ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙΟΥ
[π. ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ]

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
Καθηγητής: Χρήστος Ε. Τσουραμάνης

ΘΕΜΑ:
«Το Ηλεκτρονικό Έγκλημα στην Ελλάδα από το 2013 έως το 2015»

ΦΟΙΤΗΤΕΣ:
ΚΑΤΣΙΒΕΛΑ ΜΑΡΙΑ ΑΜ 14807
ΚΑΤΣΙΒΕΛΑΣ ΑΓΓΕΛΟΣ ΑΜ 14808

Μεσολόγγι 2016

Ευχαριστούμε τον κ. Χρήστο Ε. Τσουραμάνη για τη βοήθειά του

και τη συνεργασία του μαζί μας!

Ευχαριστούμε ο ένας τον άλλον

για την άψογη συνεργασία που είχαμε!

Πίνακας περιεχομένων

Εισαγωγή 5

Κεφάλαιο 1ο 9

1.1 Το Ηλεκτρονικό Έγκλημα 9

1.2 Κυβερνοχώρος και παραβατική συμπεριφορά 14

1.3 Μορφές Κυβερνοεγκλήματος 17

1.4 Ηλεκτρονικοί εγκληματίες (Hackers - Crackers) 24

Μέθοδοι Επιθέσεων 28

Κίνητρα 30

Αυτοκριτική και κοινή γνώμη 31

1.5 Ιοί και κακόβουλο λογισμικό 32

Τύποι Ιών 34

Τρόποι Δράσης και Διάδοσης 36

Τρόποι Αντιμετώπισης 36

Κεφάλαιο 2ο Στατιστική μελέτη 38

2.1 Προβολή στατιστικών στοιχείων ηλεκτρονικού εγκλήματος στην Ελλάδα από το 2013 έως το 2015 38

2.2 Ανάλυση των στατιστικών στοιχείων 42

2.3 Αναφορά στα ηλεκτρονικά εγκλήματα των στατιστικών στοιχείων 43

Παραβίαση Απορρήτου (επικοινωνιών) 43

Εξύβριση – Συκοφαντική Δυσφήμηση 43

Ρατσισμός (ξενοφοβία) 44

Πνευματική Ιδιοκτησία 44

Προσωπικά Δεδομένα 45

Παιδική Πορνογραφία 45

Οικονομικές Απάτες 46

Απειλή 47

Spam – Phishing 47

Κεφάλαιο 3ο Καταπολέμηση Ηλεκτρονικού Εγκλήματος 49

3.1 Ελληνική νομοθεσία και οι αδυναμίες της 49
3.2 Καταπολέμηση, πώς συμβάλλει η κοινωνία και πώς η αστυνομία 51
Συμπεράσματα.....56
Βιβλιογραφία.....58
Ηλεκτρονική Βιβλιογραφία 58

Εισαγωγή

Ο ένοχος ενός εγκλήματος πληροί τρείς προϋποθέσεις: ***είχε κίνητρο, είχε τα μέσα και είχε και την ευκαιρία.***

Θεωρία της καθημερινής δραστηριότητας ή της ευκαιρίας

Το 2200 π.Χ. δημιουργήθηκε ο πρώτος υπολογιστής από τους αρχαίους Βαβυλώνιους με επίσημο όνομα Άβακας. Έκτοτε κατασκευάστηκαν δεκάδες υπολογιστές στην αρχαιότητα και στην περίοδο της Αναγέννησης. Το 1946 εμφανίζεται η πρώτη γενιά ηλεκτρονικών υπολογιστών και πλέον από το 1971 διανύουμε την τέταρτη γενιά. Στις αρχές του 1970 πραγματοποιούνται και οι πρώτες συνδέσεις στο διαδίκτυο με ονομασία Internet Protocol (I.P. – Πρωτόκολλο Διαδικτύωσης), ενώ το 1980 αναπτύσσεται ένας παγκόσμιος ιστός για τις ακαδημαϊκές κοινότητες, φτάνοντας στο 1990 να έχουμε ένα παγκόσμιο δίκτυο για όλους που συνεχίζει να εξελίσσεται.

Η παγκόσμια λοιπόν, αυτή ελευθερία του διαδικτύου, έδωσε τη δυνατότητα σε εκατομμύρια ανθρώπους να μαθαίνουν μέσα από μια κολοσσιαία πηγή πληροφοριών και επίκαιρων ειδήσεων και να επικοινωνούν ταχύτερα από ποτέ με το πάτημα ενός κουμπιού. Το διαδίκτυο έχει αλλάξει τον τρόπο με τον οποίο αναζητάμε στοιχεία, μαθαίνουμε, επικοινωνούμε, ζούμε μέσα στις ψηφιακές κοινωνίες, παρέχοντάς μας ταχύτητα και άνεση.

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου.

Η συμβολή του διαδικτύου στην εκπαίδευση και την εκμάθηση είναι καθοριστική, όμως η άπλετη ελευθερία που χαρίζει σε εκατομμύρια κόσμο και η μη ασφάλεια των πληροφοριών του, συνεπάγουν και την κακή χρήση του από μη

εγκεκριμένους χρήστες που εισχωρούν στον κυβερνοχώρο, επεξεργάζονται στοιχεία και αρχεία παράνομα, δημιουργώντας νέες μορφές εγκληματικότητας και παραβατικής συμπεριφοράς.

Οι νέες αυτές μορφές εγκληματικότητας έχουν ονομαστεί «Ηλεκτρονικό Έγκλημα» και παρουσιάζονται όταν το διαδίκτυο χρησιμοποιείται με σκοπό την εκμετάλλευση των καταναλωτών ή των επιχειρήσεων ιδιωτικών ή δημόσιων, την παραπλάνηση, την πειρατεία, την παιδική πορνογραφία, την εξύβριση, το ρατσισμό, τις οικονομικές απάτες και την παραβίαση απορρήτου, πνευματικών δικαιωμάτων και προσωπικών στοιχείων, λαμβάνοντας υπόψη μας πως για να διαπράξει κανείς ένα οποιοδήποτε ηλεκτρονικό έγκλημα, πρέπει να κατέχει γνώσεις ψηφιακής τεχνολογίας και ιδίως εκείνης που σχετίζεται με το διαδίκτυο.

Η εύκολη πρόσβαση με το πάτημα ενός κουμπιού από το πληκτρολόγιο του υπολογιστή, το χαμηλό κόστος, το μειωμένο ποσοστό κινδύνου, η έλλειψη γεωγραφικών περιορισμών και η ανωνυμία που έρχεται σε ρήξη με την ασφάλεια που νιώθουν οι χρήστες στο διαδίκτυο, είναι τα πιο ισχυρά όπλα που διαθέτουν οι ηλεκτρονικοί εγκληματίες.

Σύμφωνα με την επίσημη ιστοσελίδα της Ελληνικής Αστυνομίας τα χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο είναι τα εξής:

- ✓ Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- ✓ Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
- ✓ Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- ✓ Μπορεί να διαπραχθεί χωρίς τη μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.
- ✓ Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεων (new groups) ή μέσα σε chat rooms.
- ✓ Οι "εγκληματίες του Κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλουν ηλεκτρονικά μηνύματα (e-mail) με ψευδή στοιχεία.

- ✓ Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- ✓ Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.
- ✓ Η έρευνα απαιτεί κατά κανόνα συνεργασία δυο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνο κράτους είναι σπάνια.
- ✓ Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς, κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

(http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang)

Στην παρούσα εργασία θα προσπαθήσουμε να αναλύσουμε το ηλεκτρονικό έγκλημα στην Ελλάδα κατά την περίοδο του 2013 έως το 2015 με τη χρήση των επίσημων στατιστικών στοιχείων της Ελληνικής Αστυνομίας.

Πιο συγκεκριμένα, στο πρώτο κεφάλαιο επιχειρείται μια θεωρητική προσέγγιση του φαινομένου της διαδικτυακής εγκληματικότητας όπου παρουσιάζονται όλες οι διαφορετικές εννοιολογικές προσεγγίσεις και οι μορφές που μπορεί να πάρει το ηλεκτρονικό έγκλημα, οι δράστες του (hackers) και η άπλετη ελευθερία των πληροφοριών στο χώρο του διαδικτύου.

Στο δεύτερο κεφάλαιο παρουσιάζονται τα στατιστικά στοιχεία για τα ηλεκτρονικά εγκλήματα στην Ελλάδα από το 2013 έως το 2015, τα οποία και θα αναλυθούν, καθώς επίσης θα πραγματοποιηθεί και μια αναφορά σε καθένα από τα εγκλήματα των στατιστικών στοιχείων.

Στο τρίτο κεφάλαιο θα αναφερθεί η Ελληνική νομοθεσία σχετικά με το ηλεκτρονικό έγκλημα, θα τονιστούν κάποιες αδυναμίες της και θα προσπαθήσουμε να προτείνουμε μεθόδους για την καταπολέμηση και εξάλειψη των μορφών αυτών εγκληματικής συμπεριφοράς.

Τέλος, στα συμπεράσματα αποπειράται μια ανάλυση του φαινομένου του διαδικτυακού εγκλήματος, οι πιθανές εκδοχές στο μέλλον και η προσωπική γνώμη και πιθανές λύσεις επί του θέματος.

Κεφάλαιο 1ο

1.1 Το Ηλεκτρονικό Έγκλημα

«Η τεχνολογική πρόοδος είναι σαν ένα τσεκούρι στα χέρια ενός παθολογικού εγκληματία»

Albert Einstein (1879-1955)

«Ηλεκτρονικό έγκλημα είναι κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή και τη μετάδοση δεδομένων»

Ο.Ο.Σ.Α. (1986)

«Ηλεκτρονικό έγκλημα είναι μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσω τέλεσής της».

Forester-Morrison (1994)

Εγκληματικότητα δια μέσου των υπολογιστών αποτελεί κάθε εγκληματική συμπεριφορά στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης.

Rainer Von Zur Muehlen (σύμβουλος ασφάλειας)

(http://www.slideshare.net/kevopoylos/ss-2682867026)

Η τεχνολογία διαρκώς εξελίσσεται και μάλιστα ραγδαία, διεισδύοντας όλο και περισσότερο στη ζωή μας. Η ανάπτυξη των ηλεκτρονικών υπολογιστών και ιδιαίτερα της πληροφορικής και της ευρύτατης χρήσης του διαδικτύου έχουν επισύρει τεράστιες αλλαγές στην καθημερινότητα μας. Το τελευταίο χρονικό διάστημα ο όρος

"Κοινωνία της Πληροφορίας" αμφισβητείται και τείνει να αντικατασταθεί από τον όρο "Κοινωνία των Υπολογιστών".

Μέχρι σήμερα, η πληροφορία δεσμευόταν στο πλαίσιο της έντυπης μορφής και το κύριο ερώτημα ήταν πως θα λάβει χώρα η πληροφόρηση του ανθρώπου, η πρόσφατη όμως εμφάνιση της πληροφορίας σε ψηφιακή μορφή και η διάδοσή της μέσω των ηλεκτρονικών δικτύων, την καθιστά ως το κυρίαρχο μοντέλο σε κάθε κοινωνία, αποτελώντας μια από τις σημαντικότερες προτεραιότητες του ανεπτυγμένου κόσμου και το ζητούμενο είναι η αποδοτική διαχείριση και η δυναμική και αποτελεσματική επεξεργασία του όγκου της ψηφιοποιημένης πληροφορίας η οποία έχει καταλύσει κάθε άνθρωπο που έχει πρόσβαση στο διαδίκτυο. Η δυνατότητα των ηλεκτρονικών υπολογιστών να επεξεργάζονται ταχύτατα και με μεγάλη ακρίβεια τεράστιο όγκο δεδομένων, τους καθιστά ολοένα και πιο απαραίτητους σε σχεδόν όλους τους τομείς την ανθρώπινης δραστηριότητας.

Ένα όμως, πληροφοριακό σύστημα για να είναι έμπιστο και ασφαλές θα πρέπει να παρέχει στο χρήστη του:

- ✓ **Διαθεσιμότητα (availability)**: Να είναι, δηλαδή, προσπελάσιμες και ακώλυτες οι υπηρεσίες του για τους εξουσιοδοτημένους χρήστες του.
- ✓ **Εμπιστευτικότητα (confidentiality)**: Να εγγυάται, δηλαδή, ότι τα δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες (χρήστες). Και
- ✓ **Ακεραιότητα (integrity)**: Να εξασφαλίζει, δηλαδή, τη μη τροποποίηση των δεδομένων από μη εξουσιοδοτημένους χρήστες.

Όταν οι άνωθεν ιδιότητες απουσιάζουν τότε καθιστούν το εκάστοτε δίκτυο ανασφαλές, καθώς επίσης το δικαίωμα πληροφόρησης και το δικαίωμα διάθεσης της πληροφορίας τίθενται συχνά υπό αμφισβήτηση ευνοώντας την ανάπτυξη μορφών εγκληματικότητας. Οι μορφές αυτές εγκληματικότητας έχουν κατά καιρούς λάβει διάφορους ορισμούς που έχουν συνυφαστεί με εκείνον του ηλεκτρονικού εγκλήματος (electronic crime), όπως ψηφιακό έγκλημα (digital crime), κυβερνοέγκλημα (cybercrime), διαδικτυακό έγκλημα (internet crime), τεχνολογικό έγκλημα (technological crime) και έγκλημα υψηλής τεχνολογίας (high tech crime).

Ως «Ηλεκτρονικό Έγκλημα» λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων ή κατά ενός υπολογιστικού συστήματος 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.
(http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414)

Το πρώτο «ηλεκτρονικό» έγκλημα διαπράχθηκε περίπου το 1920 στη Γαλλία, ενάντια στον Joseph-Marie Charles, γνωστό ως Joseph-Marie Jacquard (7 Ιουλίου 1752, Λυών, Γαλλία – 7 Αυγούστου 1834). Ο Jacquard ήταν εφευρέτης του ζακαργαλειού, που πρωταγωνίστησε στην τεχνολογική επανάσταση της βιομηχανικής κλωστοϋφαντουργίας και αποτέλεσε τη βάση για το σύγχρονο αργαλειό. Η ιδέα του αργαλειού σχηματίστηκε από το Jacquard το 1790, αλλά κόπηκε άδοξα από τη Γαλλική Επανάσταση, στην οποία και αγωνίστηκε από την πλευρά των επαναστατών στην άμυνα της Λυών. Το 1801 τιμήθηκε με χάλκινο μετάλλιο ευρεσιτεχνίας για τον αργαλειό και το 1806 ο αργαλειός του δηλώνεται επίσημα δημόσια περιουσία, για την οποία ο Jacquard ανταμείβεται με ισόβια σύνταξη και δικαιώματα από κάθε μηχανή που θα παρασκευαζόταν εφ' εξής. Η μηχανή του ξύπνησε πικρία και εχθρότητα μεταξύ των μεταξοϋφαντουργών, οι οποίοι φοβούμενοι πως οι μηχανές θα στερήσουν τις θέσεις εργασίας τους, έκαψαν όσες είχαν τεθεί σε παραγωγή και επιτέθηκαν στον Jacquard με σκοπό τη δολοφονία του. Τα πλεονεκτήματα όμως του αργαλειού αναγνωρίστηκαν, με αποτέλεσμα το 1812 να υπάρχουν 11.000 σε χρήση στη Γαλλία, κάνοντάς τον να εξαπλωθεί στην Αγγλία κατά το 1820 και από κει σχεδόν σε όλο τον κόσμο.

(https://translate.google.gr/translate?hl=el&sl=en&u=http://www.britannica.com/biography/Joseph-Marie-Jacquard&prev=search)

Σύμφωνα όμως, με το 1^{ο} Γενικό Λύκειο Σταυρούπολής και την ερευνητικής τους εργασία με θέμα Διαδίκτυο και Ανθρώπινες σχέσεις, η εγκληματικότητα μέσω ηλεκτρονικών υπολογιστών κάνει την εμφάνισή της ως νέο ποινικό φαινόμενο στα μέσα του 1970. Γρήγορα συνειδητοποιείται από τους νομικούς κύκλους ότι οι υπάρχοντες νομικοί κανόνες δεν είναι δυνατό να καλύψουν εννοιολογικά τις νέες

αυτές μορφές εγκληματικής συμπεριφοράς, διότι παρουσιάζουν τόσο ιδιαίτερα χαρακτηριστικά που δεν μπορούν να αντιμετωπισθούν με τους ήδη θεσπισμένους κανόνες δικαίου.

(http://diadiktiosxeseis.blogspot.gr/p/blog-page_7135.html)

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, όπου υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα, όπως αδικήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών (computer data and systems), αδικήματα σχετιζόμενα με υπολογιστές, αδικήματα σχετιζόμενα με το περιεχόμενο και αδικήματα σχετιζόμενα με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων.

(http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414)

Τα βασικά χαρακτηριστικά της εγκληματικότητας του διαδικτύου, όπως η έλλειψη φυσικής επαφής με το δράστη, η έλλειψη βίας (φυσικά όμως υπάρχουν και περιπτώσεις με βίαιες συμπεριφορές) και η διεθνή φύση της, τονίζουν τη διαφορετικότητά της από την κοινή συμβατική εγκληματικότητα. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον υπολογιστών, χωρίς να υπάρχει σύνδεση με το διαδίκτυο ή αν υπάρχει δε χρησιμοποιείται και άλλα διαπράττονται αποκλειστικά στον κυβερνοχώρο. Σύμφωνα μάλιστα με τη Μήτρου το ηλεκτρονικό έγκλημα προηγείται χρονικά και λογικά της κατηγορίας των κυβερνοεγκλημάτων.

Η διεθνή τους φύση και οι διαφορετικότητά των ηλεκτρονικών εγκλημάτων από τα παραδοσιακά εγκλήματα, καθιστά την εξιχνίασή τους πιο περίπλοκη καθώς οι ηλεκτρονικοί υπολογιστές πλέον λειτουργούν όλο και συχνότερα σε δίκτυα. Η αλληλεπίδραση που υπάρχει μεταξύ των υπολογιστικών συστημάτων αυξάνεται όπως

και οι ανταλλαγές πληροφοριών και αρχείων ανάμεσά τους και το πιο σημαντικό η τεχνολογία αναπτύσσεται ταχύτατα.

Το ηλεκτρονικό έγκλημα μπορεί να θεωρηθεί πιο σοβαρό από τα συμβατικά εγκλήματα διότι διαπράττεται από μακρινή απόσταση κι ο εντοπισμός του δράστη είναι τεχνολογικά περίπλοκος κι απαιτεί άριστες ηλεκτρονικές γνώσεις, οι εγκληματίες δεν έχουν φυσική παρουσία στον τόπο του εγκλήματος και αποδίδει πολύ μεγάλα κέρδη με μικρό ρίσκο για το δράστη.

1.2 Κυβερνοχώρος και παραβατική συμπεριφορά

«Η εγκληματικότητα μέσω υπολογιστών αφορά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και μεταφορά στοιχείων.»

(Ο.Ο.Σ.Α.)

«Ο κόσμος δεν διοικείται από όπλα πια, ή από ενέργεια, ή από χρήματα, διοικείται από μονάδες και μηδενικά. – από μικρά κομμάτια δεδομένων. – είναι όλα ηλεκτρονικά… Υπάρχει ένας πόλεμος εκεί έξω, ένας παγκόσμιος πόλεμος. Δεν είναι σχετικά με το ποιος έχει τις περισσότερες σφαίρες. Είναι σχετικά με το ποιος ελέγχει τις πληροφορίες – αυτό που βλέπουμε και ακούμε, πως δουλεύουμε, πως σκεφτόμαστε. Είναι όλα σχετικά με τις πληροφορίες…»

(Γραμμές από το χαρακτήρα "Cosmos" στην ταινία "Sneakers", MCA / Universal Pictures, 1992)

Κυβερνοχώρος. Τί είναι ο κυβερνοχώρος; Η αγγλική λέξη cyberspace πρώτη φορά χρησιμοποιήθηκε από τον William Gibson στο "Burning Chrome" και μεταφράστηκε στα ελληνικά (κατά λέξη) Κυβερνο-διάστημα. Η λέξη διάστημα όμως προκαλούσε συνειρμούς όπως πλανήτες, αστέρια κ.λπ. και γι' αυτό αντικαταστάθηκε από την πιο γενική λέξη "χώρος". Κυβερνοχώρος λοιπόν είναι ο χώρος που δημιουργείται χάρη στην επιστήμη της Κυβερνητικής (της επικοινωνίας μεταξύ μηχανικών και ηλεκτρονικών συσκευών), ο οποίος στερείται διαστάσεων, καθορισμένων ορίων και αμετακίνητων σημείων προσανατολισμού και έχει σαν σημείο αναφοράς του τον άνθρωπο και τις πράξεις του. Μπορούμε λοιπόν να πούμε πως ο κυβερνοχώρος είναι το σύνολο των ανθρώπινων πράξεων, αποτυπωμένων σε μαγνητικό υλικό.

Ο κυβερνοχώρος είναι κάτι απρόσμενο που συναντά την ανθρωπότητα, κάτι καινούριο που μας ξενίζει κι όπως καθετί διαφορετικό, σαν μια νέα τεχνολογία, μια

νέα περιοχή, κάτι πρωτοποριακό κ.λπ., μέχρι να το επεξεργαστούμε, να το δεχθούμε και να το ενσωματώσουμε στην καθημερινότητά μας, το σαμποτάρουμε, το θεωρούμε απρόσωπο και μας κάνει να νιώθουμε άβολα.

(http://www.eeei.gr/interbiz/articles/cybspace.htm)

Από το 1990, όμως, που δημιουργήθηκε ο παγκόσμιος ιστός έως και σήμερα, ο κυβερνοχώρος έχει μετεξελιχθεί σε μέσω επικοινωνίας και πεδίο ανάπτυξης οποιασδήποτε δραστηριότητας συμπεριλαμβανομένης και της παραβατικής συμπεριφοράς, με τους ανηλίκους να κατέχουν την πρώτη θέση.

Παρατηρείται υψηλός βαθμός εξάρτησης της κοινωνίας, της διοίκησης και της οικονομίας από την αξιοπιστία, την ασφάλεια και την αποτελεσματικότητα των δικτύων, των διάφορων πληροφοριών και των πληροφοριακών συστημάτων.

Μέσω του ηλεκτρονικού υπολογιστή ανταλλάσσουμε μηνύματα, μπαίνουμε σε διάφορες ιστοσελίδες, τοποθετούμε αρχεία στο ιντερνέτ ή στο σκληρό μας δίσκο και εδώ διακρίνουμε την ορατή πλευρά του κυβερνοχώρου, που συνιστά την αποτύπωση σε ηλεκτρονική μορφή των σκέψεων, των απόψεων που αποστέλλουμε μέσω μηνυμάτων, ή αναρτούμε σε αρχεία που έχουν πρόσβαση κι άλλοι χρήστες, καθώς και ημερολόγια που χρησιμοποιούνται από εμάς τους ίδιους.

Ο κυβερνοχώρο προσφέρει ανωνυμία, μέσω της οποίας αναδεικνύονται πάσης φύσεως εγκληματικών πράξεων. Εκ πρώτης όψεως θεωρούμε πως είναι αδύνατη η ανεύρεση - ανίχνευση των πράξεων μας ή των στοιχείων μας, με μια δεύτερη σκέψη όμως, μπορούμε εύλογα να καταλάβουμε πως μέρος του κυβερνοχώρου είναι και τα αποτυπώματα που αφήνουν οι πράξεις μας σε αυτόν. Κάθε κίνησή μας καταγράφεται σε βάσεις δεδομένων που κανείς μας δεν ξέρει πως και από ποιον μπορούν να χρησιμοποιηθούν. Ο κυβερνοχώρος αλλάζει άπειρες μορφές, συνεχώς έκταση, βάθος και υφή.

Όλο και περισσότεροι άνθρωποι “αποικίζουν” στον παγκόσμιο κυβερνοχώρο, συνδέοντας τους υπολογιστές τους με χιλιάδες άλλους. Γίνονται μέλη μιας ψηφιακής κοινωνίας που όπως σε κάθε κοινωνία, οι πράξεις, οι παραλήψεις και οι παραβατικές συμπεριφορές επηρεάζουν και τους γύρω τους.

Κάθε παραβατική συμπεριφορά αποτελεί κι ένα έγκλημα, το οποίο για να στοιχειοθετηθεί πρέπει να υπάρχουν, η περιγραφή της πράξης ή της παράλειψης που συνιστά την ποινικά κολάσιμη συμπεριφορά, ο χρόνος τέλεσης ή παράλειψης, ο τόπος τέλεσης και τα πρόσωπα που εμπλέκονται σε αυτήν, ώστε να προσδιοριστεί ο παραβάτης και το θύμα.

(www.icsd.aegean.gr/website_files/proptyxiako/452470770.ppt)

1.3 Μορφές Κυβερνοεγκλήματος

«Το ηλεκτρονικό έγκλημα αναφέρεται σε κάθε έγκλημα που περιλαμβάνει υπολογιστές και υπολογιστικά δίκτυα»

Eoghan Casey (ψηφιακός εγκληματολόγος, ερευνητής και συγγραφέας)

Τα εγκλήματα που τελούνται στον κυβερνοχώρο κατά καιρούς έχουν κατηγοριοποιηθεί από διάφορους συγγραφείς, μεταξύ των οποίων όμως δεν παρατηρείται απόλυτη ομοιότητα απόψεων.

Ο David L. Carter, Ph. D. σε άρθρο που δημοσιεύθηκε τον Ιούλιο του 1995 στο FBI Magazine διακρίνει τα εγκλήματα σε τέσσερις γενικούς τύπους:

1. **Υπολογιστής ως στόχος:** Εγκλήματα τα οποία περιλαμβάνουν κλοπή πνευματικής ιδιοκτησίας, κλοπή πληροφοριών μάρκετινγκ ή εκβιασμό με βάση τις πληροφορίες που έχουν αποκτηθεί από μηχανογραφημένα αρχεία, σαμποτάζ λειτουργικών συστημάτων και προγραμμάτων με σκοπό τη διάλυση ή δημιουργία χαωδών καταστάσεων σε επιχειρηματικές δραστηριότητες. Εν ολίγοις, όταν μια μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή προκαλεί βλάβη σε αρχεία ή προγράμματα, όχι τόσο για το κέρδος αλλά για την πρόκληση ή την εξερεύνηση του υπολογιστή θεωρείτε τεχνο-βανδαλισμός ή τεχνο-καταπάτηση.

Ένα από τα καλύτερα παραδείγματα της εγκληματικότητας στην οποία ο υπολογιστής είναι ο στόχος μπορεί να βρεθεί στο βιβλίο “The Cuckoo’s Egg” του Cliff Stoll. Το βιβλίο αφηγείται την αληθινή ιστορία ενός χάκερ από το Ανόβερο της Γερμανίας, ο οποίος διείσδυσε σε έναν μεγάλο αριθμό υπολογιστών στις Ηνωμένες Πολιτείες, συμπεριλαμβανομένων των πανεπιστημίων, του στρατού και της κυβέρνησης. Ο χάκερ προσπάθησε να εντοπίσει και να κλέψει την εθνική ασφάλεια των πληροφοριών, προκειμένου να τα πουλήσει σε ξένες κυβερνήσεις.

2. **Υπολογιστής ως όργανο του εγκλήματος:** Οι διαδικασίες ενός υπολογιστή και όχι τα περιεχόμενα του υπολογιστή, συμβάλλουν στο έγκλημα. Οι κυβερνοπειρατές (hackers) εισάγουν νέους κωδικούς (οδηγίες προγραμματισμού) για να χειραγωγήσουν αναλυτικά τις διαδικασίες του υπολογιστή ώστε να διευκολύνουν

το έγκλημα. Σε αυτήν την κατηγορία ανήκουν απάτες με ηλεκτρονικές μεταφορές χρημάτων και συναλλαγές όπως μεταβιβάσεις μετοχών, πωλήσεις ή τιμολογήσεις, απάτες που έχουν σχέση με την ηλεκτρονική ανταλλαγή δεδομένων και το ηλεκτρονικό εμπόριο, απάτες αυτόματων ταμειολογιστικών μηχανών (Α.Τ.Μ.), απάτες πιστωτικών καρτών και απάτες τηλεπικοινωνιών.

3. Υπολογιστής ως «συνεργός / πλατφόρμα» σε άλλα εγκλήματα: Σε αυτήν την κατηγορία ο υπολογιστής δεν είναι απαραίτητος για να συμβεί το έγκλημα, αλλά συμβάλλει στην εγκληματική πράξη. Η μηχανοργάνωση βοηθά το έγκλημα να συμβεί γρηγορότερα, επιτρέποντας την επεξεργασία μεγαλύτερων όγκων πληροφοριών, κάνοντας πιο δύσκολο τον εντοπισμό των ιχνών του ηλεκτρονικού παραβάτη. Τέτοια εγκλήματα είναι το ξέπλυμα μαύρου χρήματος, οι παράνομες τραπεζικές συναλλαγές, ο τζόγος και τα παράνομα στοιχήματα, η διάδοση ναρκωτικών, η πορνογραφία και ιδιαίτερα η παιδική και ενδεχομένως μια διάπραξη φόνου, αλλάζοντας τη φαρμακευτική αγωγή ασθενούς ή τη δοσολογία σε υπολογιστή νοσοκομείου.

Χαρακτηριστικό παράδειγμα τέτοιου εγκλήματος αναφέρει ο Μανώλης Σφακιανάκης (επικεφαλής της δίωξης ηλεκτρονικού εγκλήματος) σε συνέντευξή του στις 12/1/2013 στο Έθνος και στη Μαρία Ψαρά λέγοντας χαρακτηριστικά «Ιδιωτικός χώρος στο ιντερνέτ δεν υπάρχει» και συμπληρώνει «Πριν λίγα χρόνια, σε χώρα του εξωτερικού, η Αστυνομία αντιμετώπισε δολοφονία ενός ασθενούς που λόγω σακχαρώδους διαβήτη νοσηλευόταν σε νοσοκομείο της χώρας. Ύστερα από εντατικές έρευνες, εμβρόντητοι οι αστυνομικοί διαπίστωσαν πως ένας ανταγωνιστής του ασθενούς, είχε πληρώσει χάκερ για να μπει στη βάση δεδομένων του νοσοκομείου και να αλλάξει τα φάρμακα του άτυχου άνδρα. Ήταν η πρώτη δολοφονία μέσω διαδικτύου, που συγκλόνισε την παγκόσμια κοινή γνώμη. Το παραδοσιακό έγκλημα μετακομίζει στο διαδίκτυο.»

(http://cert.auth.gr/index.php/el/mnu-announce/101-interview-sfakianakis)

4. Εγκλήματα σχετικά με την επικράτηση / εξάπλωση των υπολογιστών: Η τεχνολογική ανάπτυξη δημιουργεί νέους στόχους εγκλήματος παραβίασης πνευματικών δικαιωμάτων του εμπορικού λογισμικού, όπως πειρατεία λογισμικού / παραποίηση, παραβίαση πνευματικής ιδιοκτησίας των προγραμμάτων ηλεκτρονικών υπολογιστών, πλαστούς εξοπλισμούς ηλεκτρονικών υπολογιστών και προγραμμάτων της μαύρης αγοράς.

(https://translate.google.gr/translate?hl=el&sl=en&u=http://www.lectlaw.com/files/cri14.htm&prev=search)

Από την άλλη πλευρά ο Ιωάννης Αγγελής (όπως αναφέρεται από τη Λίλιαν Μήτρου, Ηλεκτρονικό και Διαδικτυακό Έγκλημα, Το Ποινικό Δίκαιο της Πληροφορικής, χωρίς χρονολογία) προτείνει την ακόλουθη διάκριση των εγκλημάτων:

- **Εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο:** Τέτοια εγκλήματα είναι η συκοφαντική δυσφήμηση με τη χρήση του ηλεκτρονικού ταχυδρομείου (e-mail), η αντιγραφή πνευματικού έργου ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Πρόκειται για εγκλήματα σχετιζόμενα με τον κυβερνοχώρο ή εγκλήματα που διαπράττονται με τη βοήθεια του κυβερνοχώρου (internet related crime).
- **Εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενίοτε χωρίς τη χρήση του διαδικτύου):** Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παράγραφος 1 του Ποινικού Κώδικα, όπως η παράνομη αντιγραφή δισκέτας ή DVD-Rom ή CD-Rom σε ηλεκτρονικό υπολογιστή.
- **«Γνήσια εγκλήματα κυβερνοχώρου» (cyber crimes):** Εγκλήματα δηλαδή που τελούνται αποκλειστικά στον κυβερνοχώρο (με τη χρήση του διαδικτύου). Τέτοιες αξιόποινες συμπεριφορές είναι η μη εξουσιοδοτημένη μεταβίβαση κρυπτογραφημένων κειμένων και η διάδοση παιδικού πορνογραφικού υλικού.

Στο ίδιο βιβλίο, όμως, η Λίλιαν Μήτρου κατηγοριοποιεί τα ηλεκτρονικά εγκλήματα σε τρεις κατηγορίες:

1. **Προσβολές ιδιωτικότητας:** Συναντώνται συνήθως στα επαγγελματικά απόρρητα όπως το ιατρικό, το δικηγορικό και το τραπεζικό.
2. **Αδικήματα κατά της περιουσίας:**
   - **Computer hacking:** Η προσβολή πληροφοριακών συστημάτων που δεν πραγματοποιείται με σκοπό τη χειραγώγηση, το σαμποτάζ ή την κατασκοπεία αλλά χάριν της ευχαρίστησης της προσβολής των τεχνικών συστημάτων ασφαλείας.

- **Ηλεκτρονική κατασκοπεία:** Η παράνομη αυτή δραστηριότητα διευκολύνει ιδιαίτερα τη σύγκλιση των τεχνολογιών πληροφορικής και τηλεπικοινωνιών.
- **Πειρατεία προϊόντων πνευματικής ιδιοκτησίας**
- **Σαμποτάζ και εκβίαση:** Διακρίνουμε διαφορά μεταξύ των φυσικών ζημιών και των ζημιών στο σύστημα. Υπάρχουν προγράμματα, οι λεγόμενοι ιοί και σκουλήκια, κακόβουλα δηλαδή λογισμικά, που δημιουργούν προβλήματα και καταστρέφουν δεδομένα.
- **Ηλεκτρονική απάτη:** Αφορούν διαχείριση παραστατικών όπως πληρωμή λογαριασμών, μισθών και κίνηση λογαριασμών τραπέζης.

3. **Παράνομο και αθέμιτο / επιβλαβές περιεχόμενο:** Στις μέρες μας το παράνομο υλικό εστιάζεται στην παιδική πορνογραφία, με τη δίωξη των εγκληματιών να είναι εξαιρετικά δύσκολη καθώς πολύ παραβάτες δρουν από το εξωτερικό και επίσης κρύβονται πίσω από την ανωνυμία και την τεχνική κάλυψη που εξασφαλίζουν συστήματα όπως οι anonymous remailers. (www.icsd.aegean.gr/website_files/proptyxiako/714097945.doc)

Αντιθέτως ο Χρ. Ε. Τσουραμάνης χωρίζει τα ηλεκτρονικά εγκλήματα με κριτήριο τα μέσα τέλεσης και εξιχνίασής τους σε δυο κατηγορίες:

1. Τα **γνήσια** ψηφιακά εγκλήματα που τελούνται και εξιχνιάζονται, με τη χρήση της ψηφιακής τεχνολογία:
   - **Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking):** Η συγκεκριμένη εγκληματική συμπεριφορά αφορά απλά και μόνο την παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών που τελείται με την παραβίαση των μέτρων ασφαλείας από το δράστη.
   - **Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ:** Αποκτώντας πρόσβαση σε ένα δίκτυο ο ψηφιακός εγκληματίας έχει την ευχέρεια να κλέψει, να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων και γενικά να κάνει οποιαδήποτε άλλη ενέργεια θα τα αχρηστεύσει μόνιμα ή προσωρινά, επιφέροντας ανυπολόγιστες οικονομικές ζημίες στα θύματά του.
   - **Η κλοπή ταυτότητας (identity theft)**
   - **Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης «επίθεσης άρνησης παροχής**

υπηρεσιών» (denial of service attack – Dos): Η πιο συνηθισμένη μορφή είναι εκείνη που ο Παγκόσμιος Ιστός κατακλύζεται με πολυάριθμες αιτήσεις σύνδεσης, οι οποίες δεν είναι δυνατό να ικανοποιηθούν. Αυτό τον υποχρεώνει να ασχολείται τόσο πολύ με το να προσπαθεί να απαντήσει στις συγκεκριμένες αιτήσεις έτσι ώστε να αγνοεί άλλες καλοπροαίρετες αιτήσεις σύνδεσης.

- **Η διασπορά κακόβουλων προγραμμάτων όπως:** ιών (viruses), σκουληκιών (worms), Δούρειων ίππων (Trojan horses), κατασκοπευτικού λογισμικού (spyware), διαφημιστικού λογισμικού (adware), προγραμμάτων καταγραφής πληκτρολόγησης (Keystroke loggers), παραπλανητικών προγραμμάτων κλήσεων (dialers), προγραμμάτων μετατροπής σε υπολογιστές "ζόμπι", rootkit
- **Η πειρατεία λογισμικού,** δηλαδή, προγραμμάτων Η/Υ, που αφορά την παράνομη αντιγραφή τους και στη συνέχεια τη διάθεσή τους στην αγορά – κυρίως μέσω του Διαδικτύου – σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου:

2. Τα **παραδοσιακά** εγκλήματα που τελούνται και εξιχνιάζονται, με τη βοήθεια της ψηφιακής τεχνολογίας αλλά και χωρίς αυτήν:

- Διάφορα **κοινά** εγκλήματα όπως: κλοπή ενός Η/Υ ή τμημάτων του, εγκλήματα που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου (e-mail) ή ιστοσελίδων κοινωνικής δικτύωσης (websites of social networking) ή των δωματίων ανοικτής επικοινωνίας (chat-rooms) π.χ. απάτες, εξυβρίσεις, εκβιασμοί, δυσφημίσεις, πωλήσεις απαγορευμένων προϊόντων (ναρκωτικών, μη εγκεκριμένων φαρμάκων), παροχή υπηρεσιών call- girls, η κυκλοφορία πορνογραφικού υλικού (κυρίως παιδικού), η αποπλάνηση ανηλίκων (grooming) και η παρενόχληση χρηστών με ανεπιθύμητα διαφημιστικά μηνύματα (spamming). Επίσης, οι προσβολές της πνευματικής ιδιοκτησίας, οι ανταλλαγές πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου μεταξύ τρομοκρατικών οργανώσεων αλλά και συμμοριών του κοινού ποινικού δικαίου και το ηλεκτρονικό ξέπλυμα μαύρου χρήματος.
- **Η κατασκοπεία** είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική.

- **Οι υποκλοπές** τηλεφωνικών συνομιλιών που έχουν σα συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

Σύμφωνα με τα αποτελέσματα έρευνα που διεξήγαγε η McConnell International σε πενήντα δύο χώρες, με τίτλο «Cyber Crime… and Punishment?» κατατάσσει τα κυβερνοεγκλήματα σε δέκα κατηγορίες:

1) Παρεμπόδιση (κυβερνο) κυκλοφορίας
2) Τροποποίηση δεδομένων
3) Κλοπή δεδομένων
4) Εισβολή σε δίκτυο
5) Σαμποτάζ δικτύου
6) Μη εξουσιοδοτημένη πρόσβαση
7) Διασπορά ιών
8) Υπόθαλψη αδικημάτων
9) Πλαστογραφία
10) Απάτη

Οι κύριες μορφές κυβερνοεγκλήματος που έχει κληθεί το ελληνικό Τμήμα Ηλεκτρονικού Εγκλήματος / ΔΑΑ να εξιχνιάσει είναι οι ακόλουθες:

- ✓ Απάτες μέσω διαδικτύου
- ✓ Παιδική πορνογραφία
- ✓ Cracking και Hacking
- ✓ Διακίνηση – πειρατεία λογισμικού
- ✓ Πιστωτικές κάρτες
- ✓ Διακίνηση ναρκωτικών
- ✓ Έγκλημα στα chat rooms

Εν κατακλείδι, μπορεί να μην ταυτίζονται απολύτως όλες οι γνώμες, αλλά μπορούμε να συμφωνήσουμε ότι όλες οι απόψεις που προαναφέρθηκαν μας οδηγούν συμπερασματικά να κατατάξουμε τα ηλεκτρονικά εγκλήματα σε δυο μεγάλες κατηγορίες:

→ Στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, με τη χρήση του διαδικτύου ή και χωρίς αυτήν και

→ Στα εγκλήματα που διαπράττονται εναντίον ηλεκτρονικών υπολογιστών και των εξαρτημάτων τους.

1.4 Ηλεκτρονικοί εγκληματίες (Hackers - Crackers)

«Η τεχνολογική υποδομή μαζί με τη νομοθεσία είναι απολύτως αναγκαίες για τη σωστή τεκμηρίωση των εξιχνιασθέντων υποθέσεων που αφορούν ηλεκτρονικά εγκλήματα. Στην περίπτωση που θα υπάρχει τεχνολογική υποδομή χωρίς την κατάλληλη νομοθεσία, μέσα από την οποία θα οριοθετούνται οι εγκληματικές συμπεριφορές, τότε θα έχουμε πρόβλημα ως προς την απονομή δικαιοσύνης. Σύμφωνα με έρευνα μέσω των πληροφοριακών δικτύων (κυρίως του διαδικτύου) και με τη χρήση των συστημάτων ηλεκτρονικής μεταφοράς οικονομικών μεγεθών (electronic fundstransfer system ή EFTC) διακινούνται καθημερινά πάνω από 2 τρισεκατομμύρια δολάρια μόνο στις ΗΠΑ σε 700.000 συναλλαγές, ενώ στον κόσμο η εκτίμηση ανεβάζει το ποσό στα 5 τρισεκατομμύρια. Κατά μέσο όρο λοιπόν, στον κόσμο διακινούνται ηλεκτρονικά πάνω από 3,5 δισεκατομμύρια δολάρια το λεπτό. Αυτά τα ποσά εποφθαλμιούν οι κράκερς, οι οποίοι διαθέτουν τις γνώσεις για να τολμήσουν να επιτεθούν και ίσως να σπάσουν τους κωδικούς προστασίας των συστημάτων, αποκτώντας πρόσβαση σε αυτά τα ποσά».

(Αστυνόμος Α’ κ. Εμμανουήλ Σφακιανάκης, Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος / ΔΑΑ)

Τα ηλεκτρονικά εγκλήματα ανεξαρτήτως κατηγορίας, τόπου και χρόνου για να υφίστανται πρέπει κάποιος να τα διαπράξει. Και σε αυτή την περίπτωση οι γνώμες διίστανται ανάμεσα σε δυο κατηγορίες ηλεκτρονικών παραβατών, στους hackers και τους crackers.

Η ιστορία των ηλεκτρονικών παραβατών ξεκινάει περίπου το 1960 από σπουδαστές του Τεχνολογικού Ινστιτούτου Μασαχουσέτης (MIT – Massachusetts Institute of Technology), οι οποίοι χρησιμοποιούσαν κεντρικούς υπολογιστές (mainframes), κλειδωμένους σε ένα δωμάτιο με ελεγχόμενη θερμοκρασία, γεγονός που τους περιόριζε σε θέμα χρόνου εργασίας. Τότε κάποιοι δημιούργησαν τα πρώτα

hacks, προγράμματα δηλαδή που βοηθούσαν στη γρηγορότερη εκτέλεση υπολογισμών, πολλές φορές βέβαια τα hacks ήταν καλύτερα από το αρχικό πρόγραμμα. Μάλιστα, το 1969, δυο υπάλληλοι της Bell συνέθεσαν ένα hack, με την ονομασία UNIX, το οποίο είχε εντολές με σκοπό την αύξηση της ταχύτητας των υπολογιστών και στις μέρες μας αποτελεί ένα ευρέως γνωστό λειτουργικό σύστημα.

Ηλεκτρονικός παραβάτης (hacker) ονομάζεται το άτομο που έχει την ικανότητα να εισβάλει σε υπολογιστικά συστήματα, είτε για διασκέδαση, είτε για πειραματισμό, είτε για υποκλοπή εγγράφων, πληροφοριών καθώς και άλλων κακόβουλών πράξεων. Ένας παραβάτης διαθέτει άριστες γνώσεις διαχείρισης υπολογιστικών συστημάτων και συνήθως είναι προγραμματιστές, σχεδιαστές συστημάτων ή άτομα τα οποία δεν ασχολούνται επαγγελματικά με τους τομείς της πληροφορικής, αλλά διαθέτουν τέτοιες δεξιότητες ώστε να δουλεύουν σε ομάδες (hacking groups), είτε μόνοι τους.

Στα άτομα τα οποία εισέρχονται παράνομα σε συστήματα με σκοπό την καταστροφή, την τροποποίηση ή την κλοπή δεδομένων ή πληροφοριών έχει προσδοθεί το όνομα κράκερς (crackers). Την ονομασία αυτή θέλησαν να δώσουν οι ίδιοι οι χάκερς προκειμένου να τονίσουν την ορθή δράση τους στο χώρο του διαδικτύου και να διαχωρίσουν τη φύση τους από τα άτομα τα οποία δρουν παραβατικά. Η βασική διαφορά ανάμεσα στους hacker και στους cracker, έγκειται στο πώς χρησιμοποιεί ο καθένας τις γνώσεις του, είτε δηλαδή με σκοπό να μάθει, είτε με σκοπό να προκαλέσει ζημιά.

Ένας άλλος διαχωρισμός χρησιμοποιεί τους εξής όρους:

- **Χάκερ με μαύρο καπέλο (black hat hackers):** Είναι τα άτομα που αποκτούν πρόσβαση σε συστήματα χωρίς να τους παρέχετε άδεια, ενώ συχνά έχουν επιβλαβή δράση.
- **Χάκερ με άσπρο καπέλο (white hat hackers):** Είναι εκείνοι που εισβάλουν σε ένα σύστημα με σκοπό να αναγνωρίσουν τα τρωτά τους σημεία και να προτείνουν λύσεις. Γενικότερα η δράση τους κινείται στα πλαίσια των ηθικών αρχών.

- **Χάκερ με γκρίζο καπέλο (grey hat hackers):** Βρίσκονται στο μέσο των δυο άλλων κατηγοριών. Σε αυτήν την κατηγορία κατατάσσονται τα άτομα όπου η δράση τους δεν μπορεί να διευκρινιστεί ή τα άτομα που έχουν την τάση να αλλάζουν.

Αργότερα αποδόθηκαν τέσσερις γενιές των χάκερ:

- **Πρώτη γενιά:** Ταλαντούχοι φοιτητές, προγραμματιστές και επιστήμονες με ενδιαφέροντα σε πληροφοριακά θέματα, δημιούργησαν προγράμματα που θα ταίριαζαν με την καθημερινότητά τους.
- **Δεύτερη γενιά:** Εξέλιξη της πρώτης, συναντάμε επίσης μια πρώτη ηλεκτρονική εγκληματικότητα μέσω οικιακών υπολογιστών.
- **Τρίτη γενιά:** Δημιουργία ηλεκτρονικών παιχνιδιών (videogames) ή παράνομων αντιγράφων ηλεκτρονικών παιχνιδιών και παραβίασης κωδικών προστασίας τους με σκοπό την ψυχαγωγία μέσω των προσωπικών ηλεκτρονικών υπολογιστών.
- **Τέταρτη γενιά:** Οι χάκερ στις μέρες μας, οι οποίοι έχουν χαρακτηριστικό την εγκληματική συμπεριφορά. (https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81#cite_note-1)

Με την παρουσίαση των όρων και των γενεών των χάκερ καταφέραμε να ορίσουμε με σαφήνεια και να κατανοήσουμε τις διαφορές στη δράση τους στον κυβερνοχώρο. Για να γίνει όμως ένας ξεκάθαρος διαχωρισμός τους από τους κράκερ, ένας διαχωρισμός μεταξύ ηθικού και μη, άσπρου και μαύρου κρίνεται αναγκαία η παράθεση μερικών ακόμα ονομάτων που έχουν αποδοθεί στα άτομα της κοινότητας των χάκερ:

- ✓ **Κυβερνοπολεμιστές:** Συνήθως αφορά στρατιωτικά θέματα διότι εισβάλουν σε ένα σύστημα με το οποίο γίνονται επείγουσες υπηρεσίες, επικοινωνίες ή μεταφορές και κατατάσσονται στους χάκερ με άσπρο καπέλο.
- ✓ **Κυβερνοτρομοκράτες:** Σκοπός τους είναι να βλάψουν συστήματα ή δεδομένα πολιτικού ή κοινωνικού περιεχομένου με συνηθέστερο στόχο π.χ. μια κυβέρνηση.

- ✓ **Χακτιβιστές (hacktivists):** Υποστηρίζουν τα αιτήματα των ακτιβιστών μέσω παραποίησης ιστοσελίδων.
- ✓ **Δημιουργοί επιβλαβών συστημάτων:** Δημιουργούν ιούς (virus), Δούρειους Ίππους (Trojan Horses), σκουλήκια (warms) και άλλα επιβλαβή προγράμματα τα οποία θα αναλύσουμε στη συνέχεια. Γενικότερα είναι μια μη αποδεκτή κατηγορία χάκερ.
- ✓ **Φρίκερ:** Ειδικεύονται στην παραβίαση τηλεφωνικών δικτύων είτε με σκοπό την εξερεύνηση του δικτύου, είτε με σκοπό την πραγματοποίηση δωρεάν τηλεφωνικών κλήσεων.
- ✓ **Σαμουράι (Sneakers):** Προσλαμβάνονται για να διεξάγουν νόμιμες δραστηριότητες σχετικές με υπολογιστικά συστήματα και κατατάσσονται στους χάκερ με άσπρο καπέλο.
- ✓ **Κλέφτες προγραμμάτων (Code Kiddies):** Χρησιμοποιούν έτοιμα γραμμένα προγράμματα από άλλους πιο έμπειρους χάκερ. Οι ίδιοι δε διαθέτουν ιδιαίτερες γνώσεις χάκινγκ, έχουν συνήθως την τάση να προκαλούν φθορές ενώ δεν είναι δημοφιλείς στην κοινότητα των χάκερ.
- ✓ **Πειρατές συστημάτων (Wares Dudes):** Αντιγράφουν και παραβιάζουν προγράμματα τα οποία προστατεύονται από τους νόμους πνευματικής ιδιοκτησίας.

→ Εκτός από τις ομάδες Κυβερνοπολεμιστές και Σαμουράι οι υπόλοιπες χαρακτηρίζονται «χάκερ με μαύρο καπέλο».

Άσχετα από όλους τους χαρακτηρισμούς και τις ονομασίες που έχουν αποδοθεί στου ηλεκτρονικούς εγκληματίες έχει παρατηρηθεί ότι οι ίδιοι επιλέγουν διαφορετικά ονόματα από τα πραγματικά, τα λεγόμενα ψευδώνυμα (nicknames), τα οποία δεν παραπέμπουν σε φυσικά πρόσωπα, γεγονός που είναι χρήσιμο σε άτομα τα οποία σκοπεύουν να εμπλακούν σε παράνομες δραστηριότητες. Αυτό το νέο τους όνομα, θεωρούν πως είναι ένας άλλος χαρακτήρας, τον οποίο έχουν αναπτύξει ως το άλλο τους εγώ (alter ego) στον κυβερνοχώρο χωρίς όμως να μοιάζει με την πραγματικότητα, φερ ειπείν ένας χάκερ με τον τίτλο «Mafia boy» έκρυβε έναν δεκαπεντάχρονο μαθητή που φυσικά δεν είχε καμία σχέση με τη μαφία.

Μπορούμε να πούμε με βεβαιότητα πως πολλοί από τους χάκερ, αν όχι όλοι, αισθάνονται ανεπαρκής στον αληθινό κόσμο, με αποτέλεσμα να οδηγούνται

στη εύρεση ενός τίτλου που θα αντιπροσωπεύει τον τρόπο με τον οποίο θα ήθελε να γίνεται αντιληπτός από τους άλλους. Έχει παρατηρηθεί επίσης η αίσθηση του χιούμορ που έχουν κάποιοι χάκερ χωρίς να θέλουν να κάνουν επίδειξη δύναμης, για παράδειγμα όταν ρωτήθηκε ένα μέλος της κοινότητας των χάκερ Cult of the Dead Cow (cDc) γιατί επέλεξε το όνομα «Tweety Fish», ο ίδιος απάντησε:

«Ήθελα ένα όνομα τόσο γελοίο ώστε, αν ποτέ συλληφθώ, το δικαστήριο να γελούσε με αυτό!»

(βιβλίο: Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, Steven Furnell)

Μέθοδοι Επιθέσεων

Για να καταφέρει ένας ηλεκτρονικός εγκληματίας να μπει στο σύστημα ενός θύματος, πρέπει πρώτα να συγκεντρώσει πληροφορίες σχετικά με το σύστημα που θέλει να προσβάλει, ενώ αποκτά πρόσβαση σε αυτό αναζητώντας τους κωδικούς εισόδου που του δίνουν δικαιώματα νόμιμου χρήστη. Μόλις καταφέρει να εισβάλει στο σύστημα επιδιώκει την εκπλήρωση των στόχων του, την αποχώρηση από αυτό χωρίς να αφήσει ίχνη που θα προδώσουν την ταυτότητά του και τη δυνατότητα επανεισόδου όποτε ο ίδιος το επιθυμεί.

Η επιτυχημένη εισβολή ενός χάκερ σε ένα σύστημα σχετίζεται και με τις μεθόδους επίθεσης (hacking attacks) που χρησιμοποιεί, όπως:

- **Sniffer (Λαγωνικό):** Είναι ένα μικρό πρόγραμμα που εισχωρεί στο σύστημα κρυφά, προκειμένου να ψάξει και να αναλύσει αρχεία, σκοπεύοντας στη συλλογή πληροφοριών και τη διαβίβαση αυτών στο χρήστη του.
- **Denial of Service (DoS attack):** Οι χάκερ βομβαρδίζουν το δίκτυο με πολλαπλά προγράμματα τα οποία τρέχουν με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών, με αποτέλεσμα να υπερφορτώσουν το σύστημα ώστε να μη μπορεί να ανταποκριθεί.

- **Distributed Denial of Service (DDoS attack):** Χρησιμοποιούν δούρειους ίππους με σκοπό τον έλεγχο πολλών υπολογιστών ανυποψίαστων χρηστών. Συντονίζουν όλους τους υπολογιστές, σε μια δεδομένη στιγμή, ώστε να απαιτήσουν δεδομένα από ένα σύστημα σκοπεύοντας στην κατάρρευσή του.
- **DNS Spoofing:** Τροποποιούν το Domain Name Code (αριθμητική, δυαδική ψηφιοποιημένη διεύθυνση του site) με σκοπό να παραπέμψουν το χρήστη σε μια ιστοσελίδα, αντίγραφο της αρχικής (mirror site), αποσπώντας προσωπικά δεδομένα τα οποία ο χρήστης νομίζει πως τα δίνει στην αληθινή ιστοσελίδα που αναζήτησε.
- **Δούρειοι Ίπποι:** Ο χάκερ μεταμφιέζει έναν ίππο σε ένα άλλο πρόγραμμα (π.χ. παιχνίδι) έτσι ώστε να ξεγελάσει το χρήστη και να το εγκαταστήσει. Μόλις εγκατασταθεί, δίνει στο χάκερ πρόσβαση στο σκληρό δίσκο ή στο e-mail του χρήστη και εκμεταλλευόμενο τις αδυναμίες των προγραμμάτων δίνει τη δυνατότητα στο χάκερ να αποκτήσει πρόσβαση και σε άλλα συστήματα πραγματοποιώντας επιθέσει DDoS. Για παράδειγμα οι χρήστες εισάγουν τα στοιχεία τους (όνομα χρήστη – κωδικό πρόσβασης) στο σύστημα πιστεύοντας ότι συνδέονται σε αυτό, ενώ στην πραγματικότητα καταγράφονται από τον ίππο προς χρήση του χάκερ.
- **Ιοί – Σκουλήκια (Virus – Warms):** Είναι αυτοαναπαραγόμενα προγράμματα και έχουν τη δυνατότητα να εξαπλωθούν σε όλο το διαδίκτυο χωρίς να απαιτούν τη βοήθεια κανενός άλλου προγράμματος. Συχνά προκαλούν καταστροφή και δυσλειτουργία συστημάτων και αρχείων.

(https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81#cite_note-1)

Κίνητρα

Η πραγματοποίηση ενεργειών από το φυσικό χώρο του ατόμου στον κυβερνοχώρο, μέσω του προσωπικού υπολογιστή του, του δίνει τη δυνατότητα δράσης χωρίς καν να βγει από το σπίτι του. Βάση αυτόν τον παράγοντα, οι χάκερ έχουν την ευκαιρία να κινηθούν και να δράσουν απρόσωπα χωρίς να υπάρχει ο κίνδυνος για φυλετικές, θρησκευτικές, χρωματικές ή σεξουαλικές διακρίσεις, στοιχεία τα οποία δε χρειάζεται να γνωστοποιήσουν όταν είναι συνδεδεμένοι (εκτός κι αν το επιλέξουν οι ίδιοι). Έτσι ο χώρος του δικτύου δίνει το αίσθημα της ελευθερίας στον άνθρωπο, από ότι το καθημερινό τους περιβάλλον, ενώ του εξασφαλίζει την ασφάλεια του «να είναι εκεί χωρίς να είναι» απαλλάσσοντάς τους έτσι από ένα μεγάλο μερίδιο ευθυνών. Έχει παρατηρηθεί επίσης πως τα κίνητρα των χάκερ μπορεί να είναι η περιέργεια, η διασκέδαση και η ικανοποίηση που αντλούν από τα κατορθώματα τους καθώς και η πιθανή αναγνώριση που μπορεί να έχουν μέσα από αυτά, ενώ είναι σημαντικό να αναφερθεί και το γεγονός της πιθανότητας εθισμού ενός ατόμου στο διαδίκτυο («Διαταραχή Εθισμού στο Διαδίκτυο») και στην ανωνυμία.

Τα συνηθέστερα κίνητρα των Cyber Criminals για τη διάπραξη ενός cybercrime είναι:

- Διασκέδαση
- Χρηματικό όφελος
- Θυμό, εκδίκηση
- Πολιτικά κίνητρα
- Σεξουαλικά κίνητρα
- Σοβαρές ψυχικές ασθένειες

Αυτοκριτική και κοινή γνώμη

Για χρόνια, η κοινή γνώμη έχει μια σταθερή εικόνα για τους ηλεκτρονικού εγκληματίες. Θεωρούν πως είναι άτομα, κυρίως μαθητές ή σπουδαστές, οι οποίοι έχουν τάση να προκαλούν χάος από τους προσωπικούς τους υπολογιστές, συνήθως άντρες μεταξύ 15 έως 25 χρονών, χωρίς ιδιαίτερες κοινωνικές δεξιότητες και πιθανότατα αποτυχημένοι σε άλλους τομείς, όπως η εκπαίδευση. Επίσης, πιστεύουν πως είναι άτομα γοητευμένα από την τεχνολογία και χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές σαν μέσο για να είναι σημαντικοί ή δυνατοί. Τις περισσότερες φορές τους αποδίδουν ψυχρά χαρακτηριστικά προσωπικότητας.

Θεωρούνται εγκληματίες και παράνομοι εισβολείς σε συστήματα, οι ίδιοι πιστεύουν πως με το αδιάκοπο ψάξιμο στον κυβερνοχώρο καθώς και με τη συνεχή διαδικασία μάθησης και εξερεύνησης, ανοίγουν νέες πόρτες στο χώρο του διαδικτύου χωρίς όμως να έχουν την πρόθεση να προκαλέσουν κακό. Ο διευθυντής έκδοσης του «2600: the hackers quarterly» Emmanuel Goldstein, αναφέρει χαρακτηριστικά σχετικά με το ζήτημα παράνομης εξερεύνησης συστημάτων:

"Αν κάποιο παιδί, κάπου, μπορεί να αποκτήσει πρόσβαση στα ιατρικά σας αρχεία ή στα τηλεφωνικά σας αρχεία, δεν είναι αυτό που τα έβαλε εκεί. Ο αληθινός παραβάτης της ιδιωτικής σφαίρας σας, είναι το πρόσωπο που πήρε την απόφαση να τα καταστήσει εύκολα προσβάσιμα."

Επίσης, οι ίδιοι γνωστοποιούν το ενδιαφέρον και την έλξη τους προς την τεχνολογία, προς την πολυπλοκότητα των συστημάτων και των δικτύων στα οποία δρουν.

"Ήξερα ότι το τηλεφωνικό δίκτυο φτάνει σε κάθε σπίτι και επιχείρηση στη χώρα και σε κάθε χώρα στον κόσμο… Για εμένα, η τηλεφωνική γραμμή ήταν ο σύνδεσμος με κάτι ωσεί παρόν και εξωτερικό… νομίζω ότι κατά έναν τρόπο, ένα κομμάτι μου ακόμα θεωρεί το δίκτυο ως κάτι μυστικό και μυστηριώδες."

(Kevin Poulsen, καταδικασμένος χάκερ προς τον περιφερειακό δικαστή των ΗΠΑ Manuel Real, βιβλίο: Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, Steven Furnell)

1.5 Ιοί και κακόβουλο λογισμικό

Ένας ιός είναι η πιο αναγνωρισμένη μορφή κακόβουλου προγράμματος υπολογιστή. Μπορεί να οριστεί ως ένα μη αυτόνομο στοιχείο, που έχει τη δυνατότητα να τροποποιεί τα αντίγραφά του, όπως συμβαίνει σε έναν μεταφορικό ιό. Ο ιός αυτός, μπορεί να διαδοθεί από έναν υπολογιστή σε έναν άλλο, μέσω δικτύου ή διαδικτύου ή με τη μεταφορά του σε άλλο μέσο αποθήκευσης (CD, USB flash) ενώ η εξάπλωσή του συνεχίζει όσο αυτά χρησιμοποιούνται και προκαλούν ζημιά είτε καταστρέφοντας προγράμματα, είτε διαγράφοντας αρχεία είτε με τη μορφοποίηση του σκληρού δίσκου. Πολλοί δεν έχουν σα στόχο να προκαλέσουν κάποια ζημιά (απλή γνωστοποίηση της παρουσίας τους με ηχητικά μηνύματα, βίντεο ή κείμενα, κάποιες φορές όμως το πετυχαίνουν άθελά τους καταλαμβάνοντας τη μνήμη που χρησιμοποιούν τα κανονικά προγράμματα, προκαλούν ασταθή συμπεριφορά ή και κατάρρευση του συστήματος (system crash) και συνήθως είναι υπεύθυνοι για την απώλεια δεδομένων. Συνήθως στοχεύουν στην κλοπή προσωπικών δεδομένων του και όχι στην καταστροφή τους ή στην παρενόχληση του χρήστη.

Ο πρώτος ιός που ανιχνεύτηκε ήταν στο ARPANET (Advanced Research Projects Agency Network το πρώτο στον κόσμο δίκτυο μεταγωγής πακέτου και πρόδρομος του παγκόσμιου διαδικτύου) στις αρχές της δεκαετίας του ’70. Διαδόθηκε μέσω του λειτουργικού συστήματος που χρησιμοποιούσε το ARPANET και προσέβαλε όσους υπολογιστές έκαναν σύνδεση στο δίκτυο εμφανίζοντας το εξής μήνυμα: “I’M THE CREEPER! CATCH ME IF YOU CAN”. Λίγο αργότερα όμως εμφανίστηκε ένα πρόγραμμα αγνώστου δημιουργού, το Reaper, το οποίο ανίχνευε τον CREEPER στους υπολογιστές που είχε μολύνει και τον διέγραφε.

Ο πρώτος εξαπλούμενος εκτός συστήματος ιός δημιουργήθηκε από τον δεκαπεντάχρονο Richard Skrenta το 1982 με ονομασία Elk Cloner. Ο ιός δεν είχε προθέσεις να βλάψει και δημιουργήθηκε ως αστείο. Ο Richard αποθήκευσε τον ιό σε μια δισκέτα την οποία την έδωσε σε φίλους και γνωστούς οπότε όταν εκκινούσε ο υπολογιστής από τη δισκέτα ο ιός αντιγραφόταν μόνος του σε όποια άλλη δισκέτα

είχε πρόσβαση ο υπολογιστής. Μετά την πεντηκοστή εκκίνηση του υπολογιστή από τη δισκέτα εμφανιζόταν το εξής μήνυμα υπό μορφή στίχων:

Elk Cloner:

It will get on all your disks. (Θα καταλάβει όλους σας τους δίσκους)

It will infiltrate your chips. (Θα διεισδύσει στα τσιπ σας)

Yes it's Cloner! (Ναι, είναι ο Cloner!)

It will stick to you like glue. (Θα σας κολλήσει σαν κόλλα)

It will modify ram too. (Θα τροποποιήσει και τη RAM)

Send in the Cloner! (Διαδώστε τον Cloner!)

Εν τέλει ο ιός διαδόθηκε σε πολλούς υπολογιστές συμμαθητών του, ακόμα και του καθηγητή των Μαθηματικών του.

Τύποι Ιών

Οι ιοί μπορούν να ταξινομηθούν σε δυο κατηγορίες ανάλογα με το σημείο του υλικού ή του λογισμικού που προσβάλουν και ανάλογα με τον τρόπο που πραγματοποιούν τη μόλυνση:

- **Ιοί που μολύνουν τους τομείς σκληρού δίσκου του συστήματος (System sectors):** Οι ιοί αυτοί προσβάλουν τον τομέα εκκίνησης αντιγράφοντας τον κώδικά τους σε δισκέτα είτε στον σκληρό δίσκο και με την εκκίνηση ή την επανεκκίνηση του υπολογιστή, ο ιός φορτώνεται αυτόματα στη μνήμη με σκοπό να προσβάλλει οποιονδήποτε μη προσβεβλημένο δίσκο που έχει πρόσβαση στο σύστημα.
- **Ιοί αρχείων (προγραμμάτων):** Προσκολλώνται ή αντικαθιστούν εκτελέσιμα αρχεία (.com και .exe)σε έναν υπολογιστή.
- **Ιοί μακροεντολών (Macros Viruses):** Προσβάλλουν έγγραφα και πρότυπα, όχι προγράμματα και χρησιμοποιούν μια γλώσσα προγραμματισμού μακροεντολών μιας εφαρμογής για να μεταδοθούν.
- **Ιοί πηγαίου κώδικα (Source Code Viruses)**
- **Ιοί συμπλεγμάτων (σκληρού) δίσκου**
- **Πολυμορφικοί ιοί:** Είναι μια ειδική κατηγορία ιών διότι κάνουν χρήση ενός συνδυασμού τεχνικών προκειμένου να προσβάλουν ένα σύστημα αλλά κι ένα έγγραφο και ένα εκτελέσιμο αρχείο και του τομέα εκκίνησης. Η μόλυνση, λοιπόν, λαμβάνει κάθε φορά διαφορετική μορφή, καθιστώντας δύσκολη την ανίχνευσή του.
- **Αόρατοι ιοί (Stealth Viruses):** Επιχειρούν να κρύψουν τις αποδείξεις της παρουσίας τους προκειμένου να αποφύγουν τον εντοπισμό. Για παράδειγμα εάν προσβάλουν ένα εκτελέσιμο αρχείο το μέγεθός του θα αλλάξει, έτσι ο ιός φροντίζει να αποκρύψει αυτήν την αλλαγή αναφέροντας το αρχικό μέγεθος. Αυτό πετυχαίνεται από τον ιό με το να εμποδίζει όλες τις κλήσεις προσπέλασης του δίσκου.

- **Θωρακισμένοι ιοί (Armored Viruses):** Έχουν σχεδιαστεί για να εμποδίζουν τις προσπάθειες των αναλυτών από την εξέταση του κώδικα, ενώ προστατεύουν τον εαυτό τους από τα προγράμματα εντοπισμού ιών, καθιστώντας πιο δύσκολο να εντοπιστεί.
- **Πολυτμηματικοί ιοί (Multipartite Viruses):** Ο ιός αυτός μολύνει και εξαπλώνεται με πολλούς τρόπους. Ο όρος επινοήθηκε για να περιγράψει τους πρώτους ιούς, που περιλαμβάνουν DoS εκτελέσιμα αρχεία και PC BIOS κώδικα του ιού του τομέα εκκίνησης.
- **Ιοί πλήρωσης κενών (Space filler Viruses):** Είναι ένα Microsoft Windows 9x, αρκετά επιζήμιος ιός υπολογιστών, που εμφανίστηκε το 1998. Αντικαθιστά κρίσιμες πληροφορίες σχετικά με τους δίσκους στο μολυσμένο σύστημα και το πιο σημαντικό, στις περισσότερες περιπτώσεις καταστρέφει το σύστημα BIOS.
- **Ιοί παραλλαγής (Camouflage Viruses):** Μολύνουν έναν υπολογιστή και συνήθως λογίζονται σαν αβλαβής εφαρμογή από το λογισμικό antivirus, που είναι εγκατεστημένο στον υπολογιστή.

(https://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE)

(https://support.microsoft.com/el-gr/kb/187243)

(http://physblogedu.blogspot.gr/2009/08/blog-post_8954.html)

(https://esafetykapandriti.wikispaces.com/%CE%B8%CF%89%CF%81%CE%B1%CE%BA%CE%B9%CF%83%CE%BC%CE%AD%CE%BD%CE%BF%CE%B9+%CE%B9%CE%BF%CE%AF)

(https://en.wikipedia.org/wiki/Multipartite_virus)

(https://en.wikipedia.org/wiki/CIH_(computer_virus))

(http://creatingcomputervirus.blogspot.gr/2010/08/camouflage-viruses.html)

Τρόποι Δράσης και Διάδοσης

Ένας ιός πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης, προκειμένου να δράσει, ανεξάρτητα από τι και πως μολύνει ένα σύστημα. Έτσι πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία του λειτουργικού συστήματος ή του λογισμικού ενός συστήματος, εξασφαλίζοντας την αναπαραγωγή τους και την εκτέλεση του κώδικά τους.

Οι ιοί διαδίδονται από τον έναν υπολογιστή στον άλλο, είτε μέσω φορητού μέσου αποθήκευσης (CD, USB), είτε μέσω διαδικτύου, ο οποίος είναι και πιο διαδεδομένος, λόγω της ευρείας διάδοσης του διαδικτύου διεθνώς. Το ηλεκτρονικό ταχυδρομείο (e-mail) είναι η βασικότερη υπηρεσία διάδοσης ιών, από το οποίο αποστέλλονται ή ως συνημμένα ή ως τμήμα του μηνύματος.

Τρόποι Αντιμετώπισης

Οι ιοί είναι από τους πιο διαδεδομένους κακόβουλους λογισμικού, είναι πολύ δύσκολο έως και αδύνατο να ανιχνευθούν από έναν απλό χρήστη, ενώ πολλοί από αυτούς είναι δημιουργημένοι τόσο προσεκτικά ώστε και οι πλέον ειδικευμένοι χρήστες να μη μπορούν να τους εντοπίσουν. Προκειμένου να εξασφαλιστεί η λειτουργία ενός συστήματος χωρίς μολύνσεις δημιουργήθηκε μια ειδική κατηγορία λογισμικού, το λεγόμενο αντιϊκό (antivirus), τα οποία εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς να χρειάζονται εντολές από το χρήστη, ενώ παραμένουν ως διαδικασίες στη μνήμη (memory resident) προκειμένου να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα antivirus εκτός από το να εντοπίζουν τη μόλυνση τη στιγμή που δρα, είναι σε θέση και να "καθαρίζουν' τυχόν μολυσμένα αρχεία που εντοπίζουν. Οι δημιουργοί ιών λαμβάνουν υπόψη τις μεθόδους εντοπισμού και προσπαθούν να τις εξουδετερώσουν, ακόμα και με την απενεργοποίηση του αντιϊκού, γι' αυτό ο χρήστης θα πρέπει να ενημερώνει συχνά το λογισμικό του και να δημιουργεί τις ειδικές δισκέτες, έτσι ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

Μερικά γνωστά antivirus είναι:

- AVG
- Avast
- Bitdefender
- McAfee
- Norton
- Kaspersky
- Windows Defender
- ZoneAlarm

(https://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE)

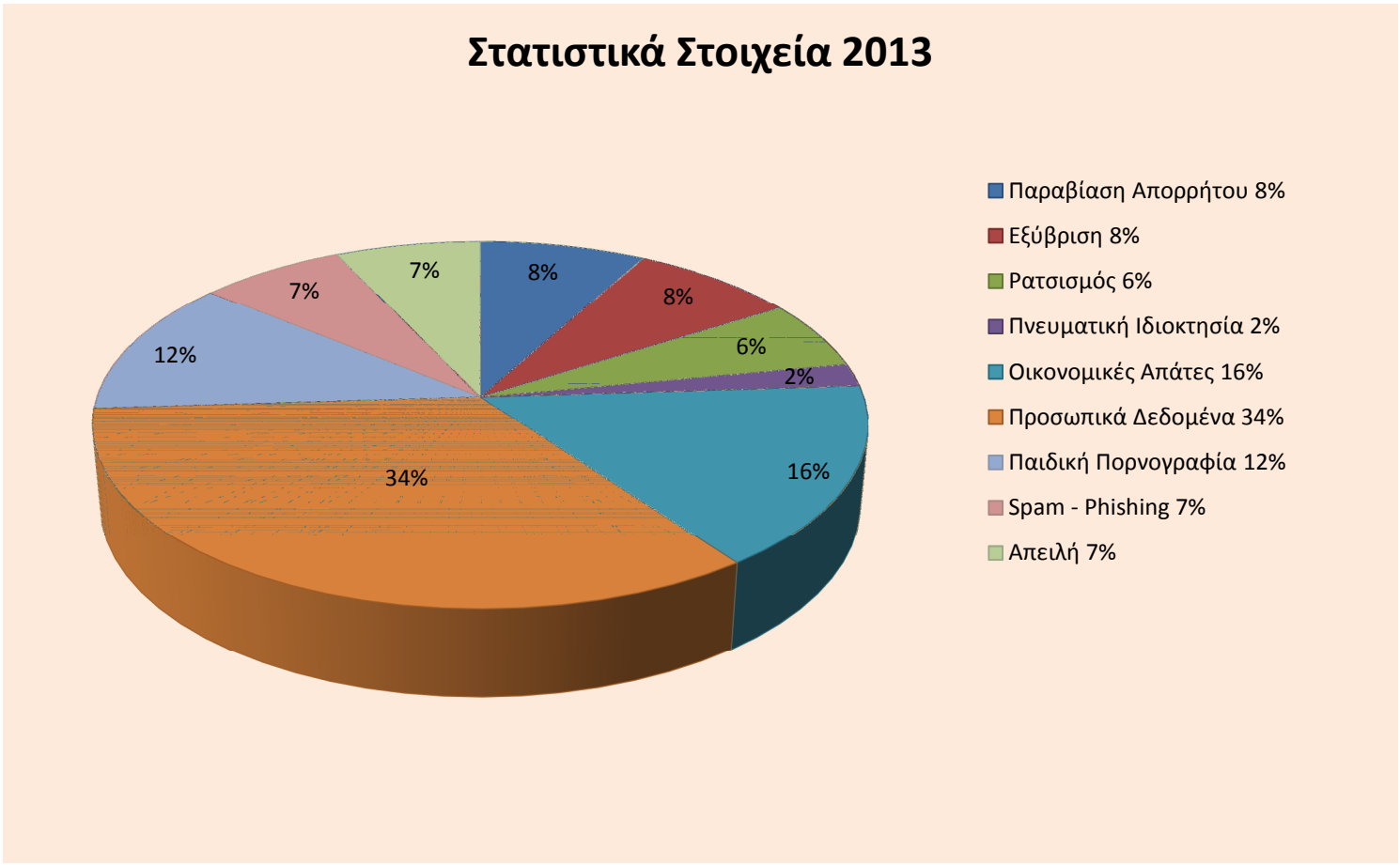
Κεφάλαιο 2ο Στατιστική μελέτη

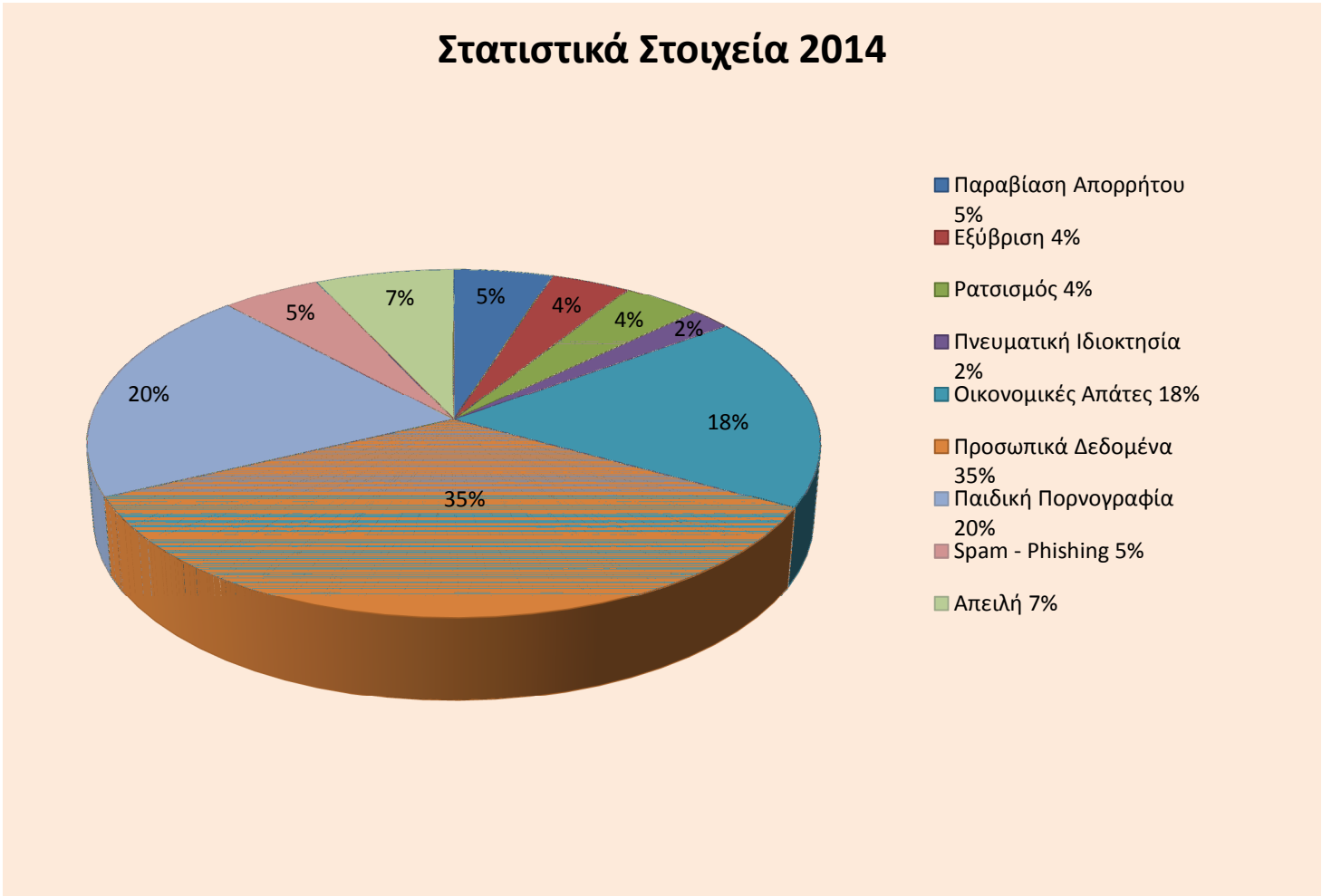
2.1 Προβολή στατιστικών στοιχείων ηλεκτρονικού εγκλήματος στην Ελλάδα από το 2013 έως το 2015

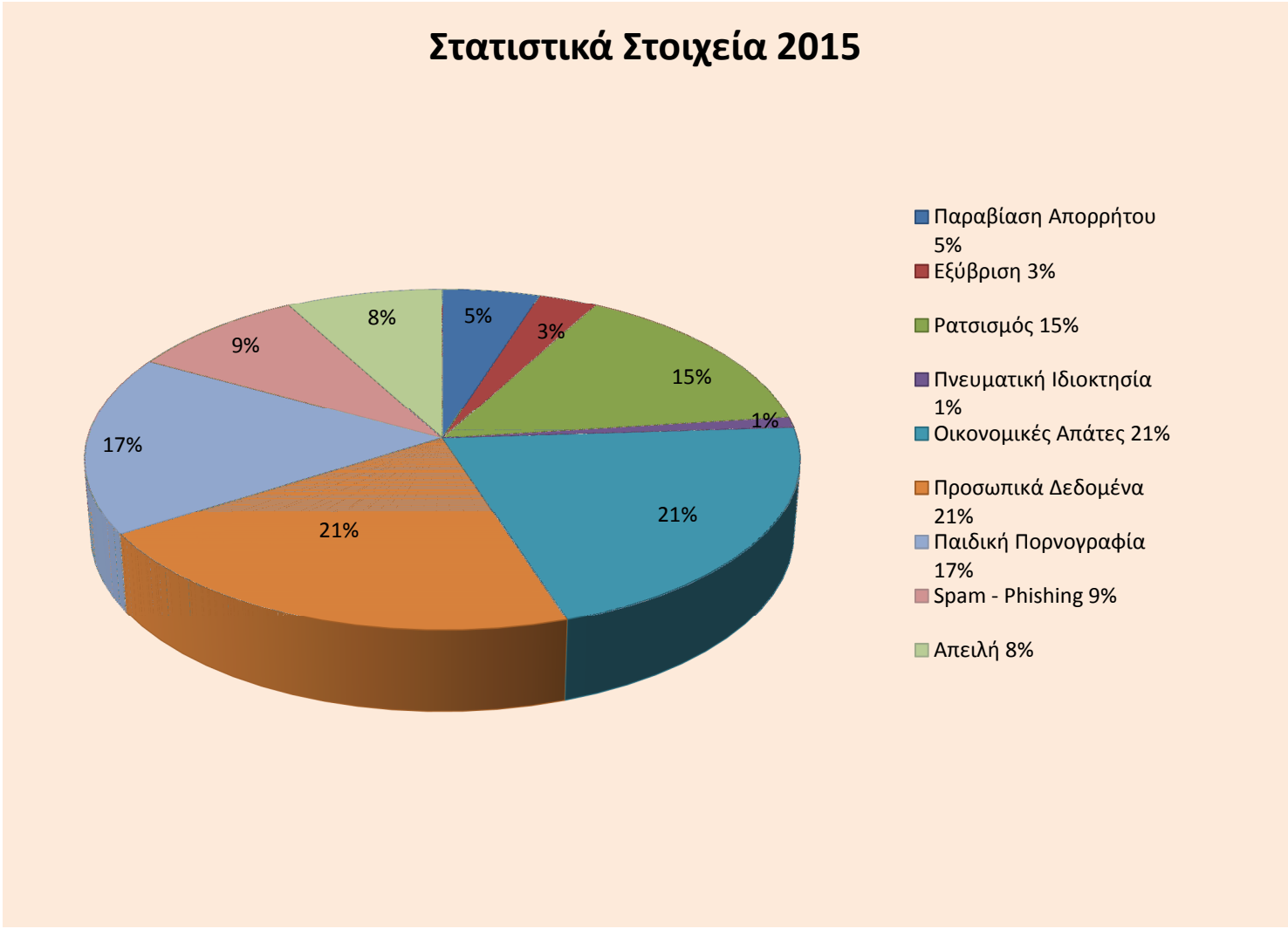
Τα στατιστικά στοιχεία που ακολουθούν αναφέρονται σε τέσσερα (4) έτη και είναι βασισμένα σε καταγγελίες που έγιναν στη safeline.

Η Safeline ιδρύθηκε στις 14 Απριλίου του 2003 από την Ελληνική Εταιρία Τηλεπικοινωνιών και Τηλεματικών Εφαρμογών (FORTHNET), το Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Internet (SAFENET), το Ίδρυμα Τεχνολογίας και Έρευνας – Ινστιτούτο Πληροφορικής (ΙΤΕ - ΙΠ) και το Ίδρυμα Μείζονος Ελληνισμού (ΙΜΕ). Είναι η μοναδική ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο και επίσημο μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) από τις 18 Οκτωβρίου του 2005.

(http://www.safeline.gr/kataggelies/statistika-stoiheia)


Στατιστικά Στοιχεία 2013
8%
8%
6%
2%
16%
34%
12%
7%
7%
Παραβίαση Απορρήτου 8%
Εξύβριση 8%
Ρατσισμός 6%
Πνευματική Ιδιοκτησία 2%
Οικονομικές Απάτες 16%
Προσωπικά Δεδομένα 34%
Παιδική Πορνογραφία 12%
Spam - Phishing 7%
Απειλή 7%


Στατιστικά Στοιχεία 2014
5%
4%
4%
2%
18%
35%
20%
5%
7%
Παραβίαση Απορρήτου 5%
Εξύβριση 4%
Ρατσισμός 4%
Πνευματική Ιδιοκτησία 2%
Οικονομικές Απάτες 18%
Προσωπικά Δεδομένα 35%
Παιδική Πορνογραφία 20%
Spam - Phishing 5%
Απειλή 7%


Στατιστικά Στοιχεία 2015
5%
3%
15%
1%
21%
21%
17%
9%
8%
Παραβίαση Απορρήτου 5%
Εξύβριση 3%
Ρατσισμός 15%
Πνευματική Ιδιοκτησία 1%
Οικονομικές Απάτες 21%
Προσωπικά Δεδομένα 21%
Παιδική Πορνογραφία 17%
Spam - Phishing 9%
Απειλή 8%

2.2 Ανάλυση των στατιστικών στοιχείων

Η Safeline διακρίνει τα ηλεκτρονικά εγκλήματα σε εννέα κατηγορίες:

- ✓ Παραβίαση Απορρήτου (επικοινωνιών)
- ✓ Εξύβριση – Συκοφαντική Δυσφήμηση
- ✓ Ρατσισμός (ξενοφοβία)
- ✓ Πνευματική Ιδιοκτησία
- ✓ Προσωπικά Δεδομένα
- ✓ Παιδική Πορνογραφία
- ✓ Οικονομικές Απάτες
- ✓ Απειλή
- ✓ Spam – Phishing

Παρατηρούμε αυξομειώσεις στα κυβερνοεγκλήματα με μέγιστη έξαρση παραβατικών συμπεριφορών το 2013.

Όπως φαίνεται και στα διαγράμματα, όσο προχωρά η τεχνολογία και οι γνώσεις πληθαίνουν, η ελληνική αστυνομία έχει καταφέρει να ελαττώνει σταδιακά τις παραβατικές συμπεριφορές, ελπίζοντας πως με την πάροδο του χρόνου και φυσικά με τη βοήθεια της κοινωνίας (καταγγέλλοντας τυχόν εγκληματικές συμπεριφορές στο διαδίκτυο) να εξαλειφτεί τελείως κάθε μορφή ηλεκτρονικού εγκλήματος.

2.3 Αναφορά στα ηλεκτρονικά εγκλήματα των στατιστικών στοιχείων

Παραβίαση Απορρήτου (επικοινωνιών)

Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία θεωρούνται απόρρητα:

- ✓ Το περιεχόμενο της επικοινωνίας.
- ✓ Η ταυτότητα του καλούντος και του καλούμενου.
- ✓ Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
- ✓ Τα δεδομένα θέσης της τερματικής συσκευής.

(http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι μια συνταγματικά καθιερωμένη Ανεξάρτητη Αρχή με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύων φορέας για να προστατεύει το απόρρητο της επικοινωνίας.

(http://www.adae.gr/online-ypiresies/erotiseis-gia-polites/)

Εξύβριση – Συκοφαντική Δυσφήμηση

Όποιος ισχυρίζεται ή διαδίδει για κάποιον, ενώπιον τρίτου, γεγονότα που μπορεί να βλάψουν την υπόληψη ή την τιμή του (την αξιοπρέπειά του). Ο νόμος δε δίνει σαφή ορισμό για το τι εστί εξύβριση, έχει όμως παγιωθεί (ιδίως στη γερμανική νομολογία) ο ορισμός "εξύβριση συνιστά η επίθεση κατά της τιμής του άλλου δια της εξωτερίκευσης του μη σεβασμού αυτής (beleidigung ist der Angriff auf die Ehe einer anderen person durch kundgabe den missachtung oder nichtachtung)". Συγκεκριμένα, η έμπρακτη εξύβριση, απαιτεί άμεση σωματική επίδραση στον προσβαλλόμενο, η οποία από μόνη της συνιστά το μη σεβασμό της τιμής του άλλου.

Από την άλλη, το έγκλημα της δυσφήμισης στοιχειοθετείται, με οποιοσδήποτε ισχυρισμό περί της προσβολής της τιμής του άλλου, ασχέτως εάν ισχύει, απέναντι σε τρίτους και φυσικά να αποδειχθεί πως ειπώθηκαν οι εκάστοτε ισχυρισμοί.

Τέλος, η διαφορά της δυσφήμισης από το έγκλημα της συκοφαντικής δυσφήμισης, έγκειται στη γνώση του ενεργούντος για τη μη ισχύ των ισχυρισμών για κάποιον άλλον, άρα δεν αρκεί μόνο ο δόλος, αλλά και η γνώση της ψευδής του δήλωσης.

(http://nomika-analata.blogspot.gr/2013/04/361.html)

(http://paparopoulos-watch.blogspot.gr/p/blog-page.html)

Ρατσισμός (ξενοφοβία)

Ο παραδοσιακός ρατσισμός είναι η διάκριση των φυλών (λαών – εθνών) σε ανώτερες και κατώτερες. Η σύγχρονη προσέγγισή είναι ένα πλέγμα αντιλήψεων, στάσεων, συμπεριφορών και θεσμικών δομών, που εξαναγκάζει ορισμένους ανθρώπους σε υποτελή διαβίωση επειδή ανήκουν σε μια διακριτή ομάδα ανθρώπων.

Η ξενοφοβία είναι η αρνητική αντιμετώπιση οποιουδήποτε ξένου, η τάση για αποφυγή του ξένου τρόπου ζωής, των ξένων παραδόσεων και εθίμων, ως μη γόνιμο, αρνητικό και επομένως μη υιοθετήσιμο.

Ας σκεφτούμε όμως πως από το 1950 έως το 1970 έφυγαν πάνω από 900.000 Έλληνες και από το 2010 ως σήμερα πάνω από 150.000 για αναζήτηση εργασίας στο εξωτερικό.

(https://eclass.duth.gr)

(http://www.tokleidi.com/2013/10/ksenofovia-ratsismos/)

Πνευματική Ιδιοκτησία

Η πνευματική ιδιοκτησία παρέχει στο δημιουργό το δικαίωμα (συναντάται και με τον όρο “copyright”) να εκμεταλλεύεται το έργο του και να απολαμβάνει τα τυχόν οικονομικά οφέλη που του αποφέρει (περιουσιακό δικαίωμα). Επίσης, προστατεύεται

ο προσωπικός δεσμός του δημιουργού με το έργο του, το οποίο αποτελεί έκφραση σκέψεων και συναισθημάτων του (ηθικό δίδαγμα), προάγει το κοινωνικό συμφέρον, διευκολύνει την ελεύθερη κυκλοφορία ιδεών, την κοινωνική εξέλιξη και την ανάπτυξη της πολιτιστικής ζωής.

(http://eclass.uoa.gr/modules/document/file.php/LAW169/%CE%A0%CE%BD%CE%B5%CF%85%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%99%CE%B4%CE%B9%CE%BF%CE%BA%CF%84%CE%B7%CF%83%CE%AF%CE%B1%20%CE%BA%CE%B1%CE%B9%20%CE%99nternet%20(1888)%20-%20%CE%9C%CE%B1%CE%BD%CF%84%CE%B6%CE%AC%CF%81%CE%B7%20%CE%94%CE%AD%CF%83%CF%80%CE%BF%CE%B9%CE%BD%CE%B1.pdf)

Προσωπικά Δεδομένα

Είναι **κάθε** πληροφορία που αναφέρεται και περιγράφει κάθε άτομο όπως: στοιχεία αναγνώρισης (όνομα, επώνυμο, ηλικία, επάγγελμα, οικογενειακή κατάσταση, κατοικία), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία, οικονομική κατάσταση, ενδιαφέροντα, δραστηριότητες, συνήθειες. Το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

(https://el.wikipedia.org/wiki/%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1)

(http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL)

Παιδική Πορνογραφία

Η αύξηση τις παιδικής πορνογραφίας (όπως δείχνουν και τα στατιστικά το 2012 ήταν 12% ενώ την επόμενη χρονιά εκτινάχθηκε στο 20%) είναι θεαματική. Η διακίνηση πορνογραφικού υλικού αποφέρει 3 δις ευρώ τζίρο ετησίως σε παγκόσμια κλίμακα σε εκείνους που ασχολούνται με αυτήν. Εντύπωση προκαλούν οι καταθέσεις των κατηγορούμενων, που πέρα από την κερδοσκοπία, ισχυρίζονται πως ότι κάνουν

το κάνουν από το πάθος τους για το γυμνό παιδικό κορμί, εμείς πάλι θα το χαρακτηρίζαμε ψυχολογική αρρώστια, καθώς η πλειονότητα των φωτογραφιών και των βίντεο που δείχνουν παιδιά, είναι βρέφη ακόμα από οκτώ μηνών έως και εφήβους 17 ετών, που βρίσκονται σε άσεμνες ερωτικές στάσεις και περιπτύξεις είτε μεταξύ τους, είτε με κάποιον ενήλικα.

Κάποιες φορές μπορεί να χρησιμοποιηθεί, το παράνομο αυτό υλικό και ως μέσω απειλής. Χαρακτηριστικό παράδειγμα μαθητές που απειλήθηκαν με ανέβασμα φωτογραφιών τους από τα αποδυτήρια στο διαδίκτυο και αναγκάστηκαν να αλλάξουν σχολικό περιβάλλον.

(https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjFl47EudTLAhWHjCwKHUKBCOMQFgghMAA&url=http%3A%2F%2Fwww.nomikoi-prosanatolismoi.com%2Fuploads%2F1%2F1%2F6%2F4%2F11646921%2F____.doc&usg=AFQjCNEbTBJmYzknAD84TbmwgSYOCyn63Q&bvm=bv.117218890,d.bGg&cad=rja)

Γενικά, παιδική πορνογραφία σημαίνει, οποιαδήποτε αντιπροσώπευση με οποιοδήποτε μέσο, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς.

Η πιο αποτρόπαιη κατάληξη παιδοφιλίας που συγκλόνισε την Ελλάδα, ήταν η δολοφονία του 6 χρόνου Νίκου Δουρή στις 31 Δεκεμβρίου του 1993, από τον πατέρα του Μανώλη Δουρή που τον φίμωσε και τον βίαζε αφήνοντάς τον να ξεψυχήσει σε μια αλάνα.

Οικονομικές Απάτες

Το phishing είναι η πιο διαδεδομένη μορφή που χρησιμοποιείται για τις οικονομικές απάτες. Δίνονται μέσω μηνυμάτων παραπλανητικές οδηγίες, για μεταφορά χρημάτων σε άλλου άγνωστους τραπεζικούς λογαριασμούς δήθεν για λογιστικό έλεγχο. Επίσης, εισχωρούν στην ηλεκτρονική διεύθυνση του θύματος παρακολουθώντας τις συνομιλίες του και προσποιούνται κάποιο οικείο άτομο αποσπώντας μεγάλα χρηματικά ποσά. Τέλος, τα θύματα πραγματοποιούν αγορές μέσω του διαδικτύου από άγνωστους και αναξιόπιστους ιστότοπους, πέφτοντας στην παγίδα εικονικών ιστοσελίδων.

(http://www.ant1iwo.com/news/cyprus/article/213887/exarsi-stis-oikonomikes-apates-meso-idernet/)

Απειλή

Η έρευνα που πραγματοποίησε η Ευρωπαϊκή Ένωση (Ευρωβαρόμετρο για την ασφάλεια του κυβερνοχώρου-2013) σε πάνω από 27.000 άτομα σε όλα τα κράτη μέλη, έδειξε πως:

- Το 87% των ερωτηθέντων αποφεύγουν να αποκαλύπτουν προσωπικά δεδομένα στο διαδίκτυο (ελαφριά μείωση από 89% το 2012).
- Οι περισσότεροι χρήστες εξακολουθούν να μην αισθάνονται καλά ενημερωμένοι σχετικά με τους κινδύνους του ηλεκτρονικού εγκλήματος (52% σε σύγκριση με 59% το 2012).
- Το 7% έχουν πέσει θύμα διαδικτυακής απάτης σε σχέση με την πιστωτική τους κάρτας ή τον τραπεζικό τους λογαριασμό.
- Έχουν αυξηθεί σημαντικά οι χρήστες που έχουν πρόσβαση στο διαδίκτυο μέσω smart phone (35% από 24% το 2012) ή tablet (14% από 6%).

(http://internet-safety.sch.gr/index.php/articles/parents/item/261-euba)

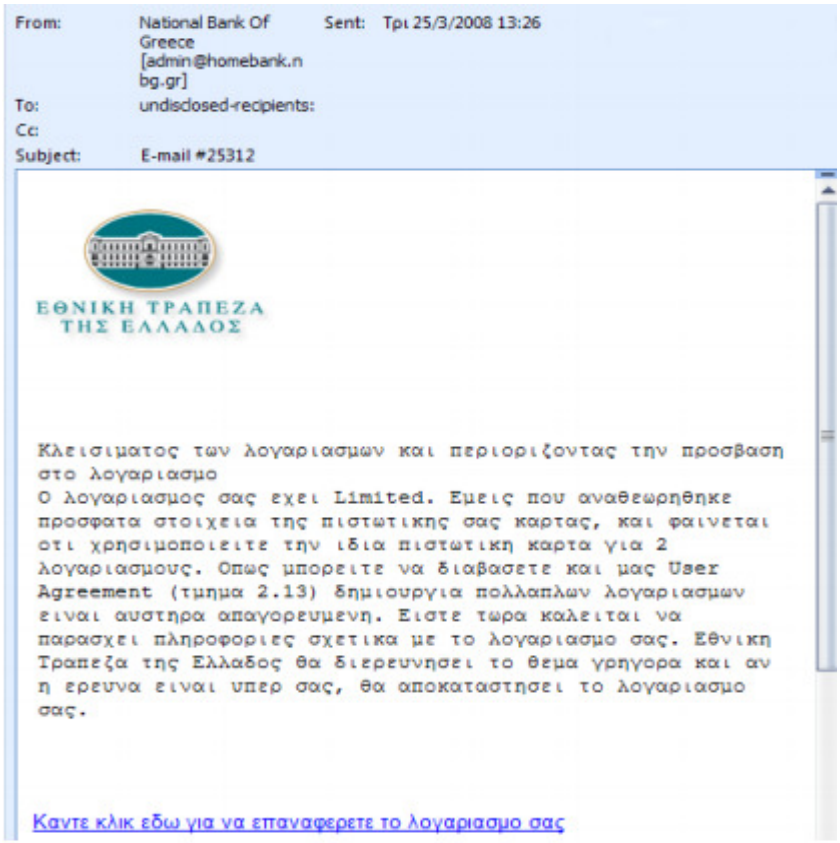
Spam – Phishing

Με τον όρο spam χαρακτηρίζουμε τη μαζική αποστολή μηνυμάτων, συνήθως διαφημιστικών. Η εύρεση των διευθύνσεων είναι εύκολη διαδικασία καθώς οι spammers τις παίρνουν από καταλόγους εταιρειών με ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester (σαρώνει το διαδίκτυο και συλλέγει διευθύνσεις).

Το phishing είναι μια νέα μέθοδος εξαπάτησης των καταναλωτών, με σκοπό την οικονομική απολαβή ή την υφαρπαγή εμπιστευτικών πληροφοριών. Με βοήθεια το spam οι phishers εμφανίζονται ως εκπρόσωποι εταιρειών καταφέρνοντας να

αποσπάσουν από τα θύματά τους αριθμούς λογαριασμών, κωδικούς πιστωτικών καρτών κ.λ.π..

Παραδείγματος χάρη: Εθνική Τράπεζα της Ελλάδος



Η ονομασία phishing αναφέρεται πρώτη φορά το 1996 από χάκερ που έκλεβαν ή παράνομα ιδιοποιούνταν λογαριασμούς νόμιμων χρηστών της εταιρείας America Online (AOL). Η πρώτη αναφορά για το phishing έγινε σε newsgroup hackers γνωστό ως alt.2600 τον Ιανουάριο του 1996 και η πρώτη αναφορά των μέσων ενημέρωσης το Μάρτιο του 1997.

(http://ikee.lib.auth.gr/record/115622/files/ptuxiaki.pdf)

(http://www.saferinternet.gr/index.php?objId=Category116&parentobjId=Page2)

(http://ikee.lib.auth.gr/record/115622/files/ptuxiaki.pdf)

Κεφάλαιο 3ο Καταπολέμηση Ηλεκτρονικού Εγκλήματος

3.1 Ελληνική νομοθεσία και οι αδυναμίες της

Η ελληνική νομοθεσία προβλέπει νόμους για τα εξής ηλεκτρονικά εγκλήματα:

- **Απάτη με υπολογιστή:** Σύμφωνα με το άρθρο αυτό, όποιος, με σκοπό να προσπορίσει στον εαυτό ή σε άλλον παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία, επηρεάζοντας τα αρχεία 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 οποιοδήποτε άλλο τρόπο, τιμωρείται με τις ποινές φυλάκισης που προβλέπονται για την απάτη.
- **Παράνομη πρόσβαση σε απόρρητα:** Απαγορεύεται η αθέμιτη αντιγραφή, αποτύπωση, χρήση, αποκάλυψη ή εν γένει παραβίαση στοιχείων ή προγραμμάτων υπολογιστών ή κρατικών, επιστημονικών, επαγγελματικών απορρήτων ή ιδιωτικών απορρήτων.

(www.icsd.aegean.gr/website_files/proptyxiako/452470770.ppt).

- **Προστασία πνευματικής ιδιοκτησίας και προσωπικών δεδομένων:** Η χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων ηλεκτρονικών υπολογιστών, το άρθρο προστατεύει και το δημιουργό και το χρήστη.
- **Προστασία απορρήτου τηλεφωνικής επικοινωνίας:** Ψηφίστηκε ο νόμος για να ενισχύσει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, θεσπίζοντας ειδικές υποχρεώσεις του παρόχου υπηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της ΑΔΑΕ.
- **Προστασία στις εξ αποστάσεως συμβάσεις:** Αφορά τις εξ αποστάσεως συμβάσεις πρόσβασης σε υπηρεσίες ηλεκτρονικού εμπορίου, απαγορεύει τις παραπλανητικές εμπορικές πρακτικές.

- **Τόπος διαπράξεως εγκλήματος του κυβερνοχώρου:** Τόπος τέλεσης της πράξης θεωρείται ο τόπος που ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη καθώς και ο τόπος που επήλθε, ή σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαίτιου να επέλθει το αξιόποινο αποτέλεσμα.

Όπως αναφέρεται στην ιστοσελίδα της Ελληνικής Αστυνομίας, από τον Προϊστάμενο του Τμήματος Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής, κ. Εμμανουήλ Σφακιανάκης «οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών.»

Σε ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος (Foresight Crime Prevention Panel) διαπιστώθηκε πως το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να υπερκεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο!

(http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414)

3.2 Καταπολέμηση, πώς συμβάλλει η κοινωνία και πώς η αστυνομία

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

Συγκεκριμένα, όσον αφορά τα ηλεκτρονικά εγκλήματα, που έχουν εισέλθει στην καθημερινότητά μας τα τελευταία χρόνια, το ενδιαφέρον της αστυνομίας εστιάζεται περισσότερο στις ασταμάτητες αλλαγές που προκύπτουν στους κόλπους της, καθιστώντας τα ηλεκτρονικά εγκλήματα δύσκολα ανιχνεύσιμα, τόσο στο εξωτερικό όσο και στον ελλαδικό χώρο. Αυτό που φαίνεται να κάνει αποτελεσματικότερο το έργο των διοικητικών αρχών είναι η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού της αστυνομίας, σε θέματα κυρίως τεχνικής φύσεως σχετικά με τη διερεύνηση κατά τη δίωξη του ηλεκτρονικού εγκλήματος. Η ελληνική αστυνομία, έχει προχωρήσει στη σύσταση Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος, ενώ, οι καταγγελίες των πολιτών που διαπιστώνουν ότι έχουν παραβιαστεί προσωπικά τους δεδομένα ή ότι έπεσαν θύματα κάποιας ηλεκτρονικής απάτης ή γενικότερα έχουν αντιληφθεί κάτι ύποπτο σχετικά με το διαδίκτυο ή τη χρήση Η/Υ θα πρέπει να απευθύνονται άμεσα στην αρμόδια αρχή.

Για να προφυλαχτούμε από τις παραβατικές συμπεριφορές, έχοντας μια ομαλή και ασφαλή πλοήγηση στο διαδίκτυο, θα πρέπει να γνωρίζουμε τους κινδύνους που παραμονεύουν, τόσο για τα ενήλικα όσο και για τα ανήλικα μέλη της ψηφιακής κοινωνίας, καθώς και τις βασικές οδηγίες και συμβουλές, ορθής χρήσης του κυβερνοχώρου.

- **Κίνδυνοι για τα παιδιά:**
  - → Μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο.
  - → Μπορούν να έρθουν σε επαφή με αγνώστους που να τα βλάψουν.
  - → Υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο διαδίκτυο.

→ Μπορούν να εθιστούν στη χρήση του διαδικτύου και έτσι κινδυνεύουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις, τα παιχνίδια τους με φίλους.

- **Συμβουλές για τα παιδιά:**

→ Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο διαδίκτυο. Μιλήστε στους γονείς σας για όσα βλέπετε και ζείτε όταν «σερφάρετε» στο internet.

→ Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.

→ Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Μη δίνετε το όνομα, τη διεύθυνσή σας, ή το όνομα και τη διεύθυνση του σχολείου σας, το τηλέφωνο σας και φωτογραφίες σας σε αγνώστους στο διαδίκτυο ακόμα και αν σας το ζητήσουν.

→ Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό, τα μόνα άτομα που πρέπει να τον γνωρίζουν είναι οι γονείς σας.

→ Σκεφτείτε πολύ καλά πριν αποφασίσετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο διαδίκτυο. Ζητήστε την άποψη των γονιών σας. Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συναντήσετε κάποιο άτομο που γνωρίσατε στο διαδίκτυο, προτιμείστε η συνάντηση να γίνει σε δημόσιο χώρο.

→ Μην απαντάτε σε ηλεκτρονικά μηνύματα και σε συνομιλίες σε chat rooms που σας κάνουν να αισθάνεστε «άβολα». Σε περίπτωση που λάβετε τέτοιου είδους μήνυμα, μην διστάσετε να το πείτε στους γονείς σας ή σε κάποιο ενήλικο πρόσωπο που εμπιστεύεστε.

→ Μην εμπιστεύεστε ότι διαβάζετε στο διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

- **Συμβουλές για τους γονείς:**

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

→ Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή.

→ Διδάξτε τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας και να μη χρησιμοποιούν την κάρτα σας.

→ Να είστε ιδιαίτερα προσεκτικοί όταν τα παιδιά χρησιμοποιούν τα chat rooms χωρίς την επίβλεψή σας. Μην αφήνετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω διαδικτύου χωρίς να είστε και εσείς μαζί.

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

→ Εγκαταστήστε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του διαδικτύου με σκοπό την παρεμπόδιση της πρόσβαση σε μη επιθυμητές θέσεις «sites».

→ Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.α., που αγοράζουν τα παιδιά σας ή ανταλλάσουν με τους φίλους τους.

→ Συζητήστε με τα παιδιά σας για την ασφάλεια του διαδικτύου, που προκύπτουν από την πλοήγηση σ' αυτό. Συζητώντας τους μελλοντικούς κινδύνους μέσω του διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.

→ Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω διαδικτύου.

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

→ Ενημερωθείτε σχετικά με τις αρμόδιες αρχές, όπως είναι το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος (210-6476463 & 210-6476464), που θα πρέπει να επικοινωνήσετε σε περίπτωση που συναντήσετε βλαβερό ή παράνομο περιεχόμενο στο internet.

- **Συμβουλές για ασφαλείς οικονομικές συναλλαγές:**

→ Αποφεύγετε να πραγματοποιείτε οικονομικές συναλλαγές μέσω διαδικτύου από internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές.

→ Ως προς τους κωδικούς πρόσβασης για τις διαδικτυακές συναλλαγές:

- ❖ Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.
- ❖ Αποφεύγετε να χρησιμοποιείται κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα.
- ❖ Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια κάρτες σας.
- ❖ Μη δίνετε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις.

→ Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό πρόσβασής σας, στην υπηρεσία internet banking.

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

→ Κάνετε αγορές μόνο από γνωστές εταιρείες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το διαδίκτυο, χρησιμοποιείται μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δε θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.

→ Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας:

- ❖ Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το

λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του.

- ❖ Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall) και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους.
- ❖ Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση μη εξουσιοδοτημένων χρηστών σε αυτόν.

→ Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου:

- ❖ Μην ανοίγετε τα ηλεκτρονικά μηνύματα για την προέλευση ή τον αποστολέα τον οποίο δεν είστε βέβαιοι. Επίσης πρέπει να γνωρίζεται πως πολλοί ιοί λαμβάνουν τις διευθύνσεις που υπάρχουν στις επαφές στο βιβλίο διευθύνσεων του υπολογιστή, που σημαίνει πως μπορεί να φαίνεται πως έχει σταλεί μήνυμα από γνωστό σας.
- ❖ Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία.

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

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

(https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjFl47EudTLAhWHjCwKHUKBCOMQFgghMAA&url=http%3A%2F%2Fwww.nomikoi-prosanatolismoi.com%2Fuploads%2F1%2F1%2F6%2F4%2F11646921%2F____.doc&usg=AFQjCNEbTBJmYzknAD84TbmwgSYOCyn63Q&bvm=bv.117218890,d.bGg&cad=rja)

Συμπεράσματα

«Είμαι εκ φύσεως αισιόδοξος. Εντούτοις, κάθε τεχνολογία ή δώρο της επιστήμης έχει και μια σκοτεινή πλευρά. Ο ψηφιακός κόσμος δεν αποτελεί εξαίρεση σε αυτόν τον κανόνα. Η επόμενη δεκαετία θα γνωρίσει περιπτώσεις κατάχρησης πνευματικής ιδιοκτησίας και εισβολής στην προσωπική μας ζωή. Θα γνωρίσουμε ψηφιακούς βανδαλισμούς, πειρατείες λογισμικού και κλοπές δεδομένων…..»

(Ν. Νεγρεπόντε «ψηφιακός κόσμος 1995»)

Η χρήση του διαδικτύου μέσω των ηλεκτρονικών υπολογιστών παρέχει απεριόριστες δυνατότητες σε όλους τους χρήστες ανεξαρτήτου ηλικίας και γένους. Το διαδίκτυο χρησιμοποιείται καθημερινά είτε σε εμπορικό επίπεδο, για την προώθηση των προϊόντων ή των υπηρεσιών τους ή για τη συναλλαγή με άλλες επιχειρήσεις, είτε σε προσωπικό επίπεδο με σκοπό την ψυχαγωγία, την ενημέρωση, την ανταλλαγή μηνυμάτων και κάθε άλλη μορφή επικοινωνίας.

Η παραβατική συμπεριφορά στο διαδίκτυο κάποιων ατόμων, που βασίζονται στην ελευθερία και την ανωνυμία που τους παρέχει απλόχερα ο κυβερνοχώρος, συνάδουν το ηλεκτρονικό έγκλημα, καθώς αυτού του είδους τα άτομα έχουν ανακαλύψει τρόπους καταστρατήγησης των δυο αυτών εννοιών προβαίνοντας σε ανέλεγκτη ηλεκτρονική επεξεργασία βασικών δεδομένων. Η τεχνολογική εξέλιξη παρέχει πλέον νέες μεθόδους ηλεκτρονικών εγκλημάτων με βασικό στόχο το οικονομικό όφελος. Ο ηλεκτρονικός εγκληματίας έχει τη δυνατότητα να εισβάλει σε επιχειρήσεις αλλά και στο σπίτι του κάθε ιδιώτη καταστρέφοντας και το πιο ασφαλές μέσο προστασίας που μπορούν να διαθέτουν.

Οι παραβατικές συμπεριφορές δεν έχουν όρια και θεωρείται πως στο μέλλον θα πολλαπλασιάζονται οι μορφές των διαδικτυακών εγκλημάτων. Η κατάσταση αυτή μπορεί να επιδεινωθεί με την απουσία των κατάλληλων νομοθετικών πλαισίων, καθώς και με την παράληψη προληπτικών μέτρων έναντι σε τέτοιου είδους παραβάσεων. Η ελληνική αστυνομία έχει δημιουργήσει το Τμήμα της Δίωξης Ηλεκτρονικού Εγκλήματος, με το οποίο όλοι οι καταναλωτές θα πρέπει να

συνεργαζόμαστε εάν διαπιστώσουμε παραβίαση των λογαριασμών μας στο διαδίκτυο, ώστε να διασφαλιστούν η ελευθερία διακίνησης ιδεών και οι ελευθερίες διάθεσης και απόκτησης πληροφοριών.

Θα πρέπει, επίσης, να δημιουργηθεί το κατάλληλο νομοθετικό πλαίσιο που θα αποτελεί το αποδοτικό και αποτελεσματικό «δίχτυ» προστασίας έναντι της λαίλαπας του διαδικτυακού εγκλήματος. Παρατηρείται ότι, στο πλαίσιο της ελληνικής Αστυνομίας, το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος έχει δείξει τις δυνατότητές του και το ζητούμενο για αυτό είναι η πλέον η διασυνοριακή συνεργασία με ομοειδείς φορείς με σκοπό την πλήρη πάταξη του συγκεκριμένου εγκλήματος και όλων των μορφών του.

Βιβλιογραφία

- Χρήστος Ε. Τσουραμάνης, συνεργασία Μαρ. – Ευγ. Κορολή, Οικονομία και Εγκληματικότητα, Σεπτέμβριος 2010
- Χρήστος Ε. Τσουραμάνης, συνεργασία Ι. Γουσέτη, Μ. Στ. Ζεάκη, Μ. Ε. Κορολή, Μ. Λεμπέση, Β. Μεντή, Μ. Μπαρπάτση, Το Έγκλημα, Αύγουστος 2009
- Steven Furnell, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας
- Λίλιαν Μήτρου, Το δίκαιο στην Κοινωνία της Πληροφορίας, 2002

Ηλεκτρονική Βιβλιογραφία

- Ηλεκτρονικό και Διαδικτυακό Έγκλημα, Το Ποινικό Δίκαιο της Πληροφορικής, Πανεπιστήμιο Αιγαίου, χωρίς χρονολογία, ανακτήθηκε από (www.icsd.aegean.gr/website_files/proptyxiako/714097945.doc)
- Comprehensive Study on Cybercrime, Draft February 2013, United Nations Office on Drugs and Crime UNODS, ανακτήθηκε από (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf)
- Παναγιώτης Κιντής και Σπύρου Ραψομανίκης, Ηλεκτρονικό Έγκλημα, Privacy and Computer Forensics και ο Νομικός Αντίκτυπος, 2010-2011, Πανεπιστήμιο Αιγαίου, ανακτήθηκε από (http://eurydice.lib.aegean.gr/_original_/a12040/file0.pdf)
- Κασπαρίδης Παναγιώτης και Χατζιπαναγιώτου Αγγελική, «Παιδική Εγκληματικότητα στον Κυβερνοχώρο», ΤΕΙ Καβάλας Τμήμα Διαχείρισης Πληροφοριών ΣΔΟ, Ιούνιος 2010, ανακτήθηκε από (http://digilib.teiemt.gr/jspui/bitstream/123456789/6677/1/SDO1622010.pdf)
- Ιωάννης Β. Θεοδωράκης, «Οικονομικό Έγκλημα: Εννοιολογικές προσεγγίσεις, θεσμοί και βέλτιστες πρακτικές διακυβέρνησης σε ένα παγκοσμιοποιημένο περιβάλλον», Πανεπιστήμιο Μακεδονίας, Σεπτέμβριος 2011, ανακτήθηκε από (https://dspace.lib.uom.gr/bitstream/2159/14604/6/TheodorakisIoannisMsc2011.pdf)
- Ελληνική Αστυνομία, χωρίς χρονολογία, ανακτήθηκε από
  → (http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang)

→ (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414)

- Joseph-Marie Jacquard, χωρίς χρονολογία, ανακτήθηκε από (https://translate.google.gr/translate?hl=el&sl=en&u=http://www.britannica.com/biography/Joseph-Marie-Jacquard&prev=search)
- Διαδίκτυο και Ανθρώπινες σχέσεις (ερευνητική εργασία 1ου ΓΕ.Λ Σταυρούπολης), χωρίς χρονολογία, ανακτήθηκε από (http://diadiktiosxeseis.blogspot.gr/p/blog-page_7135.html)
- Τι είναι κυβερνοχώρος, Inter BIZ news letter, χωρίς χρονολογία, ανακτήθηκε από (http://www.eeei.gr/interbiz/articles/cybspace.htm)
- Λίλιαν Μήτρου, Κανονιστικό πλαίσιο ΚτΠ Ηλεκτρονικό έγκλημα και κυβερνοέγκλημα, χωρίς χρονολογία, ανακτήθηκε από (www.icsd.aegean.gr/website_files/proptyxiako/452470770.ppt)
- Συνέντευξη Μανώλη Σφακιανάκη, Επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος, «Ασφαλής υπολογιστής είναι μόνο ο…κλειστός», χωρίς χρονολογία, ανακτήθηκε από (http://cert.auth.gr/index.php/el/mnu-announce/101-interview-sfakianakis)
- David L. Carter, Rh. D. καθηγητής στη σχολή της ποινικής δικαιοσύνης, Michigan State University, East Lansing, Michigan, ανακτήθηκε από (https://translate.google.gr/translate?hl=el&sl=en&u=http://www.lectlaw.com/files/cri14.htm&prev=search)
- Λίλιαν Μήτρου, Παραβατικότητα και ποινικό δίκαιο στην κοινωνία της πληροφορίας, Πανεπιστήμιο Αιγαίου, Τμήμα Πληροφοριακών και Επικοινωνιακών Συστημάτων, χωρίς χρονολογία, ανακτήθηκε από (www.icsd.aegean.gr/website_files/proptyxiako/714097945.doc)
- Wikipedia, Χάκερ, Μάρτιος 2016, ανακτήθηκε από (https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81#cite_note-1)
- Wikipedia, Ιός υπολογιστή, Απρίλιος 2016, ανακτήθηκε από (https://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE)
- Microsoft, Ιοί μακροεντολών, Μάιος 2015, ανακτήθηκε από (https://support.microsoft.com/el-gr/kb/187243)
- Οι ιοί στους υπολογιστές, χωρίς χρονολογία, ανακτήθηκε από (http://physblogedu.blogspot.gr/2009/08/blog-post_8954.html)

- Θωρακισμένοι ιοί, 2016, ανακτήθηκε από (https://esafetykapandriti.wikispaces.com/%CE%B8%CF%89%CF%81%CE%B1%CE%BA%CE%B9%CF%83%CE%BC%CE%AD%CE%BD%CE%BF%CE%B9+%CE%B9%CE%BF%CE%AF)
- Wikipedia, Multipartite virus, Νοέμβριος 2013, ανακτήθηκε από (https://en.wikipedia.org/wiki/Multipartite_virus)
- Wikipedia, CIH computer virus, Μάιος 2016, ανακτήθηκε από (https://en.wikipedia.org/wiki/CIH_(computer_virus)
- Camouflage Viruses, Αυγουστος 2010, ανακτήθηκε από (http://creatingcomputervirus.blogspot.gr/2010/08/camouflage-viruses.html)
- Safeline, καταγγελίες και στατιστικά στοιχεία, χωρίς χρονολογία, ανακτήθηκε από (http://www.safeline.gr/kataggelies/statistika-stoiheia)
- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, χωρίς χρονολογία, ανακτήθηκε από
  - → (http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/)
  - → (http://www.adae.gr/online-ypiresies/erotiseis-gia-polites/)
- Δημήτριος Δημητριάδης, Εγκλήματα κατά της τιμής, άρθ. 361 ΠΚ επ. (εξύβριση, δυσφήμιση, συκοφαντική δυσφήμιση), Νομικά Ανάλατα, Απρίλιος 2013, ανακτήθηκε από (http://nomika-analata.blogspot.gr/2013/04/361.html)
- Γιώργος Πιπερόπουλος, Συκοφαντική Δυσφήμηση και Ποινικός κώδικας, χωρίς χρονολογία, ανακτήθηκε από (http://paparopoulos-watch.blogspot.gr/p/blog-page.html)
- (https://eclass.duth.gr)
- Το κλειδί της σκέψης, Ξενοφοβία και Ρατσισμός, Οκτώβριος 2013, ανακτήθηκε από (http://www.tokleidi.com/2013/10/ksenofovia-ratsismos/)
- Μάντζαρη Δέσποινα, «Πνευματική Ιδιοκτησία και Interne» (Η Συνταγματική τους Προστασία) Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών Τμήμα Νομικών, Οικονομικών και Πολιτικών Επιστημών Τομέας Δημοσίου Δικαίου, ανακτήθηκε από (http://eclass.uoa.gr/modules/document/file.php/LAW169/%CE%A0%CE%BD%CE%B5%CF%85%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%99%CE%B4%CE%B9%CE%BF%CE%BA%CF%84%CE%B7%CF%83%CE%

AF%CE%B1%20%CE%BA%CE%B1%CE%B9%20%CE%99nternet%20(1888)%20-%20%CE%9C%CE%B1%CE%BD%CF%84%CE%B6%CE%AC%CF%81%CE%B7%20%CE%94%CE%AD%CF%83%CF%80%CE%BF%CE%B9%CE%BD%CE%B1.pdf)

- Wikipedia, Προσωπικά δεδομένα, Απρίλιος 2016, ανακτήθηκε από (https://el.wikipedia.org/wiki/%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1)
- Αρχή προστασίας Δεδομένων προσωπικού χαρακτήρα, χωρίς χρονολογία, ανακτήθηκε από (http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL)
- Δίωξη Ηλεκτρονικού Εγκλήματος του Internet από την ΕΛ.ΑΣ. (παγκοσμίως καλύτερη υπηρεσία) και Μορφές Ηλεκτρονικού Εγκλήματος, χωρίς χρονολογία, ανακτήθηκε από (https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjFl47EudTLAhWHjCwKHUKBCOMQFgghMAA&url=http%3A%2F%2Fwww.nomikoi-prosanatolismoi.com%2Fuploads%2F1%2F1%2F6%2F4%2F11646921%2F____.doc&usg=AFQjCNEbTBJmYzknAD84TbmwgSYOCyn63Q&bvm=bv.117218890,d.bGg&cad=rja)
- Έξαρση στις οικονομικές απάτες, ant1iwo, Ιούλιος 2015 ανακτήθηκε από (http://www.ant1iwo.com/news/cyprus/article/213887/exarsi-stis-oikonomikes-apates-meso-idernet/)
- Ασφάλεια Στο Διαδίκτυο, Ενημερωτικός Κόμβος Πανελλήνιου Σχολικού Δικτύου, sch.gr, , χωρίς χρονολογία, ανακτήθηκε από (http://internet-safety.sch.gr/index.php/articles/parents/item/261-euba)
- (http://ikee.lib.auth.gr/record/115622/files/ptuxiaki.pdf)
- Safer internet, Μάιος 2016, ανακτήθηκε από (http://www.saferinternet.gr/index.php?objId=Category116&parentobjId=Page2)