που αφορούν την περίοδο Σεπτέμβριος 2005 - Ιούνιος 2010 και δείχνουν ότι[33]:

- Οι ανοικτές γραμμές επικοινωνίας που συνεργάζονται με τον οργανισμό INHOPE, έλαβαν και επεξεργάστηκαν κατά μέσο όρο 60.200 αναφορές ανά μήνα, με κάθε μια από αυτές να είναι ξεχωριστή από τις υπόλοιπες.
- 51% όλων των αναφορών αναφέρονται στην κυκλοφορία παράνομου περιεχομένου
- 66% περιέχουν υλικό σεξουαλικής κακοποίησης παιδιών
- 13% έχουν υλικό που σχετίζεται με άλλα θέματα σχετικά με παιδιά
- 18% από τις αναφορές περιέχουν υλικό πορνογραφίας ενηλίκων

Ας δούμε τώρα τις κορυφαίες 20 χώρες που διαπιστώθηκε ότι έχουν τα περισσότερα εγκλήματα στον Διαδίκτυο[34]:



Διάγραμμα 8: Χώρες με περισσότερα εγκλήματα στο Διαδίκτυο

2 στους 3 καταδικασθέντες εγκληματίες του κυβερνοχώρου είναι μεταξύ των ηλικιών 15 και 26, σύμφωνα με διεθνή έρευνα που διεξήγαγε αυστραλιανός φορέας[35].

3.13 ΠΑΡΑΔΕΙΓΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Ας δούμε κάποια περιστατικά Ηλεκτρονικού Εγκλήματος που συνέβησαν στην Ελλάδα και στο εξωτερικό[8]. Σε αυτά τα παραδείγματα μπορούμε να διακρίνουμε αρκετές από τις μορφές του ηλεκτρονικού εγκλήματος όπως κακόβουλες εισβολές σε δίκτυα, διακίνηση παιδικού πορνογραφικού υλικού, επίθεση παρενόχλησης (cyberbullying) κ.ά.

- Παραβίαση Του Playstation Network

Όταν στις 20 Απριλίου του 2011 , οι χρήστες του Playstation Network , της διαδικτυακής υπηρεσίας της Sony για τους κατόχους Playstation 3 και Playstation Portable , ήταν ανήμποροι να συνδεθούν στους λογαριασμούς τους, κανείς δεν μπορούσε να φανταστεί το τι είχε συμβεί.

Αν και η υπηρεσία ενημέρωνε τους χρήστες ότι το σύστημα βρισκόταν υπό καθεστώς συντήρησης και ως εκ τούτου αδυνατούσε να τους εξυπηρετήσει, στην πραγματικότητα επρόκειτο για μια από τις μεγαλύτερες επιθέσεις που είχε δεχθεί η Sony στην πολύχρονη ιστορία της. Παρότι η εταιρεία ήταν ενήμερη για το γεγονός της επίθεσης, η οποία τοποθετείται μεταξύ 17 και 19 Απριλίου του 2011, εντούτοις από επίσημα χείλη άφηνε να εννοηθεί πως διερευνούσε τα αίτια της απροσδόκητης διακοπής της υπηρεσίας, καθησυχάζοντας τους συνδρομητές με την υπόσχεση πως οι λογαριασμοί τους θα τεθούν και πάλι σε λειτουργία σε διάστημα δυο ημερών.

Με τις ημέρες να περνούν και τις υποψίες να αυξάνονται για το τι πραγματικά συνέβαινε, η Sony εγκατέλειψε την αρχική της θέση , ότι δηλαδή η συντήρηση του δικτύου ήταν μια χρονοβόρος διαδικασία και αναγκάστηκε να παραδεχθεί δημοσίως ότι το σύστημά της είχε παραβιαστεί.

Δεν ήταν η πρώτη φορά που συνέβαινε κάτι τέτοιο. Παρόμοιο περιστατικό είχε λάβει χώρα και το 2007, όταν εισβολέας υπέκλεψε τα στοιχεία 45 εκατομμυρίων χρηστών. Αυτή τη φορά όμως τα θύματα ήταν περισσότερα. Όπως καθυστερημένα γνωστοποίησε η ίδια η εταιρεία, στις 4 Μαΐου του 2011, ως επακόλουθο της επίθεσης που δέχθηκε, είχαν διαρρεύσει ευαίσθητα προσωπικά δεδομένα 77 εκατομμυρίων χρηστών, όπως τηλέφωνα, αριθμοί πιστωτικών καρτών ακόμα και διευθύνσεις κατοικίας. Σε απάντησή της στις έντονες ανησυχίες που εκδήλωναν οι συνδρομητές της, η Sony υποστήριξε ότι η επίθεση προήλθε από τους Anonymous οι οποίοι είχαν βάλει στόχο την εταιρεία και προσπαθούσαν να την πλήξουν.

Παρόλα αυτά, οι Anonymous αποποιήθηκαν την ευθύνη της επίθεσης, με την Sony να ξεκινά ένα νέο κύκλο ερευνών για την ανακάλυψη και την ποινική δίωξη των υπευθύνων, χωρίς ωστόσο η συγκεκριμένη προσπάθεια να αποδώσει καρπούς.

Τελικά, η Sony αναγκάστηκε να κρατήσει κλειστές τις υπηρεσίες της για συνολικά 24 ημέρες, κάτι που της κόστισε 171 εκατομμύρια δολάρια, καθώς και χιλιάδες νομικές κινήσεις εναντίον της από τους χρήστες, που μεταξύ άλλων την κατηγορούσαν για ανεπάρκεια προστασίας των προσωπικών τους στοιχείων και για την μη έγκαιρη ενημέρωσή τους.

- Επίθεση στο ελληνικό Υπουργείο Οικονομικών

Ένα παράδειγμα ηλεκτρονικού εγκλήματος που αποτελεί μία από τις μεγαλύτερες ηλεκτρονικές κυβερνοεπίθεσεις που έχει πραγματοποιηθεί τα τελευταία χρόνια στον Ελλαδικό χώρο είναι η επίθεση από τους Anonymous, με ταυτόχρονη διαρροή απόρρητων και διαβαθμισμένων εγγράφων, που δέχθηκαν οι υπηρεσίες του Γενικού Λογιστηρίου του Κράτους όπως επιβεβαίωσε το υπουργείο Οικονομικών.

Συγκεκριμένα, στοιχεία της Γενικής Γραμματείας Δημοσιονομικής Πολιτικής και ειδικότερα αρχεία της Γενικής Διεύθυνσης Θησαυροφυλακίου και Προϋπολογισμού υπεξαιρέθηκαν από τους χάκερς και εν συνεχεία δημοσιοποιήθηκαν. Το υπουργείο Οικονομικών επιβεβαίωσε ότι υπηρεσίες του Γενικού Λογιστηρίου του Κράτους δέχθηκαν επίθεση από τους Anonymous.

Πολλά από τα έγγραφα τα οποία υπεξαιρέθηκαν από το σύστημα του υπουργείου «ανέβηκαν» πρώτα στην ιστοσελίδα των Anonymous και έπειτα σε ελληνική ιστοσελίδα ασφαλούς ανάρτησης μαζί με ένα μήνυμα στα Αγγλικά για την επίθεση στο υπουργείο. Η επίθεση είχε κύριο στόχο την διαρροή εγγράφων και πληροφοριών σχετικά με την κατάσταση της Ελληνικής οικονομίας. Μετά από εντολή του Εισαγγελέα Πρωτοδικών η Δίωξη Ηλεκτρονικού Εγκλήματος ανέλαβε τη διερεύνηση της υπόθεσης της κλοπής αρχείων από το Γενικό Λογιστήριο του κράτους.

Οι hackers ανάρτησαν εσωτερικούς κωδικούς πρόσβασης του Υπουργείου Οικονομικών και συνδέσμους με έγγραφα που μπορεί να κατεβάσει ο οποιοσδήποτε. Τα στοιχεία που δίνουν στην δημοσιότητα οι hackers περιλαμβάνουν ονόματα χρηστών και κωδικούς πρόσβασης πιθανόν από εσωτερικό σύστημα του Υπουργείου. Εντύπωση προκαλεί η συχνή χρήση ευκολομνημόνευτων κωδικών (ακόμα και 123456) από πλήθος χρηστών υπογραμμίζοντας σαφέστατα την έλλειψη επαρκούς πολιτικής ασφάλειας ακόμα και στο πιο απλό, δηλαδή την επιλογή ενδυναμωμένων κωδικών πρόσβασης.

Σύμφωνα με όσα αναφέρουν στο μήνυμά τους οι άγνωστοι hackers Anonymous, η πρόσβαση τους κατέστει δυνατή μέσω αδυναμίας που επηρεάζει τα γνωστά SAP συστήματα. Επιπλέον αναφέρουν ότι απέκτησαν πρόσβαση σε εσωτερικούς εξυπηρετητές (servers) ενώ οι απλοί κωδικοί πρόσβασης που εμφανίζουν οι χρήστες, πιθανολογείται ότι αφορούν στοιχεία πρόσβασης σε εσωτερικά συστήματα και βάσεις δεδομένων. Πιθανολογείται επίσης ότι οι hackers απέκτησαν πρόσβαση στο σύστημα διαχείρισης εγγράφων (document management system) του Υπουργείου Οικονομικών και συγκεκριμένα του Οργανισμού Διαχείρισης Δημοσίου Χρέους (Ο.Δ.Δ.Η.Χ). Δεν αποσαφηνίστηκε από τους hackers που ακριβώς διαθέτουν μη εξουσιοδοτημένη πρόσβαση, αλλά από το είδος των εγγράφων που αναρτήθηκαν είναι εξακριβωμένο ότι αφορά πλήθος υπηρεσιών του Υπουργείου Οικονομικών.

- Gridlock: Υπόθεση παιδικής πορνογραφίας

Μια ευρεία αστυνομική επιχείρηση, με την κωδική ονομασία «Gridlock», πραγματοποιήθηκε σε διάφορες περιοχές της Ελλάδας (Αττική, Δράμα, Χαλκίδα, Ικαρία και Ρόδο), από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης

Ηλεκτρονικού Εγκλήματος, στο πλαίσιο της καταπολέμησης του φαινομένου της κατοχής και διακίνησης υλικού παιδικής πορνογραφίας, μέσω του διαδικτύου.

Στη διάρκεια της επιχείρησης, που πραγματοποιήθηκε το τελευταίο δεκαπενθήμερο του Νοεμβρίου του 2012, σχηματίστηκαν 10 αυτοτελείς δικογραφίες και συνελήφθησαν με την αυτόφωρη διαδικασία 8 ημεδαποί, ηλικίας από 25 έως 71 ετών, για πορνογραφία ανηλίκων, μέσω διαδικτύου. Τέσσερις συνελήφθησαν στην Αττική και από ένας σε Δράμα, Χαλκίδα, Ικαρία και Ρόδο. Ανάμεσά τους ήταν ένας στρατιωτικός, ένας δικαστικός επιμελητής, ένας 71χρονος συνταξιούχος και ένας επιχειρηματίας.

Μετά από Εισαγγελική διάταξη, δημοσιοποιήθηκε η ταυτότητα τριών εκ των συλληφθέντων. Ειδικότερα, ύστερα από αστυνομική διαδικτυακή ψηφιακή έρευνα στον παγκόσμιο ιστό, που πραγματοποιήθηκε μέσω του ειδικού προγράμματος TLO (λογισμικό σάρωσης ηλεκτρονικών ιχνών διακίνησης πορνογραφικού υλικού), που διαθέτει η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, εντοπίστηκαν ηλεκτρονικά ίχνη ημεδαπών χρηστών του διαδικτύου, που διακινούσαν «σκληρό» υλικό παιδικής πορνογραφίας. Το υλικό αυτό περιελάμβανε φωτογραφίες και οπτικοακουστικό υλικό παιδιών, από βρέφη μέχρι της ηλικίας των 11 χρόνων, παιδιών που υποβάλλονταν σε βασανισμό και σεξουαλική κακοποίηση από ζώα και ενήλικες.

Παράλληλα, διαμοίραζαν αυτό το υλικό σε άλλους χρήστες του διαδικτύου, μέσω ειδικών προγραμμάτων ανταλλαγής αρχείων (Peer to Peer).

Από τις έρευνες που διενεργήθηκαν στις οικίες των κατηγορουμένων, παρουσία Εισαγγελικών Λειτουργών, βρέθηκαν και κατασχέθηκαν συνολικά: 10 σκληροί δίσκοι ηλεκτρονικών υπολογιστών, 4 φορητοί ηλεκτρονικοί υπολογιστές,πλήθος εκτυπωμένων φωτογραφιών, μεγάλος όγκος ψηφιακών αρχείων, κυνηγητικά όπλα, 2 πιστόλια κρότου με συνολικά 6 φυσίγγια και 1 τυφέκιο. Τα ψηφιακά μέσα κατασχέθηκαν και στάλθηκαν στη Διεύθυνση Εγκληματολογικών Ερευνών, για εργαστηριακές εξετάσεις. Επίσης, δύο από τους εμπλεκόμενους κατηγορούνται και για παράνομη κατοχή των παραπάνω όπλων και πυρομαχικών.

Από τους οκτώ συλληφθέντες, που οδηγήθηκαν στις κατά τόπους αρμόδιες Εισαγγελικές Αρχές, οι δύο προφυλακίστηκαν. Για τα δυο άτομα, που δεν συνελήφθησαν ελλείψει των όρων του αυτοφώρου, οι σχετικές δικογραφίες υποβλήθηκαν στις Εισαγγελικές Αρχές.

- Υπόθεση Amanda Todd

Η Amanda Todd είχε γεννηθεί στο Βανκούβερ το 1996 και σε ηλικία 15 χρόνων βρέθηκε νεκρή. Η Amanda οδηγήθηκε σε προφανή αυτοκτονία δι' απαγχονισμού εξαιτίας του επίμονου και σκληρού εκφοβισμού που δεχόταν διαδικτυακά επί καθημερινής βάσεως. Πριν αυτοκτονήσει, η Amanda περιέγραψε πως ξεκίνησε η παρενόχληση της σε ένα βίντεο στο youtube που ανέβασε το Σεπτέμβριο του 2012. Η Amanda εκφράστηκε μέσα από κάρτες, χωρίς να ονοματίζει πρόσωπα, λέγοντας πως

όταν ήταν στην πρώτη γυμνασίου έδειξε επίμαχα σημεία του σώματος της σε έναν άντρα στο διαδίκτυο.

Ένα χρόνο μετά, ο άντρας αυτός την εντόπισε μέσω Facebook απαιτώντας να του στείλει πιο αισχρές φωτογραφίες και προωθούσε τις αρχικές φωτογραφίες της. Όταν η Αμάντα άλλαζε σχολεία, ο άντρας αυτός συνέχιζε να την παρενοχλεί, αυτή τη φορά φτιάχνοντας προφίλ στο Facebook, χρησιμοποιώντας τις φωτογραφίες της χωρίς επεξεργασία ως εικόνα προφίλ και δημιουργώντας έτσι παρενόχληση και στην καθημερινότητά της από τα πειράγματα των συνομήλικων της.

Η επονομαζόμενη ομάδα χάκερ Anonymous ισχυρίζεται, πως έχουν αναγνωρίσει τον «τύρρανο» της Amanda και πως είναι ένας 30χρονος υπάλληλος της εταιρίας Facebook, από το New Westminster στην Βρετανική Columbia του Καναδά. Αναφέρουν πως την παρενοχλούσε τόσο αδυσώπητα που την οδήγησε στην αυτοκτονία και αναφέρθηκαν σε αυτόν λέγοντας ότι: «αυτός είναι ο παιδεραστής που μέσω της κοινωνικής δικτύωσης πίεζε την Amanda Todd να του παρέχει γυμνές φωτογραφίες της».

Ο αναφερόμενος ως τύρρανος δε φαίνεται να έχει μιλήσει δημόσια από τη στιγμή που τον ανακάλυψαν οι Anonymous, αλλά εθεάθη στο δικαστήριο εξαιτίας μη διασταυρωμένων πληροφοριών για σεξουαλική παρενόχληση ανηλίκου. Μέχρι εκείνη τη στιγμή ισχυρίζονταν πως ήταν φίλος της Amanda και κατηγόρησε έναν άντρα από την Νέα Υόρκη ότι την παρενοχλούσε. Μετά από αυτό, το περιοδικό Vice δημοσίευσε πληροφορίες για δήθεν επαφές της Amanda με αυτόν τον άντρα περιλαμβανομένης και φωτογραφίες τραβηγμένες από υπολογιστή, αναρτήσεις στο Facebook και λογαριασμούς σε σελίδες ενηλίκων. Ο άντρας δήθεν αναρτούσε φωτογραφίες γυμνών έφηβων σε τέτοιους ιστότοπους και συστηματικά γνωστοποιούσε ότι εκβίαζε ανήλικα κορίτσια.

Η αντίδραση του κόσμου ποικίλει. Σε δημοσιεύματα έχει αναφερθεί ότι η απόδοση δικαιοσύνης των Anonymous αποτελεί απλά ένα «τσιρότο» σε ένα πολύ σοβαρό και γρήγορα αναπτυσσόμενο διαδικτυακό πρόβλημα το οποίο ωθεί ευάλωτα νεαρά κορίτσια όπως η Amanda Todd σε ένα πολύ περίπλοκο και καταστρεπτικό είδος κινδύνου[35],[36].

ΚΕΦΑΛΑΙΟ 4: ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Στο κεφάλαιο αυτό θα δούμε το νομοθετικό πλαίσιο που ισχύει στην Ελλάδα, καθώς 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.

Θα δούμε επίσης παραδείγματα νομοθεσίας άλλες χώρες με σύντομη αναφορά.

Στη συνέχεια, θα δούμε το ρόλο και την ιστορία του ελληνικού Σώματος Δίωξης Ηλεκτρονικού Εγκλήματος και πληροφορίες σχετικά με τα πνευματικά δικαιώματα.

4.1 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

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. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Άρθρα ποινικού κώδικα σχετικά με το Ηλεκτρονικό Έγκλημα[4]

Άρθρο 337 - Προσβολή της γενετήσιας αξιοπρέπειας

1. Όποιος με ασελγείς χειρονομίες ή προτάσεις που αφορούν ασελγείς πράξεις, προσβάλλει βάναυσα την αξιοπρέπεια άλλου στο πεδίο της γενετήσιας ζωής του τιμωρείται με φυλάκιση μέχρι ενός έτους ή χρηματική ποινή.

2. Με φυλάκιση τριών μηνών μέχρι δύο ετών τιμωρείται η πράξη της προηγούμενης παραγράφου, αν ο παθών είναι νεότερος από 12 ετών.

3. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δεκαπέντε έτη και με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.

4. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που εμφανίζεται ως ανήλικο κάτω των δεκαπέντε ετών και με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση με το εμφανιζόμενο ως ανήλικο πρόσωπο, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.

5. Όποιος τελεί την πράξη της παραγράφου 1 του άρθρου αυτού, εκμεταλλευόμενος την εργασιακή θέση του παθόντος ή τη θέση προσώπου που έχει ενταχθεί σε διαδικασία αναζήτησης θέσης εργασίας διώκεται κατ` έγκληση και τιμωρείται με φυλάκιση από έξι (6) μήνες μέχρι τρία (3) έτη και με χρηματική ποινή τουλάχιστον χιλίων (1.000) ευρώ.

Άρθρο 348 - Διευκόλυνση ακολασίας άλλων

1. Όποιος κατ` επάγγελμα διευκολύνει με οποιοδήποτε τρόπο την ασέλγεια μεταξύ άλλων τιμωρείται με φυλάκιση μέχρι ενός έτους.

2. Με φυλάκιση μέχρι τριών ετών και με χρηματική ποινή τιμωρείται όποιος διευκολύνει την ασέλγεια μεταξύ άλλων χρησιμοποιώντας απατηλά μέσα και αν ακόμη δεν ενεργεί κατ`επάγγελμα.

3. Όποιος κατ` επάγγελμα ή από κερδοσκοπία επιχειρεί να διευκολύνει, έστω και συγκαλυμμένα, με τη δημοσίευση αγγελίας, εικόνας, αριθμού τηλεφωνικής σύνδεσης ή με τη μετάδοση ηλεκτρονικών μηνυμάτων ή με οποιονδήποτε άλλο τρόπο την ασέλγεια με ανήλικο τιμωρείται με φυλάκιση και με χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

Άρθρο 348 Α - Πορνογραφία ανηλίκων

1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην επικράτεια ή εξάγει από αυτή, 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.

2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, 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 πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, 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.

4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ:

α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια

β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος.

Αν η πράξη της περίπτωσης β είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους

Όποιος με πρόθεση, μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας, προτείνει σε ενήλικο να συναντήσει ανήλικο, που δεν συμπλήρωσε τα δεκαπέντε έτη, με σκοπό τη διάπραξη σε βάρος του των αδικημάτων των παραγράφων 1 και 2 του άρθρου 339 και 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν στη διάπραξη των αδικημάτων αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.

Άρθρο 370 Α - Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας.

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή ή σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται και όποιος αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.

3. Με κάθειρξη μέχρι δέκα (10) ετών τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ᾽ επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή από πενήντα πέντε χιλιάδες μέχρι διακόσιες χιλιάδες ευρώ.

5. Αν οι πράξεις των παραγράφων 1 και 3 αυτού του άρθρου συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, τιμωρούνται κατά τα άρθρα 146 και 147 του Ποινικού Κώδικα.

Άρθρο 370 Β - Παράνομη αντιγραφή ή χρήση απορρήτων δεδομένων

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

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

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

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

Άρθρο 370 Γ - Παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα ευρώ έως πέντε χιλιάδων εννιακοσίων ευρώ.

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

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

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

Άρθρο 386 – Απάτη

1. Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη, ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστων τριών (3)

μηνών. Και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλακιση τουλάχιστον δύο(2) ετών.

2. Οι διατάξεις του άρθρου 72 για το κατάστημα εργασίας εφαρμόζονται και εδώ.

3. Επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών:

α. Αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των τριάντα χιλιάδων ευρώ ή

β. Αν το περιουσιακό όφελος ή η προξενηθέισα ζημία υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων ευρώ.

Άρθρο 386 Α - Απάτη με υπολογιστή

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

4.2 ΝΟΜΟΘΕΣΙΑ ΣΤΟ ΕΞΩΤΕΡΙΚΟ

4.2.1 Παραδείγματα

Ας δούμε κάποια παραδείγματα νομοθεσίας διαδικτυακών εγκλημάτων στο εξωτερικό.

Στο Ηνωμένο Βασίλειο από τον Φεβρουάριο του 2001, οι hacker, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες[24].

Επίσης, το 1990 ψηφίστηκε από το Κονοβούλιο του Ηνωμένου Βασιλείου και τέθηκε σε ισχύ το Computer Misuse Act, που είναι ένας νόμος για την εξασφάλιση του υλικού του υπολογιστή από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση και για σχετικά θέματα.

Το Computer Misuse Act, εισήγαγε τρία ποινικά αδικήματα:

1. Τη μη εξουσιοδοτημένη πρόσβαση στο υλικό του υπολογιστή, που τιμωρείται με κάθειρξη τουλάχιστον 6 μηνών ή με χρηματική ποινή, που δεν υπερβαίνει το επίπεδο 5 στο επίπεδο κλίμακας των χρηματικών ποινών (σήμερα είναι £ 5000).
2. Τη μη εξουσιοδοτημένη πρόσβαση με την πρόθεση την διάπρξη ή τη διευκόλυνση της διάπραξης νέων αδικημάτων, που τιμωρείται με 6 μήνες κάθειρξη και μέγιστο πρόστιμο που προβλέπεται για συνοπτική καταδίκη (δηλαδή με συνοπτικές διαδικασίες, χωρίς δικαίωμα σε δίκη με ενόρκους).
3. Τη μη εξουσιοδοτημένη τροποποίηση του υλικού του υπολογιστή, που υπόκειται στις ίδιες ποινές όπως στα αδικήματα που είδαμε στο τμήμα 2.

Ο νόμος αυτός έχει γίνει ένα πρότυπο από το οποίο αρκετές άλλες χώρες, όπως ο Καναδάς και η Δημοκρατία της Ιρλανδίας , άντλησαν έμπνευση κατά τη σύνταξη των δικών τους νόμων σχετικά με την ασφάλεια των πληροφοριών, καθώς θεωρείται ως ένα ισχυρό και ευέλικτο κομμάτι της νομοθεσίας όσον αφορά την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο[37],[38].

Στις Ηνωμένες Πολιτείες θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης της ποινής. Κάθε χρόνο το ηλεκτρονικό έγκλημα στις Ηνωμένες Πολιτείες εκτιμάται ότι κοστίζει 100 δισεκατομμυρίων δολάρια.

Σε κάποιες πολιτείες των ΗΠΑ, πχ Αϊόβα και Ουάσιγκτον, υπάρχουν νόμοι που ποινικοποιούν ορισμένες μορφές spyware. Οι εν λόγω νόμοι καθιστούν παράνομο για οποιονδήποτε άλλον εκτός από τον ιδιοκτήτη ή τον διαχειριστή του υπολογιστή για να εγκαταστήσει λογισμικό που αλλοιώνει τις ρυθμίσεις του προγράμματος περιήγησης, να παρακολουθεί πληκτρολογήσεις, ή να απενεργοποιεί το λογισμικό ασφαλείας του υπολογιστή.

Στις Ηνωμένες Πολιτείες, οι νομοθέτες εισήγαγαν ένα νομοσχέδιο το 2005, με τίτλο "Internet Spyware Prevention Act", σύμφωνα με το οποίο προβλέπεται φυλάκιση των δημιουργών του spyware[35].

4.2.2 Η Συνθήκη της Βουδαπέστης

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

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.
2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με η/υ και πλαστογραφία.
3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας
4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα

αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή Ένωση[7],[8],[42].

Ρόλος και ιστορία του ελληνικού Σώματος Δίωξης Ηλεκτρονικού Εγκλήματος.

Η Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΠΟΑΔΗΕ), λειτουργεί από τις 18 Ιουλίου 2011, ως ειδική αυτοτελής Κεντρική Υπηρεσία της Ελληνικής Αστυνομίας.

Η αποστολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από[39]:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων που ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.
- Το Τμήμα Προστασίας Ανηλίκων που ασχολείται με τα εγκλήματα που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων που ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, που ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

Μετά από πρωτοβουλία της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και του Υπουργείου Δημόσιας Τάξης & Προστασίας του Πολίτη, δημιουργήθηκε το site:

http://www.cyberkid.gov.gr/

του οποίου ο στόχος είναι να ενημερώσει γονείς και παιδιά έως 12 ετών για τους κινδύνους που μπορεί να αντιμετωπίσουν σερφάροντας στο Διαδίκτυο, όπως και να δώσει συμβουλές στους γονείς για ό, τι αφορα την ασφάλεια των παιδιών τους.

Εικόνα 11: Το σήμα των cyberkids

4.3 ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

Πνευματική ιδιοκτησία ή πνευματικά δικαιώματα, ονομάζονται τα αποκλειστικά δικαιώματα των πνευματικών δημιουργών στο έργο τους. Παραχωρούνται από τον νόμο για ορισμένο χρόνο για να απαγορεύσουν σε τρίτους τη χρήση των έργων χωρίς την άδεια του δημιουργού.

Το πνευματικό δικαίωμα υφίσταται σε έργα λογοτεχνίας και τέχνης, όπως βιβλία, θέατρο, ζωγραφική, γλυπτική, φωτογραφία, αρχιτεκτονική αλλά και άλλες δημιουργίες όπως λογισμικό ή βάσεις δεδομένων *(databases).*

Περιλαμβάνει το δικαίωμα της εκμετάλλευσης του έργου (περιουσιακό δικαίωμα) και το δικαίωμα της προστασίας του προσωπικού δεσμού του δημιουργού του προς αυτό (ηθικό δικαίωμα). Το πνευματικό δικαίωμα αποκτάται αυτοδικαίως χωρίς να απαιτείται αίτηση του δημιουργού ή καταχώριση του έργου σε κάποια υπηρεσία[39].

Η Ημέρα Ασφαλούς Διαδικτύου (SID) διοργανώνεται από το INSAFE στο τέλος Φεβρουαρίου κάθε έτους για την προώθηση της ασφαλέστερης και πιο υπεύθυνης χρήσης των online τεχνολογιών και των κινητών τηλεφώνων, ιδίως μεταξύ των παιδιών και των νέων σε όλο τον κόσμο.

Φέτος η Ημέρα Ασφαλούς Διαδικτύου την ***Τρίτη, 5 Φεβρουαρίου 2013,*** *στο πλαίσιο του πρώτου επετειακού εορτασμού των 10 χρόνων από την καθιέρωσή της. Η Ημέρα Ασφαλούς Διαδικτύου εορτάστηκε για πρώτη φορά στις 6 Φεβρουαρίου 2004 σε 16 χώρες, στο πλαίσιο της εκστρατείας επαγρύπνησης για ένα ασφαλέστερο διαδίκτυο SafeBorders, ένα έργο χρηματοδοτούμενο από το πρόγραμμα πλαίσιο Safer Internet της Ευρωπαϊκής Επιτροπής. Το 2005 ανέλαβε τα ηνία το Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων Ενημέρωσης & Επαγρύπνησης INSAFE, και σήμερα ο αριθμός των χωρών έχει ξεπεράσει κάθε ρεκόρ φθάνοντας τις 99 παγκοσμίως.*

Το το Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων Ενημέρωσης & Επαγρύπνησης INSAFE είναι ένα ευρωπαϊκό δίκτυο κέντρων ευαισθητοποίησης για την προώθηση της ασφαλούς και υπεύθυνης χρήσης του Διαδικτύου και των κινητών συσκευών για τους νέους[40].

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΒΟΥΛΕΣ ΑΣΦΑΛΕΙΑΣ

ΣΥΜΒΟΥΛΕΣ ΑΣΦΑΛΕΙΑΣ

Στο κεφάλαιο αυτό θα παρατεθούν κάποιες συμβουλές σε γονείς και νέους για την ασφαλή περιήγηση στο Διαδίκτυο, όπως και προτάσεις για την προστασία από παρενοχλήσεις, spam κ.ά.

Στη συνέχεια γίνεται σύντομη αναφορά σε λογισμικά φίλτρα και αναλύεται η λειτουργία των antivirus λογισμικών.

5.1 ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΗΝ ΠΕΡΙΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Συμβουλές για τους γονείς:

- Είναι προτιμότερη η τοποθέτηση το Η/Υ σε χώρους, όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι δίνεται τη δυνατότητα επίβλεψης των παιδιών, χωρίς αυτά να αισθάνονται ότι ελέγχονται.
- Η πλοήγηση στο Διαδίκτυο θα μπορούσε να είναι μια οικογενειακή δραστηριότητα. Χρησιμοποιείται έτσι ο υπολογιστής από τους γονείς μαζί με τα παιδιά τους.
- Οι γονείς οφείλουν να ενημερώνουν τα παιδιά τους για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chatrooms.
- Η πραγματοποίηση συζητήσεων των γονιών με τα παιδιά τους για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο, είναι μια πολύ καλή ιδέα.
- Οι γονείς θα πρέπει να διδάξουν τα παιδιά τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά τους (π.χ. επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ακόμα και ωράρια σχολείου ονόματα φίλων κ.λπ.) και φυσικά να μην χρησιμοποιούν τις πιστωτικές κάρτες τους.
- Τα παιδιά δεν πρέπει σε καμία περίπτωση να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου.
- Επίσης, τα παιδιά πρέπει να διδαχθούν από τους γονείς του να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο, αφού οι άγνωστοι με τους οποίους θέλουν να συναντηθούν, μπορεί να είναι επικίνδυνοι.
- Συνιστάται η χρήση των λεγόμενων «φίλτρων» που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητές σελίδες (βία, πορνογραφία).
- Όπως επίσης συνίσταται ο έλεγχος του περιεχομένου των οπτικοακουστικών υλικών, όπως CDs, δισκέτες κ.ά., που αγοράζουν τα παιδιά ή ανταλλάσσουν με τους φίλους τους.

- Καλό θα ήταν επίσης όλοι οι γονεις να ενημερωθούν σχετικά με τις αρμόδιες αρχές, που θα πρέπει να επικοινωνήσουν σε περίπτωση που συναντήσουν βλαβερό ή παράνομο περιεχόμενο στο Internet.

Συμβουλές για νέους:

- Δεν πρέπει να δίνετε σε κανέναν, ακόμα και στον καλύτερό σας φίλο, τοω κωδικό πρόσβασης στο Διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τον κωδικό είναι οι γονείς.
- Ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεστε «άβολα», δε θα πρέπει σε καμία περίπτωση να απαντώνται Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάσετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε.
- Αν αισθανθείτε άβολα την ώρα που συνομιλείτε μέσω chatroom, διακόψτε αμέσως τη συνομιλία.
- Αποφύγετε να στέλνετε τη φωτογραφία σας και τα προσωπικά στοιχεία σας μέσω Διαδικτύου σε αγνώστους.
- Σκεφτείτε πολύ καλά πριν αποφασίσετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο Διαδίκτυο. Ζητείστε την άποψη των γονιών σας σχετικά με αυτό το θέμα.
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με το «διαδικτυακό σας φίλο», ενημερώστε τους γονείς σας ή κάποιο άτομο που εμπιστεύεστε και φροντίστε αυτή η συνάντηση να γίνει σε δημόσιο χώρο.
- Αναπτύξτε κριτική διάθεση σε ό,τι διαβάζετε στο Διαδίκτυο. Μην εμπιστεύεστε αμέσως ότι δείτε.
- Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν «σερφάρετε» στο Internet.

5.2 ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΕΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Στην ενότητα αυτή θα δούμε συμβουλές για να είναι ασφαλείς οι οικονομικές συναλλαγές που πραγματοποιούμε.

Κατ αρχήν οι οικονομικές συναλλαγές μέσω Διαδικτύου από Internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές,, δεν θα πρέπει να πραγματοποιούνται. Προτιμούμε πάντα τον προσωπικό μας υπολογιστή ή κάποιον για τον οποίο είμαστε βέβαιοι για το επίπεδο ασφάλειας.

Στη συνέχεια, ως προς τους κωδικούς πρόσβασης είναι χρήσιμο να:

- Να αλλάζουμε συχνά τους κωδικούς πρόσβασης.
- Να αποφεύγουμε να έχουμε τον προσωπικό μας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες και

- Να μη δίνουμε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις.

5.3 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΑ SPAM

Σε αυτό το σημείο ας δούμε πως μπορούμε να προστατευτούμε από την ανεπιθύμητη αλληλογραφία:

- Δε θα πρέπει να απαντάμε ποτέ σ' ένα spam e-mail και να μην κάνουμε πουθενά κλικ, γιατί απλούστατα η απάντησή μας ή και η άρνησή μας ακόμα θα επιβεβαιώσει την εγκυρότητα του δικού μας e-mail κι έτσι το e-mail μας θα γίνει μια πολύτιμη πληροφορία για πολλούς spammers.
- Αναζητούμε και εγκαθιστούμε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails.
- Δεν κάνουμε ποτέ προώθηση (forward) των spam e-mails σε φίλους ή και τρίτους, γιατί κι αυτοί θα προστεθούν στην λίστα αποδοχής.
- Δεν πρέπει να παρασυρόμαστε ποτέ από δελεαστικούς τίτλους, όπως "a very special message for you".
- Δε δίνουμεε εύκολα την διεύθυνση του ηλεκτρονικού ταχυδρομείου μας (e-mail).
- Δεν απαντάμε ποτέ στα spam e-mails ακόμα και στην υποτιθέμενη ένδειξη διαγραφής, γιατί έτσι διαπιστώνεται η εγκυρότητα της ηλεκτρονικής μας διεύθυνσης και επομένως όπως είδαμε και νωρίτερα θα αποτελούμε πολύτιμο στόχο για τους spammers.
- Και βέβαια αγνοούμε το προιόν όσο θελκτικό και να φαίνεται και δεν πρέπει καν να διανοηθούμε να αγοράσουμε τις υπηρεσίες/σκεύασματα που διαφημίζονται.

5.4 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Σε αυτό το σημείο ας δούμε πως μπορούμε να προστατευτούμε από τα κακόβουλα προγράμματα. Τα βήματα που θα πρέπει να ακολουθούμε είναι τα εξής:

- Επιλογή ενός καλού antivirus προγράμματος
- Συνεχής ανανέωση (update) του antivirus και τακτική ανίχνευση όλου του δίσκου
- Έλεγχος κάθε δισκέτας/cd με το antivirus πριν την ανοίξετε
- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε cd ή δισκέτα
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows

(το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού μας.

- Επιλέγουμε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να στείλει μια «φωτογραφία» ως photo.jpg. Αν δεν έχουμε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσουμε το αρχείο το οποίο θα περιέχει κάτι άλλο και όχι φωτογραφία.
- Διατήρηση της ανωνυμίας μας με την ενημέρωση του φυλλομετρητή που χρησιμοποιούμε.
- Σωστή ρύθμιση των δικτυακών εφαρμογών.

5.5 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΠΑΡΕΝΟΧΛΗΣΕΙΣ

Σε αυτό το σημείο θα δούμε πως μπορούμε να προστατευτούμε από παρενοχλήσεις:

- Επιλέγουμε ένα ουδέτερο όνομα χρήστη, e-mail κλπ. Αποφεύγουμε οτιδήποτε χαριτωμένο, σεξουαλικό, ή γυναικείο.
- Διατηρούμε τη βασική μας διεύθυνση ηλεκτρονικού ταχυδρομείου μυστική. Την χρησιμοποιούμε μόνο με ανθρώπους που γνωρίζουμε και εμπιστευόμαστε.
- Δε δίνουμε προσωπικές μας πληροφορίες απλά επειδή μας τις ζητάνε.
- Πριν συμμετάσχουμε σε οποιαδήποτε on-line δραστηριότητα, θα πρέπει να παρακολουθήσουμε για αρκετό χρονικό διάστημα το περιεχόμενο των συζητήσεων.
- Ποτέ δε δίνουμε το κωδικό πρόσβασης σε κανέναν.

5.6 ΛΟΓΙΣΜΙΚΑ ΦΙΛΤΡΑ

Ένα φίλτρο είναι ένα πακέτο λογισμικού το οποίο μπορεί να αποκλείσει την προσπέλαση σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο.

Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από το πόσο ανανεωμένες είναι οι λίστες με τους απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό περιεχόμενο. Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να αποκλείει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε περιεχόμενο με βία η ρατσισμό[7].

5.7 ANTIVIRUS

Το antivirus ή αλλιώς antivirus λογισμικό, είναι το λογισμικό εκείνο που χρησιμοποιείται για την πρόληψη, τον εντοπισμό και την άρση των κακόβουλων προγραμμάτων όλων των ειδών, όπως: ιοί υπολογιστών, rootkits, trojans, σκουλήκια, adware και spyware. Τέτοιου είδους πακέτα ασφάλειας υπολογιστών συνήθως προσφέρονται ως προϊόντα και υπηρεσίες εξειδικευμένων εταιρειών antivirus λογισμικού (π.χ., mcafee, kaspersky κά.).

Τέτοιου ειδους λογισμικά που χρησιμοποιουνται για την πρόληψη και την απομάκρυνση απειλών ακολουθούν μια ευρεία ποικιλία από στρατηγικές. Για παράδειγμα άλλοτε συμπεριλαμβάνεται η αναζήτηση για γνωστά μοτίβα δεδομένων μέσα σε εκτελέσιμο κώδικα, η ανταλλαγή αποκρυπτογραφημένων μηνυμάτων τα οποία ως επί των πλείστων μπορούν να είναι διαθέσιμα μόνο από συγκεκριμένα ασφαλή (έγκυρα), ή οχι, προγραμματα*. Ωστόσο, αυτές οι στρατηγικές δεν μπορούν να καλύψουν όλες τις δυνατές περιπτώσεις επιθέσεων, ενώ πολλές φορές οι εταιρείες καταπιάνονται με την επίλυση συγκεριμένων περιπτώσεων μόνο, αφού οι αντίστοιχες απειλές έχουν ήδη εκδηλωθεί σε υπολογιστές χρηστών, π.χ. πολλές φορές έχει τύχει ένας υπολογιστής να μολυνθεί με νέο κακόβουλο λογισμικό, για το οποίο δεν υπάρχει ακόμη γνωστή υπογραφή (ή μοτιβο λειτουργίας δεδομένων). Συνεπώς, δε μπορούσε να ελεχθεί.

Για την αντιμετώπιση τέτοιων απειλών, που αποκαλούνται και ως zero-day απειλές, μπορούν να χρησιμοποιηθούν ευριστικές προσεγγίσεις. Για παράδειγμα ένα λογισμικό προστασίας μπορεί να ψάχνει γενικά για συμπεριφορές που είναι παραλλαγές γνωστών κακόβουλων λογισμικών, ωστε να εντοπίσει νέα. Άλλες φορές ορισμένα λογισμικά προστασίας 'τρεχουν' προεπιλεγμένο κωδικα που μπορεί να προέρχεται από τον υπολογιστή κάποιου χρήστη σε ένα περιορισμένο και ασφαλές περιβάλλον. Στη συνέχεια, αναλύουν τις πιθανώς κακόβουλες ενέργειες που κάνει το αντίστοιχο εκτελέσιμο, έτσι ώστε το λογισμικό προστασίας να μπορεί να προβλέψει τη λειτουργία του συγκεκριμένου αρχείου εαν γίνει χρήση του σε άλλο περιβάλλον.

Παρ' όλα αυτά, όσο χρήσιμο και να είναι ένα λογισμικό προστασίας, ενίοτε έχει και μειονεκτήματα, π.χ. ένα λογισμικό προστασίας από ιούς μπορεί να επηρεάσει την απόδοση του υπολογιστή καταναλώνοτας υπερβολικά πολλούς υπολογιστικούς πόρους (οπως η μνήμη, η μονάδα επεξεργασίας κτλ.). Άλλες φορες, μη έμπειροι χρήστες μπορεί να έχουν προβλήματα κατανόησης των αποφάσεων που παίρνει ένα εκάστοτε λογισμικό προστασίας. Τέτοιου είδους καταστάσεις μπορούν να οδηγήσουν εν τέλει σε μια καλώς εννοούμενη αλλά λανθασμένη απόφαση η οποία μπορεί να καταλήξει ακόμη και στη δημιουργία μιας νέας δυνατότητας παραβίασης της ασφάλειας. Εξάλλου εάν το λογισμικό προστασίας βασίζεται σε ευριστικές τεχνικές ανίχνευσης απειλών, η επιτυχία εξαρτάται από την επίτευξη μιας σωστής προβλεψης.

Σε καμία περίπτωση όμως ένα λογισμικό προστασίας δεν αποτελεί λύση για όλα τα θέματα ασφαλείας. Ακόμη κι αν ένας χρήστης έχει εγκαταστήσει πολλά τέτοια λογισμικά με σκοπό τα πλεονεκτήματα του ενός να εξισορροπούν τα μειονεκτήματα κάποιου άλλου και πάλι μπορεί να υπάρξουν καταστροφικά αποτελέσματα.

Κλείνοντας, μπορούμε να πούμε ότι την πιο χρήσιμη πρόληψη μπορεί να την κάνει ο ίδιος ο χρήστης με τη συμπεριφορά του, αποφεύγοντας ύποπτες ενέργειες και ακολουθώντας τις συμβουλές ασφαλείας που αναφέραμε προηγουμένως[41].

ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η εργασία αυτή είχε ως στόχους να παραθέσει στον αναγνώστη πληροφορίες σχετικά με το ηλεκτρονικό έγκλημα.

Αρχικά, εξήγησε τί είναι το ηλεκτρονικό έγκλημα και ποιά είναι τα χαρακτηριστικά του. Στη συνέχεια είδαμε τα είδη του ηλεκτρονικού εγκλήματος και κάποια από αυτά αναλύθηκαν περαιτέρω. Ένα σημαντικό στοιχείο για τη σωστή πληροφόρηση επί του θέματος είναι και οι στατιστικές έρευνες που έχουν πραγματοποιηθεί . Κάποιες από αυτές, ίσως οι πιο σημαντικές, αναφέρθηκαν νωρίτερα στο αντίστοιχο κεφάλαιο.

Επίσης, αναλύθηκε το νομοθετικό πλαίσιο που ισχύει στην Ελλάδα και αναφέρθηκαν κάποια παραδείγματα νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα σε χώρες του εξωτερικού.

Στο τέλος, που πλέον ο αναγνώστης έχει μια σφαιρική εικόνα επί του θέματος, δίνονται κάποιες συμβουλές για την ασφάλειά του κατά την περιήγησή του στο Διαδίκτυο. Επιπλέον στο ίδιο κεφάλαιο, αναλύθηκαν και οι τρόποι λειτουργίας του antivirus λογισμικού.

Ο αναγνώστης μέσω αυτής της εργασίας εύκολα μπορεί να συνειδητοποιήσει ότι οι κίνδυνοι κατά την περιήγηση στο Διαδίκτυο είναι πολλοί σε αριθμό και μπορούν να έχουν καταστροφικά αποτελέσματα είτε στον ίδιο το χρήστη (βλ. Επιθέσεις παρενόχλησης, Απάτες μέσω Διαδικτύου κ.ά.), είτε στον υπολογιστή του (βλ. Ιοί, Trojans κ.ά.).

Παρόλ' αυτά όμως, η παρούσα εργασία εξηγεί στον αναγνώστη ότι ο πανικός δεν είναι λύση, αφού ο κάθε χρήστης μπορεί να προστατευθεί από τους κινδύνους όχι μόνο εγκαθιστώντας λογισμικά φίλτρα και antivirus λογισμικά, αλλά και προσαρμόζοντας ο ίδιος τη συμπεριφορά του.

Τα βασικά ερωτήματα που δημιουργήθηκαν και επιχειρήθηκε να απαντηθούν στην παρούσα εργασία είναι:

1. «Τί εννοούμε με τον όρο ηλεκτρονικό έγκλημα;»

   Απάντηση:

   Μια σύντομη απάντηση είναι ότι όταν λέμε ηλεκτρονικό έγκλημα, εννοούμε εκείνες τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων.

2. «Πώς ταξινομούνται τα ηλεκτρονικά εγκλήματα;»

   Απάντηση:

   Τα ηλεκτρονικά εγκλήματα ταξινομούνται σε μη βίαια ηλεκτρονικά εγκλήματα και βίαια ή δυνητικά βίαια ηλεκτρονικά εγκλήματα.

3. «Σε ποιές κατηγορίες διακρίνεται το κακόβουλο λογισμικό;»

   Απάντηση:

   Το κακόβουλο λογισμικό οι τέσσερις κύριες κατηγορίες περιλαμβάνουν: Ιούς (viruses), σκουλήκια (worms), Δούρειους ίππους (Trojan Horses) και Rootkits.

4. «Τί είναι το spam;»

Απάντηση:

Όταν λέμε spam, εννοούμε την ανεπιθύμητη ηλεκτρονική επικοινωνία, δηλαδή κάθε ηλεκτρονικό μήνυμα που αποστέλλεται με σκοπό την εμπορική προώθηση προϊόντων ή υπηρεσιών ή και κάθε άλλο διαφημιστικό σκοπό χωρίς ο παραλήπτης να έχει δώσει τη συγκατάθεσή του γι' αυτό.

5. «Ποιές είναι οι απάτες που μπορεί να συμβούν μέσω Διαδικτύου;»

   Απάντηση:

   Κάποιες από τις σημαντικότερες απάτες που μπορούν να συμβούν μέσω Διαδικτύου είναι οι απάτες συναλλαγών, οι απάτες με πλαστές ταχυδρομικές επιταγές, απάτες με πωλήσεις αυτοκινήτων στο Διαδίκτυο, απάτες με δημοπρασίες, απάτες μεταφοράς χρημάτων, και άλλες.

6. «Πόσα χρόνια υπάρχει το ελληνικό Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος;»

   Απάντηση:

   Η ελληνική Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΠΟΑΔΗΕ), λειτουργεί από τις 18 Ιουλίου 2011. Αξιοσημείωτο είναι ότι η ΥΠΟΑΔΗΕ συνεργάζεται στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας με την Interpol και τη Europol.

7. «Τί είναι το antivirus;»

   Το antivirus ή αλλιώς antivirus λογισμικό, είναι το λογισμικό που χρησιμοποιείται για την πρόληψη, τον εντοπισμό και την άρση των κακόβουλων προγραμμάτων από τον υπολογιστή του χρήστη.

8. «Υπάρχει περίπτωση να εμφανιστούν στο μέλλον και άλλες μορφές/είδη ηλεκτρονικού εγκλήματος;»

   Απάντηση:

   Ναι, στο μέλλον υπάρχει περίπτωση να εμφανιστούν και άλλες μορφές/είδη ηλεκτρονικού εγκλήματος. Με την εξέλιξη της τεχνολογίας θα αναπτυχθούν και νέες εφαρμογές, γεγονός που θα ευνοήσει τους κακόβουλους χρήστες να σχεδιάσουν και/ή να δημιουργήσουν νέες ή βελτιωμένες τεχνικές ανάπτυξης κακόβουλου λογισμικού.

Ένα από τα ανοιχτά ζητήματα που θα μπορούσαν να διερευνηθούν από μια μελλοντική επέκταση της παρούσας εργασίας είναι η αντιμετώπιση των κυβερνήσεων απέναντι στα κοινωνικά δίκτυα (π.χ. Facebook, Twitter, Blogger, My Space κ.ά.).

- Πολλές φορές για την αντιμετώπιση του ηλεκτρονικού εγκλήματος οι κυβερνήσεις ζητούν στοιχεία που αφορούν χρήστες τους ή ζητούν την κατάργηση περιεχομένου από τις υπηρεσίες τους. Για παράδειγμα η Google, όπως και άλλες εταιρείες τεχνολογίας και επικοινωνιών, λαμβάνει ανά τακτά χρονικά διαστήματα αιτήματα από κρατικούς φορείς και δικαστήρια ανά τον κόσμο προκειμένου να καταργήσει περιεχόμενο από τις υπηρεσίες της ή να εξετάσει το σχετικό περιεχόμενο για να καθορίσει εάν θα πρέπει να καταργηθεί για λόγους μη συμμόρφωσης με τις πολιτικές κοινότητας ενός προϊόντος.

- Σε αναφορά της Google για το εξάμηνο Ιουλίος-Δεκέμβριος 2012 και όσον αφορά την Ελλάδα, αξίζει να αναφερθεί ότι ως απόκριση σε μια εντολή δικαστηρίου, καταργήθηκε μια ανάρτηση ιστολογίου από τον τομέα blogspot.gr που φερόταν να δυσφημίζει έναν πρώην στρατιωτικό αξιωματούχο, ο οποίος κατηγορούνταν για αθέμιτα επιχειρηματικά κέρδη μέσω πολιτικών δεσμών, συμπεριλαμβανομένων δεσμών με έναν πρώην πρωθυπουργό της Ελλάδας[43].

- Ακόμα ένα σημαντικό παράδειγμα είναι η έκθεση του κοινωνικού δικτύου Facebook για κυβερνητικά αιτήματα σε παγκόσμια κλίμακα για τους πρώτους έξι μήνες του 2013. Για την Ελλάδα, τα συνολικά αιτήματα ήταν 122, οι χρήστες/λογαριασμοί που ζητήθηκαν ήταν 141 και το ποσοστό των αιτημάτων όπου κοινοποιήθηκαν ορισμένα δεδομένα ανέρχεται στο 54%[44].

- Ένα ακόμα από τα ανοιχτά ζητήματα που θα άξιζε περισσότερη έρευνα είναι η επιρροή που μπορεί να έχει το ηλεκτρονικό έγκλημα όταν χρησιμοποιηθεί σε μεγαλύτερη κλίμακα με στόχο πολλά υποψήφια θύματα. Σε τέτοια περίπτωση λέμε ότι έχουμε επιθέσεις μέσω Διαδικτύου, οι οποίες δυνητικά προκαλούν πολλή αναστάτωση στο δίκτυο της οικονομίας ή της εξουσίας και είναι απίθανο να έχουν τόσα θύματα, όσα σε τρομοκρατική επίθεση. Οι επιθέσεις μέσω Διαδικτύου είναι ένας φόβος των κυβερνήσεων, ακθώς απειλούν υποδομές ζωτικής σημασίας και στρατιωτικού ελέγχου.

ΠΑΡΑΡΤΗΜΑ Ι: ΑΝΑΦΟΡΕΣ

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] T. Forester and P. Morrison, *Computer ethics: Cautionary tales and ethical dilemmas in computing*. Massachusetts Institute of Technology, 1994.

[2] Debarati Halder and Dr. K. Jaishankar, *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Information Science Reference (an imprint of IGI Global), 2011.

[3] Derbra Littlejohn Shinder and Ed Tittel, *Scene of the Cybercrime.Computer Forensics Handbook.* Syngress, 2002.

[4] *Σύγχρονη νομοθεσί: Ποινικός Κώδικας*, 2013.

[5] Eoghan Casey with contributions from Susan W. Brenner, *Digital evidence and Computer crime: Forensic Science, Computers and the Internet*, 3η Έκδοση. Academic Press (is an imprint of Elsevier),2011.

WEB SITES

[6]Ηλεκτρονικό Έγλημα-Δικτυακός τόπος για το ηλεκτρονικό έγκλημα, http://www.e-crime.gr/crime.htm, τελευταία επίσκεψη (10/09/2013).

[7]Ηλεκτρονικό Έγκλημα-Ελληνική Αστυνομία: Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (Υπ. Δημόσιας Τάξης & Προστασίας του Πολίτη), http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite, τελευταία επίσκεψη (10/09/2013).

[8]Wikipedia- Ηλεκτρονικό Έγκλημα, Συνθήκη Βουδαπέστης, Παραδείγματα ηλεκτρονικού εγκλήματος, Χαρακτηριστικά ηλεκτρονικού εγκλήματος, Μορφές ηλεκτρονικού εγκλήματος, http://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα, τελευταία επίσκεψη (21/09/2013).

[9]Cambridge dictionary online- Ορισμός ψηφιακής πειρατίας, http://dictionary.cambridge.org/dictionary/business-english/digital-piracy, τελευταία επίσκεψη (28/09/2013).

[10]Wikipedia- Ιός υπολογιστή, http://en.wikipedia.org/wiki/Computer_virus, τελευταία επίσκεψη (18/09/2013).

[11]Wikipedia- Ιοί μακροεντολών, http://en.wikipedia.org/wiki/Macro_virus, τελευταία επίσκεψη (18/09/2013).

[12]Wikipedia- Σκουλήκι υπολογιστή, http://el.wikipedia.org/wiki/Σκουλήκι_υπολογιστή, τελευταία επίσκεψη (18/09/2013).

[13]Wikipedia- Δούρειος Ίππος υπολογιστή, http://el.wikipedia.org/wiki/Δούρειος_Ίππος_(υπολογιστές) , τελευταία επίσκεψη (18/09/2013).

[14]Kaspersky lab- Δούρειος Ίππος υπολογιστή, http://www.kaspersky.com/internet-security-center/threats/trojans, τελευταία επίσκεψη (05/10/2013).

[15]Wikipedia- Rootkits, http://el.wikipedia.org/wiki/Rootkit, τελευταία επίσκεψη (28/09/2013).

[16]Windows Sysinternals- Rootkits, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, τελευταία επίσκεψη (28/09/2013).

[17] Symantec- Windows Rootkit Overview, http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf, τελευταία επίσκεψη (28/09/2013).

[18]Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα- Ανεπιθύμητες Ηλεκτρονικές Επικοινωνίες- SPAM, http://www.dpa.gr/portal/page?_pageid=33,127423&_dad=portal&_schema=PORTAL, τελευταία επίσκεψη (05/10/2013).

[19]Wikipedia-Ανεπιθύμητη αλληλογραφία, http://en.wikipedia.org/wiki/Email_spam, τελευταία επίσκεψη (05/10/2013).

[20]Wikipedia- Χάκερ, κράκερ, http://el.wikipedia.org/wiki/Χάκερ, τελευταία επίσκεψη (10/10/2013).

[21]Kaspersky lab- Adware, http://www.kaspersky.com/internet-security-center/threats/adware, τελευταία επίσκεψη (05/10/2013).

[22]Kaspersky lab- Pornware, http://www.kaspersky.com/internet-security-center/threats/pornware, τελευταία επίσκεψη (05/10/2013).

[23]Web encyclopedia- Spyware, http://www.webopedia.com/TERM/S/spyware.html, τελευταία επίσκεψη (15/10/2013).

[24]Wikipedia- Spyware, http://en.wikipedia.org/wiki/Spyware, τελευταία επίσκεψη (15/10/2013).

[25]Wikipedia- Επιθέσεις παρενόχλησης, http://en.wikipedia.org/wiki/Cyberbullying, τελευταία επίσκεψη (01/10/2013).

[26]Website managed by the U.S. Department of Health & Human Services, Πληροφορίες για τις Επιθέσεις Παρενόχλησης, http://www.stopbullying.gov/cyberbullying/what-is-it/, τελευταία επίσκεψη (01/10/2013).

[27]Wikipedia- Απάτες στο Διαδίκτυο, http://en.wikipedia.org/wiki/Internet_fraud, τελευταία επίσκεψη (14/10/2013).

[28]The United States Department of Justice- Απάτες στο Διαδίκτυο, http://www.justice.gov/criminal/fraud/internet/, τελευταία επίσκεψη (14/10/2013).

[29]Wikipedia- HTTP cookie, http://en.wikipedia.org/wiki/HTTP_cookie, τελευταία επίσκεψη (14/10/2013).

[30]Η ελληνική ανοιχτή γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο- Στατιστικά στοιχεία σχετικά με το Ηλεκτρονικό Έγκλημα στην Ελλάδα, http://www.safeline.gr/kataggelies/statistika-stoiheia, τελευταία επίσκεψη (08/10/2013).

[31]Ελληνική Αστυνομία, Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (Υπ. Δημόσιας Τάξης & Προστασίας του Πολίτη) Δημοσίευση στατιστικών στοιχείων συνολικής δραστηριότητας της Ελληνικής Αστυνομίας για το 2011: Στατιστικά στοιχεία εγκληματικότητας, εγκλημάτων κατά της οικονομίας, παράνομης διακίνησης μεταναστών, συγκεντρώσεων, αθλητικών εκδηλώσεων, καθώς και απολογισμού της αστυνομικής ανταπόκρισης για το έτος 2011- Στατιστικά στοιχεία σχετικά με το Ηλεκτρονικό Έγκλημα στην Ελλάδα, http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=12774&Itemid=863&lang, τελευταία επίσκεψη (08/10/2013).

[32]Στατιστικά στοιχεία εγκληματικότητας, εγκλημάτων κατά της οικονομίας, παράνομης διακίνησης μεταναστών, συγκεντρώσεων, αθλητικών εκδηλώσεων, καθώς και απολογισμού της αστυνομικής ανταπόκρισης για το έτος 2012- Στατιστικά στοιχεία σχετικά με το Ηλεκτρονικό Έγκλημα στην Ελλάδα, http://www.3comma14.gr/pi/?survey=16467, τελευταία επίσκεψη (08/10/2013).

[33]Οργανισμός INHOPE- Στατιστικά στοιχεία που αφορούν την περίοδο Σεπτέμβριος 2005 - Ιούνιος 2010, http://www.inhope.org/gns/internet-concerns/internet-trends.aspx, τελευταία επίσκεψη (12/10/2013).

[34]Enigma Software Group: Applications for the masses- Χώρες με περισσότερα εγκλήματα στο Διαδίκτυο, http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, τελευταία επίσκεψη (12/10/2013).

[35]Wikipedia- Υπόθεση Amanda Todd, http://en.wikipedia.org/wiki/Suicide_of_Amanda_Todd, τελευταία επίσκεψη (13/10/2013).

[36]Fox News- Υπόθεση Amanda Todd , http://www.foxnews.com/world/2012/10/12/canadian-teen-found-dead-weeks-after-posting-wrenching-youtube-video-detailing/, τελευταία επίσκεψη (13/10/2013).

[37]Wikipedia- Computer Misuse Act 1990, http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990, τελευταία επίσκεψη (16/10/2013).

[38]The official home of revised enacted U.K. legislation- Computer Misuse Act 1990, http://www.legislation.gov.uk/ukpga/1990/18, τελευταία επίσκεψη

[39]Wikipedia- Πνευματική Ιδιοκτησία, (16/10/2013).http://el.wikipedia.org/wiki/Πνευματική_ιδιοκτησία, τελευταία επίσκεψη(18/10/2013)

[40]Safer Internet Day Website- Ημέρα Ασφαλούς Διαδικτύου, http://www.saferinternetday.org/web/guest, τελευταία επίσκεψη(28/09/2013)

[41]Wikipedia- Antivirus λογισμικό, http://en.wikipedia.org/wiki/Antivirus_software, τελευταία επίσκεψη (20/09/2013).

[42]Council of Europe, the Official Website of the Treaty Office- Συνθήκη για το Ηλεκτρονικό Έγκλημα- Συνθήκη της Βουδαπέστης, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, τελευταία επίσκεψη (31/09/2013).

[43]Google- Αναφορά διαφάνειας, Αξιοσημείωτες παρατηρήσεις – Ιούλιος-Δεκέμβριος 2012, http://www.google.com/transparencyreport/removals/government/?hl=el, τελευταία επίσκεψη (19/10/2013).

[44]Facebook- Παγκόσμια έκθεση για τα κυβερνητικά αιτήματα, https://www.facebook.com/about/government_requests, τελευταία επίσκεψη(19/10/2013).

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΑΚΡΩΝΥΜΑ

ΕΛΛΗΝΙΚΟΙ ΟΡΟΙ

Ακρώνυμο	Επεξήγηση
δις.	Δισεκατομμύρια
Η/Υ	ηλεκτρονικός υπολογιστής (ή κοινώς computer)
κ.α.	κι άλλα
κ.λπ.	και λοιπά
Ο.Δ.ΔΗ.Χ	Οργανισμός Διαχείρισης Δημοσίου Χρέους
Π.Δ.	Προεδρικό διάταγμα
π.χ.	παραδείγματος χάριν
Φαξ	βλ. FAX

ΑΓΓΛΙΚΟΙ ΟΡΟΙ

Ακρώνυμο	Επεξήγηση
(d)DoS attack	Επίθεση Άρνησης Εξυπηρέτησης; (distributed) Denial of Service attack.
API	Application Programming Interface.
DNS	Domain Name System
FAX	Αναφέρεται στις συσκευές και στην σχετική διαδικασία τηλεφωνικής μετάδοσης ακριβούς αντιγράφου εγγράφων; προκύπτει από το λατινικό fac simile που σημαίνει 'κανω ίδιο ή παρόμοιο'.
HTTP	Hyper Text Transfer Protocol
IRC	Internet Relay Chat (υπηρεσία συνομιλιών)
MMS	Multi-Media Messaging
Sexting	Προκύπτει από το Sex και το texting που σημαίνει ανταλλαγη μυνημάτων με 'ερωτικό' περιεχόμενο.
SID	Safer Internet Day (Ημέρα Ασφαλούς Διαδικτύου)
SMS	Short Message Service
USB	Universal Serial Bus
www	World Wide Web

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΓΛΩΣΣΑΡΙΟ

ΓΛΩΣΣΑΡΙΟ

Όρος	Επεξήγηση
(d) DoS attacks	Επιθέσεις Άρνησης Εξυπηρέτησης / (distributed) Denial of Service attacks.
(Hard) Disk Cluster	Συμπλέγμα (σκληρού) δίσκου.
(Internet) Browser	Φυλλομετρητής του web (πρόγραμμα περιήγησης διαδικτύου).
(Web) page	Ιστοσελίδα (αλλιώτικα αναφέρεται και ως web-page, webpage).
(Web) site	Δικτυακός τόπος (αλλιώτικα αναφέρεται και ως web-site, website ή σκέτο site).
Add-on	(επι)πρόσθετο.
Antivirus	Αντιβιοτικό/αντικό λογισμικό.
Armored Virus	Θωρακισμένος ιός.
Black hat	Βλ. Cracker.
Browser cookie	Βλ. Cookie.
Browser hijacker	Πειρατής του προγράμματος περιήγησης.
Browser hijacking	Βλ. Browser hijacker.
Camouflage Virus	Ιός παραλλαγής.
Chat room	Με τον όρο chat room (αλλιώτικα chat-room ή chatroom) γίνεται αναφορά σε τέτοιους "εικονικούς τόπους" στο ίντερνετ όπου χρήστες μπορούν και συζητούν (chat) συγχρόνως, κυρίως με γραπτά μηνύματα ή/και με συγκεκριμένο θέμα.
Cookie	Ένα μικρό κομμάτι δεδομένων που αποστέλλεται από μια ιστοσελίδα και αποθηκεύεται στον browser του χρήστη, ενώ ο χρήστης περιηγείται στην ιστοσελίδα.
Cracker	Hacker με κακή πρόθεση. Οι crackers καλούνται και 'black hats' και οι ενεργειές τους cracking.
Cross-site scripting	Αυτό το είδους επίθεσης αναφέρεται στην περίπτωση που ο επιτιθέμενος έχει εισάγει και κρύψει δικό του κακόβουλο κώδικα μέσα σε κάποια κατά τα άλλα ασφαλή σελίδα χωρις ούτε ο χρήστης να το γνωρίζει αυτο αλλά ούτε κι ο διαχειριστής αυτής να το έχει αντιληφθεί.
Cyberbulling	Επιθέσεις παρενόχλησης.
Cyberspace	Βλ. Διαδίκτυο.
Cyberstalking	Κατασκοπία μέσω διαδικτύου ή αλλιώς διαδικτυακή

Όρος	Επεξήγηση
	καταδίωξη.
Cyberthreats	Διαδικτυακές απειλές.
Cybertrerrosism	Τρομοκρατία στον κυβερνοχώρο.
Cybertresspassing	Παρακολούθηση δικτυακών πόρων.
Database	Βάση δεδομένων (αλλιώτικα και ως data-base, data base ή σκέτο DB).
Denigration	Δυσφήμιση.
Dialer (program)	Πρόγραμμα που δημιουργεί τη σύνδεση στο διαδίκτυο.
Digital piracy	Ψηφιακή πειρατία.
Downloader	Ένα πρόγραμμα που έχει σχεδιαστεί για την ανάκτηση κι εγκατάσταση λογισμικού ή επιπρόσθετων αρχείων - π.χ., για την αυτόματη αναβάθμιση λογισμικού όπως του λειτουργικού συστήματος, προγραμμάτων περιήγησης, anti-virus κι anti-spyware εφαρμογών, κ.α.
e-Banking	Ηλεκτρονικές τραπεζικές συναλλαγές; E-banking από το electornic banking.
e-Business	Ηλεκτρονικό επιχειρείν; E-business από το electornic business.
e-Commerce	Ηλεκτρονικό Εμπόριο; E-commerce από το electornic commerce.
e-Government	Ηλεκτρονική διακυβέρνηση; E-government από το electornic government.
e-Learning	Ηλεκτρονική μάθηση; E-learning από το electornic learning.
e-Mail	Αλληλογραφεία μέσω ηλεκτρονικού ταχυδρομείου; E-mail από το electornic mail.
e-Shop	Κατάστημα ηλεκτρονικού εμπορίου.
Exclusion	Αποκλεισμός.
FAX	Φαξ.
Firewall	Λογισμικό δικτύου αποτελεί ένα όριο ασφαλείας μεταξύ του έμπιστου (εσωτερικού) δικτύου και του εξωτερικού (ίσως κακόβουλου) περιβάλλοντος. Στόχος του είναι να ελέγχει την εισερχόμενη και την εξερχόμενη κίνηση από και προς κάποιον υπολογιστή δικτύου .
Flaming	Ανάφλεξη.
Freeware	Είναι το λογισμικό εκείνο που είναι διαθέσιμο στους χρήστες χωρίς κανένα κόστος.
Gray hats	Εθελοντές hacker - δηλαδή τα άτομα αυτά που χρησιμοποιούν τους υπολογιστές για τη διερεύνηση και την προσπάθεια να

Όρος	Επεξήγηση
	τιμωρηθούν οι υποτιθέμενοι εγκληματίες του κυβερνοχώρου.
Hacker	Βλ. Χάκερ.
Hacktivist	Hacker που χρησιμοποιεί τους υπολογιστές και το διαδίκτυο για να μεταφέρει πολιτικά μηνύματα.
Harassment	Παρενόχληση.
HTTP	Το πρωτόκολλο αυτό (Hypertext Transfer Protocol ή HTTP) αποτελεί την βάση της επικοινωνίας στο web.
HTTP cookie	Βλ. Cookie.
HttpOnly cookie	Ένα είδος cookie συνεδρίας.
HTTPs	Hypertext Transfer Protocol Secure (βλ. HTTP)
Impersonation	Πλαστοπροσωπία.
In-memory cookie	Βλ. Session cookie
Internet	Βλ. Διαδίκτυο.
IRC client	Υπηρεσίες συνδιάλεξης σε πραγματικό χρόνο μέσω Διαδικτύου
Macro	Μακροεντολή - ένα ομαδοποιημένο σύνολο εντολών.
Macro-virus	Ιός μακροεντολής.
Mailbox	Ηλεκτρονική θυρίδα.
Malware	Κακόβουλο λογισμικό.
Multipartite Virus	Πολυτμηματικός ιός
Online	Η κατάσταση κατά την οποία κάποιος χρήστης (το μηχάνημά του ή κάποιο από τα προγράμματα) είναι συνδεδεμένο στο διαδίκτυο (on-line).
Outing	Ξεμπρόστιασμα.
Peer-to-peer (P2P)	Ειδικά προγράμματα ανταλλαγής αρχείων μεσω δικτύου όπου κάθε υπολογιστής μπορεί να είναι ταυτόχρονα και server και client επιτρέποντας έτσι πρόσβαση σε αρχεία και περιφερειακά χωρίς την ανάγκη κάποιου κεντρικού διαχειριστή. Αυτό το χαρακτηριστικό είναι που μπορεί να κάνει και τους αντίστοιχους χρήστες πιο ευάλωτους σε κακόβουλες επιθέσεις.
Persistent cookie	Μόνιμο cookie.
Phising	Ηλεκτρονικό ψάρεμα.
Polymorphic Virus	Πολυμορφικός ιός (self-mutating).
Pop-up (windows)	Τα pop-up ads ή pop-ups είναι νέα παράθυρα (windows) που ανοίγουν αυτόματα, συχνά με σκοπό να εμφανισθούν κάποια μυνήματα - οι διαφημίσεις που παράγονται από adware είναι

Όρος	Επεξήγηση
	μερικές φορές στη μορφή ενός pop-up.
Safer internet day (SID)	Ημέρα Ασφαλούς Διαδικτύου
Screen shots	Αρχεία εικόνας με την απεικόνιση της οθόνης του υπολογιστή όπως αυτή ήταν κάποια συγκεκριμένη στιγμή.
Server	Διακομιστής.
Session cookie	Cookie συνεδρίας
Shareware	Λογισμικό με άδεια δοκιμής για μια περιορισμένη έκδοση αυτού, η οποία διατίθεται δωρεάν προς δοκιμή για ένα συγκεκριμένο χρονικό διάστημα.
Shell	Κέλυφος
Software	Λογισμικό
Source code virus	Ιός πηγαίου κώδικα
Spacefiller Virus	Ιός πλήρωσης κενών
Spam	Ανεπιθύμητη αλληλογραφία (η ενέργεια αναφέρεται ως spamming ενώ το πρόσωπο που στέλνει τα spams λέγεται spammer).
Spyware	Λογισμικό Κατασκοπίας.
Stealth Virus	Αόρατος ιός
System monitor	Τύπος λογισμικού κατασκοπίας.
System sector	Τομέας σκληρού δίσκου συστήματος
Tracking cookie	Cookie παρακολούθησης
Transient cookie	Βλ. Session cookie
Trickery	Εξαπάτηση
Virus	Ιός (κακόβουλο λογισμικό).
Web	Βλ. Διαδίκτυο; εναλλακτικά και World Wide Web (www).
Web cookie	Βλ. Cookie.
White hats	Hackers που εισβάλλουν σε κάποιο σύστημα μόνο και μόνο για να αναγνωρίσουν ποια είναι τα τρωτά του σημεία.
Worms	Σκουλήκια (κακόβουλο λογισμικό).
Διαδίκτυο	Ο όρος διαδίκτυο (ή εναλλακτικά εντος της εργασίας και αναφερόμενος ως διεθνές ηλεκτρονικό δίκτυο ή και κυβερνοχώρος) αναφέρεται σε εκείνη την παγκόσμια δομή που συνδέει μεταξύ τους μικρότερα δίκτυα υπολογιστών που επικοινωνούν ήδη μεταξύ τους. Μέσω του διαδικτύου (internet ή ίντερνετ) πάμπολλα ιδιωτικά, εμπορικά, κυβερνητικά κ.ά. δίκτυα δικτύων μπορούν να ανταλλάσουν

Όρος	Επεξήγηση
	πληροφορίες μεταξύ τους. Η πιο συνήθης πλατφόρμα πρόσβασης σε δεδομένα εντός αυτού του περιβαλλόντος ηλεκτρονικής επικοινωνιας υπολογιστών (του λεγόμενου και κυβερνοχώρου ή cyberspace) είναι το web - ένα σύστημα αποθήκευσης και πρόσβασης σε έγγραφα συστηματικής μορφής μέσω συγκεκριμένου πρωτοκόλλου.
Internet fraud	Διαδικτυακή απάτη ή αλλιώς απάτη στο διαδίκτυο.
Internet theft	Διαδικτυακή κλοπή.
Κυβερνοχώρος	Βλ. Διαδίκτυο.
Opt-in (σύστημα)	(Αποστολή διαφημιστικών κυρίως μηνυμάτων) κατόπιν ρητής συγκατάθεσης του παραλήπτη.
Πειραματικό hacking	Προσπέλαση ηλεκτρονικών δεδομένων χωρίς τροποποίηση, χωρίς υστεροβουλία, ή με σκοπό την παρακολούθηση και συγκέντρωση πληροφοριών από πρόσβαση σε προσωπικά δεδομένα που δε διαμοιράζονται με πρωτοβουλία του ιδιοκτήτη τους.
Σελιδοδείκτης	Αποθήκευση της διεύθυνσης κάποιου website, αρχείου, κ.λπ. για πιο γρήγορη πρόσβαση στο μέλλον (στα αγγλικά αναφέρεται ως bookmark, ή η συντόμευση αυτών).
Χάκερ	Άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα μόνο για πειραματισμό, χώρις να ακολουθήσει κακόβουλες ενέργειες μετά την εισβολή. Η ενέργεια ενός χάκερ (hacker) είναι το hacking κι όταν συμβαίνει από μια ομάδα hackers, αυτοί καλούνται hacking-group.

ΠΑΡΑΡΤΗΜΑ IV: ΕΥΡΕΤΗΡΙΟ

ΕΥΡΕΤΗΡΙΟ