ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Πτυχιακή εργασία

Ηλεκτρονικό έγκλημα

Συγγραφείς Πτυχιακής Εργασίας:

Λυκούρεσης Ιωάννης

Φραντζέσκου Παναγιώτα

Επόπτης καθηγητής:

Ασημακόπουλος Γιώργος

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1:

ΕΙΣΑΓΩΓΗ

Οι ηλεκτρονικές επικοινωνίες αναμφίβολα διαδραματίζουν σπουδαίο ρόλο στη ζωή μας ενώ παράλληλα την προάγουν σημαντικά. Μπορούμε πολύ εύκολα να διαπιστώσουμε την παρουσία της υψηλής τεχνολογίας σε κάθε έκφανση της ζωής μας και για κάθε χρήση της. Καθημερινά, όλο και περισσότεροι άνθρωποι χρησιμοποιούν το Διαδίκτυο, τα κινητά τηλέφωνα, τις ψηφιακές φωτογραφικές μηχανές, τα ψηφιακά βίντεο, τους ψηφιακούς αναπαραγωγούς μουσικών τραγουδιών και, φυσικά, τους προσωπικούς ηλεκτρονικούς υπολογιστές.

Όλα τα ψηφιακά μέσα επιδρούν άμεσα στην ζωή των ανθρώπων, καθώς παράγουν πλήθος πληροφοριών, οι οποίες ρέουν συνεχώς και ασταμάτητα, ενώ είναι σε θέση να προσφέρουν τεράστιες δυνατότητες σε όλους εκείνους που έχουν την γνώση και τη διάθεση να τις εκμεταλλευτούν με οποιοδήποτε τρόπο.

Ασφαλώς, η βάση της τεχνολογίας αυτής της ψηφιακής κοινωνίας είναι το Διαδίκτυο, το οποίο έχει εισέλθει στη ζωή μας και την έχει αλλάξει ριζικά. Αναμφισβήτητα έχει επηρεάσει πολλούς παράγοντες της ζωής μας, τον τρόπο που επικοινωνούμε, δουλεύουμε και κυρίως τον τρόπο με τον οποίο ζούμε. Τα θετικά του στοιχεία το καθιστούν το κυριότερο εργαλείο στα χέρια των ανθρώπων όσον αφορά την επικοινωνία. Το σημαντικότερο πλεονέκτημα που διαθέτει είναι η ταχύτητα και η άνεση που προσφέρει στον χρήστη, καθώς όλα πραγματοποιούνται με το πάτημα ενός κουμπιού. Η συνετή του χρήση μπορεί να ανεβάσει το μορφωτικό επίπεδο των ανθρώπων προσφέροντας σημαντικές πληροφορίες για επίκαιρα ζητήματα ενώ άξια λόγου είναι και η συμβολή του στην εκπαιδευτική διαδικασία.

Το σημαντικότερο, όμως, μειονέκτημα του Διαδικτύου είναι αυτό που αποτελεί και το κυριότερο λειτουργικό πρόβλημα του, είναι η μη ασφάλεια, δηλαδή, του περιεχομένου των πληροφοριών του από αλλοιώσεις και καταστροφές που προέρχονται από μη εξουσιοδοτημένη χρήση με άμεσο αποτέλεσμα την εμφάνιση διαφόρων τύπων ηλεκτρονικών εγκλημάτων.

Η αλματώδης αύξηση των παράνομων δραστηριοτήτων στο Διαδίκτυο, οφείλεται σε δύο από τις πιο διαδεδομένες ανακρίβειες για αυτό: την ανωνυμία και την απόλυτη ελευθερία έκφρασης στους χρήστες του.

Στην παρούσα εργασία ασχοληθήκαμε με τις διάφορες και αρκετές μορφές του ηλεκτρονικού εγκλήματος. Ενδεικτικά, αναφέρουμε τις μορφές αυτές ονομαστικά: Κυβερνοσφετερισμός, Spamming, η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (Hacking, Cracking), διασπορά κακόβουλων προγραμμάτων, απάτη μέσω Διαδικτύου, τηλεχειρισμός (κατασκοπεία) του υπολογιστή, Cookies, υποκλοπή αρχείων Η/Υ, πειρατεία λογισμικού, πλαστογραφία, διακίνηση ναρκωτικών, εμπόριο οργάνων, αυτοκτονία, κυβερνοπόλεμος – κυβερνοτρομοκρατία και την παιδική πορνογραφία.

Το Internet, μπορεί να συμμετέχει στην εκμετάλλευση παιδιών με διαφόρους τρόπους. Το Διαδίκτυο γίνεται το μέσο όταν διαδραματίζει έναν σημαντικό ρόλο στην διάπραξη ενός εγκλήματος, όπως ο δελεασμός των ανηλίκων για τη συμμετοχή τους σε σεξουαλική δραστηριότητα ή τη διάδοση παιδικού πορνογραφικού υλικού. Σε άλλες περιπτώσεις, το Διαδίκτυο μπορεί απλά να δείξει ότι ένα έγκλημα έχει εμφανιστεί και να παρέχει πρόσθετη εξεταστική βοήθεια και χρήσιμες πληροφορίες για τον παραβάτη ή το θύμα. Μαζί με τη διαθεσιμότητα της επικοινωνίας με τα θύματα, το Διαδίκτυο επιτρέπει στο παραβάτη να μπει κυριολεκτικά στα σπίτια των θυμάτων. Είναι αρκετά δυνατό για έναν παραβάτη να είναι σε ανοικτή γραμμή με ένα θύμα ενώ οι γονείς του ή αυτός που το προσέχει να είναι στο σπίτι, ακόμη και στο ίδιο δωμάτιο.

Insertion

Electronic communications undoubtedly play an important role in our lives while promoting them significantly. We can very easily see the presence of high technology in every event of our lives and for every use. Every day more and more people are using the Internet, mobile phones, digital cameras, digital videos, digital music plays and, of course, personal computers.

All digital media have a direct impact on people's lives, as they produce a wealth of information that flows continuously and uninterrupted, while being able to offer enormous opportunities to all who have the knowledge and the willingness to exploit them in any way.

Of course, the technology base of this digital society is the Internet, which has come into our lives and radically changed it. It has undoubtedly influenced many factors in our lives, the way we communicate, work and most importantly the way we live. Its positive features make it the most important tool in people's hands for communication. The most important advantage is the speed and convenience it offers to the user, as everything is done at the touch of a button. Its prudent use can raise the educational level of people by providing important information on current issues while contributing to the educational process.

However, the major disadvantage of the Internet is that its main operational problem is insecurity, that is, the content of its information from tampering and disasters resulting from unauthorized use that has the immediate effect of various types of cybercrime.

The jump in illegal Internet activity is due to two of the most widespread inaccuracies: anonymity and absolute freedom of expression for its users.

In this paper we have dealt with the various and several forms of cybercrime. Indicatively, these forms are named: Cyber-Bullying, Spamming, Unauthorized computer access (Hacking & Cracking), Malware spreading, Internet fraud, Remote control (Computer spy), Cookies, Computer theft software, Piracy, Forgery, Drug trafficking, Organ trafficking, Suicide, Cyber warfare and Child pornography.

The Internet can be involved in the exploitation of children in various ways. The Internet becomes the medium when it plays an important role in the commission of a crime, such as enticing minors to engage in sexual activity or disseminating child pornography. In other cases, the Internet may simply indicate that a crime has occurred and provide additional investigative

assistance and useful information to the offender or victim. Along with the availability of communication with the victims, the Internet allows the offender to literally enter the victims' homes. It is quite possible for an offender to be in line with a victim while his or her parents are at home, even in the same room.

Παρακάτω θα εξετάσουμε και θα αναλύσουμε τα προαναφερθέντα με περεταίρω λεπτομέρειες.

1.1 Ιστορική αναδρομή

Αξίζει να κάνουμε μια σύντομη ιστορική αναδρομή στο ηλεκτρονικό έγκλημα μελετώντας κυρίως το τεχνολογικό και νομικό πλαίσιο κάθε εποχής. Ο στόχος είναι, αφενός, να προσπαθήσουμε να παρακολουθήσουμε την εξέλιξή του και, αφετέρου, να καταλάβουμε πως «πολλά προβλήματα στην ηλεκτρονική ασφάλεια είναι μετενσάρκωση παλαιών και γνωστών προβλημάτων». Τέλος, είναι απαραίτητο να δούμε πώς και με ποιο τρόπο αντιμετωπίζονταν οι πράξεις ηλεκτρονικού εγκλήματος κάθε εποχή αλλά και ποιος είναι, σε κάθε περίπτωση, ο πραγματικός επιτιθέμενος.

Στις αρχές της δεκαετίας του ’80 είχαμε την έλευση του δικτυακού πρωτοκόλλου X.25, μέσω του οποίου οι υπολογιστές εκείνης της εποχής (Sinclair Spectrum, PC XT/PC AT και Apple) μπορούσαν, με μια κατάλληλη συσκευή (του γνωστού σε όλους μας modem) καθώς και τη χρήση του τηλεπικοινωνιακού δικτύου, να επικοινωνήσουν μεταξύ τους. Σύντομα, πολλοί χρήστες ξεκίνησαν να μοιράζονται πληροφορίες μέσω των λεγόμενων BBSs (Bulletin Board Service). Ο τρόπος ήταν απλός: αρκούσε ένα τηλεφώνημα από το modem σε έναν συγκεκριμένο αριθμό.

Στην κλήση απαντούσε το modem του «απέναντι» υπολογιστή και η σύνδεση ήταν επιτυχής. Μετά, ο χρήστης που συνδεόταν στην BBS, μπορούσε να διαβάσει συγκεκριμένες πληροφορίες, να «κατεβάσει» (download) όποιες από αυτές ήθελε αλλά και να «ανεβάσει» (upload) δικές του με χρήση κατάλληλων πρωτοκόλλων.

Κύριοι φορείς των συγκεκριμένων υπηρεσιών ήταν τα πανεπιστήμια, διάφορες εμπορικές εταιρείες αλλά και πολλοί ιδιώτες. Ιστορικά και μόνο αναφέρουμε πως οι πρώτες πληροφορίες που έβρισκε ένας χρήστης που συνδεόταν σε μια BBS (στην εισαγωγική δηλαδή οθόνη), ήταν αναλυτικές οδηγίες για το πως μπορεί να συνδεθεί σε αυτήν.

Σύντομα εμφανίστηκαν και οι πρώτοι hackers οι οποίοι χρησιμοποιούσαν τα modems για να συνδεθούν σε υπολογιστές στους οποίους δεν έπρεπε κανονικά να έχουν πρόσβαση (π.χ. στρατιωτικούς υπολογιστές ή ακαδημαϊκά ιδρύματα, για εκείνους που δεν ήταν φοιτητές στη συγκεκριμένη σχολή). Καθώς τα μέτρα ασφάλειας ήταν ελάχιστα, την τριετία 1983-85 αναφέρονται στη Μεγάλη Βρετανία τα πρώτα κρούσματα hacking, τα οποία αφορούσαν κυρίως σε απόπειρες, πολλές φορές μάλιστα επιτυχημένες, για παράνομη αντιγραφή πληροφοριών καθώς και πρόκληση ζημιών σε υπολογιστικά συστήματα πανεπιστημίων.

Την ίδια εποχή, και πιο συγκεκριμένα το 1984, ιδρύεται το «τμήμα» δίωξης ηλεκτρονικού εγκλήματος στην New Scotland Yard. Επίσης, η Μεγάλη Βρετανία γίνεται η πρώτη χώρα στην Ευρώπη η οποία εκδίδει νόμο περί προστασίας των ηλεκτρονικών δεδομένων (Data Protection Act 1984). Τέλος, κυκλοφορεί περιοδικό με το «εγχειρίδιο του hacker» (the hacker's handbook), το οποίο γίνεται ανάρπαστο.

Τα επόμενα χρόνια, μέχρι τα τέλη της δεκαετίας, σημαδεύονται από την άνθιση των λεγόμενων υπολογιστικών «ιών» (computer viruses). Ο ιός Aids κάνει θραύση καθώς πολλά περιοδικά υπολογιστών στην Ευρώπη κυκλοφορούν με δισκέτα μολυσμένη από το συγκεκριμένο ιό. Η περίπτωση αυτή είναι η πρώτη μαζική μόλυνση υπολογιστικών συστημάτων αλλά και η πρώτη περίπτωση εκβιασμού, από το συγγραφέα του «ιού», ο οποίος απαιτούσε συγκεκριμένο χρηματικό αντίτιμο, για να παρέχει το «αντίδοτο».

Το 1989 είναι η χρονιά στην οποία γίνεται η πρώτη σοβαρή προσπάθεια, σε Πανευρωπαϊκό επίπεδο, για τη νομική αντιμετώπιση του ηλεκτρονικού εγκλήματος. Εκείνη την εποχή υπήρχαν ελάχιστες χώρες στον κόσμο (Ηνωμένο Βασίλειο, Αυστρία, Δανία, Γερμανία, Γαλλία, Ομοσπονδιακή Δημοκρατία της Γερμανίας, Ελλάδα, Νορβηγία, Σουηδία, Ηνωμένες Πολιτείες, Αυστραλία, Ιαπωνία και Καναδάς), οι οποίες είχαν ήδη θεσπίσει νόμους που κάλυπταν κάποια τμήματα του ηλεκτρονικού εγκλήματος.

Οι στόχοι της συγκεκριμένης επιτροπής (Legal Affairs Committee), η οποία συγκροτήθηκε από εκπροσώπους όλων σχεδόν των Ευρωπαϊκών χωρών, ήταν η δημιουργία ενός κοινού πλαισίου για γρήγορη και αποτελεσματική αντίδραση σε περιστατικά ασφάλειας που υποδήλωναν πράξεις ηλεκτρονικού εγκλήματος. Οι νομικοί της συγκεκριμένης επιτροπής είχαν καταλάβει πως το ηλεκτρονικό έγκλημα είναι ένα πρόβλημα που δεν γνωρίζει σύνορα και η ανάγκη ύπαρξης ενός ενιαίου (κατά το δυνατόν) νομικού πλαισίου ήταν παραπάνω από απαραίτητη. Η σύσταση της συγκεκριμένης επιτροπής έγινε γνωστή με την ονομασία Council of Europe Recommendation R(89)9. Τέλος, την εποχή εκείνη κυκλοφορεί το περιβόητο βιβλίο

The Cuckoo's Egg, στο οποίο ο συγγραφέας περιγράφει την πρώτη καταγεγραμμένη περίπτωση διεθνούς κατασκοπείας μέσω υπολογιστών.

Η αρχή της δεκαετίας του '90, εκτός από το κίνημα grunge, φέρνει την ίδρυση του πρώτου παγκόσμιου κέντρου συντονισμού για περιστατικά ασφάλειας σε υπολογιστικά συστήματα στο Software Engineering Institute του πανεπιστημίου Carnegie Melon, στις ΗΠΑ. Το κέντρο αυτό, είναι γνωστό σήμερα σαν CERT/CC (Computer Emergency Response Team/Coordination Center).

Παράλληλα, το Internet εξαπλώνεται ραγδαία μέσω της υπηρεσίας WWW (World Wide Web) η οποία επιτρέπει τη φιλοξενία αρχείων ήχου, βίντεο, εικόνων και υπερκειμένου (Hypertext) στις ιστοσελίδες των αντίστοιχων διακομιστών (Servers). Η άνθιση αυτή συνοδεύεται, όμως, από χιλιάδες σελίδες με πορνογραφικό υλικό, τρομοκρατικές προκηρύξεις καθώς και από αμέτρητες σελίδες μέσα από τις οποίες προσφέρεται – με παράνομο τρόπο – πειρατικό λογισμικό για υπολογιστές.

Από την άλλη πλευρά, καταγράφεται η πρώτη περίπτωση βιομηχανικής κατασκοπείας με δράστη τον περιβόητο Αμερικάνο hacker Kevin Mitnick, ο οποίος και φυλακίζεται με την κατηγορία πρόκλησης βλάβης σε υπολογιστικά συστήματα καθώς και για διαφυγόντα κέρδη 9 δισεκατομμυρίων δολαρίων.

Περίπου στα 1995 ξεκινά η ραγδαία αύξηση των παροχών Internet Υπηρεσιών (Internet Service Providers – ISPs), ενώ κάνουν δειλά-δειλά τα βήματά τους οι πρώτες εταιρείες οι οποίες προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου (e-commerce). Την ίδια εποχή, όμως, κυκλοφορεί, δωρεάν στο Internet, το εργαλείο SATAN (Security Administrator Tool for Analyzing Networks), το οποίο χρησιμεύει για να ανακαλύπτει αδυναμίες στη δικτυακή και υπολογιστική υποδομή διαφόρων οργανισμών και εταιρειών.

Το SATAN κυκλοφόρησε αρχικά σαν ένα πολύτιμο εργαλείο για τους διαχειριστές δικτύων και συστημάτων (network and system administrators) των διαφόρων εταιρειών, γρήγορα όμως οι hackers κατάλαβαν τη διττή σημασία του και άρχισαν να το χρησιμοποιούν εκτεταμένα. Παράλληλα, ξεκινά από τη Μεγάλη Βρετανία η πρώτη προσπάθεια, με το πρότυπο συμμόρφωσης BS 7799, για την έκδοση ενός «οδηγού» με κατάλληλες εταιρικές πολιτικές ασφάλειας.

Το δεύτερο μισό της δεκαετίας του '90 επιφυλάσσει πολλές δυσάρεστες εκπλήξεις στον κόσμο της πληροφορικής. Κυκλοφορεί ο πρώτος macro-virus, ο οποίος προσβάλλει μη εκτελέσιμα

αρχεία (π.χ. αρχεία κειμένου ή λογιστικά φύλλα), γνωστός με το όνομα Melissa. Ο ιός αυτός, όσο και οι κλώνοι του, προξενούν ζημιές εκατομμυρίων δολαρίων σε υπολογιστικά συστήματα σε όλα τα μήκη και πλάτη του πλανήτη.

Παράλληλα με τους macro-viruses, ανθούν και τα διάφορα freeware tools, εργαλεία λογισμικού τα οποία διατίθενται ελεύθερα στο Internet, με τα οποία μπορεί κάποιος hacker να εκμεταλλευτεί τα όποια υπάρχοντα κενά ασφάλειας. Τέλος, οι σελίδες με σχετικό (με το παραπάνω) περιεχόμενο εκείνη την εποχή ανέρχονται σε μερικές χιλιάδες, ενώ η παράνομη αντιγραφή ψηφιακού περιεχομένου γίνεται ολοένα και μεγαλύτερη με την έλευση των αντιγραφικών συσκευών οπτικών δίσκων (CD-R).

Η δεκαετία του ’90 μας αφήνει με μια τεράστια αγωνία για τα υπολογιστικά συστήματα του πλανήτη τα οποία διακυβεύουν την ασφάλεια ολόκληρης της Γης. Ο «ιός του 2000» (millennium bug), σύμφωνα με τον οποίο θα σταματούσε η λειτουργία των περισσοτέρων υπολογιστικών συστημάτων, τελικά μάλλον προκάλεσε πολύ περισσότερη αναστάτωση παρά συνέπειες και ζημιές. Όσες ζημιές, όμως, δεν προξένησε το συγκεκριμένο πρόβλημα μάλλον, παρά ιός, τις προξένησε ο πιο «ερωτικός» -μέχρι σήμερα- ιός, γνωστός με την ονομασία «I Love You Virus» ή «Love Bug», ο οποίος ταλαιπώρησε εκατομμύρια υπολογιστές σε ολόκληρο τον κόσμο.

Η καινούργια χιλιετηρίδα ξεκίνησε με την πρώτη διεθνή συνθήκη για το ηλεκτρονικό έγκλημα (Cyber Crime Convention 2001), την οποία προσυπέγραψε και η χώρα μας αλλά και με δύο πολύ καταστροφικούς ιούς (Code Red και Nimda6). Επίσης, οι φήμες για ένα παγκόσμιο σύστημα παρακολούθησης τηλεφωνικών συνομιλιών και μηνυμάτων ηλεκτρονικού ταχυδρομείου, από την κυβέρνηση των ΗΠΑ, (γνωστό με το κωδικό όνομα Carnivore) επιβεβαιώθηκαν από ορισμένους hackers οι οποίοι δημοσίευσαν απόρρητα έγγραφα της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ (National Security Agency – NSA). Κάτι ανάλογο έγινε και στην Ευρώπη, με το γνωστό πλέον -σε πολλούς - σύστημα παρακολούθησης Echelon.

Τέλος, τα δραματικά γεγονότα της 11ης Σεπτεμβρίου έμελλε να επηρεάσουν στα μέγιστα τις εξελίξεις σε όλα τα μήκη και πλάτη του πλανήτη. Σύσσωμος ο δυτικός κόσμος παραδέχθηκε πως οι τρομοκράτες χρησιμοποίησαν κρυπτογραφικές μεθόδους για να ανταλλάξουν πληροφορίες μεταξύ τους χωρίς να γίνονται αντιληπτοί, αλλά και ότι εισέβαλαν σε πολλά συστήματα των ΗΠΑ με σκοπό να αποκομίσουν πολύτιμες μυστικές πληροφορίες. Η ημερομηνία αυτή μάλλον θα είναι και η αρχή μιας σειράς εξελίξεων και στην ασφάλεια των πληροφοριών.

ΚΕΦΑΛΑΙΟ 2:

ΚΕΦΑΛΑΙΟ 2: ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΟΙ ΔΙΑΦΟΡΕΤΙΚΕΣ ΠΤΥΧΕΣ ΤΟΥ

2.1 Ορισμός Διαδικτύου (Web)

Το Διαδίκτυο (αγγλ. Internet) είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια χρήστες καθημερινά σε ολόκληρο τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται Διαδίκτυο.

2.2 Η τεχνολογία του Διαδικτύου

Το Διαδίκτυο είναι ένα επικοινωνιακό δίκτυο που επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου υπολογιστή. Η τεχνολογία του είναι κυρίως βασισμένη στην διασύνδεση επιμέρους δικτύων ανά τον κόσμο και σε πολυάριθμα πρωτόκολλα επικοινωνίας. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη μορφή του, με τον όρο Διαδίκτυο περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του. Το Διαδίκτυο χρησιμοποιεί "μεταγωγή πακέτων" και τη "στοίβα πρωτοκόλλων". Σήμερα, ο όρος διαδίκτυο κατέληξε στο να αναφέρεται στο παγκόσμιο αυτό δίκτυο. Για να ξεχωρίζει, το παγκόσμιο αυτό δίκτυο γράφεται με κεφαλαίο το αρχικό "Δ". Η τεχνική της διασύνδεσης δικτύων μέσω μεταγωγής πακέτων και της στοίβας πρωτοκόλλων ονομάζεται "Διαδικτύωση".

2.3 Η ιστορία του Διαδικτύου

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Η Σοβιετική Ένωση είχε ήδη στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1 κάνοντας τους Αμερικανούς να φοβούνται όλο και περισσότερο για την

ασφάλεια της χώρας τους. Θέλοντας λοιπόν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Ρώσων δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ARPA (Advanced Research Projects Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση.

Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ. Λικλάιντερ (J.C.R. Licklider) που ανέφερε σε συγγράμματά του το "γαλαξιακό δίκτυο". Η θεωρία αυτή υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο έτσι ώστε ακόμη κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Την λύση σε αυτό έδωσε ο Πολ Μπάραν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλάινροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο.

Στηριζόμενο λοιπόν σε αυτές τις τρεις θεωρίες δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 με 4 κόμβους μέσω των οποίων συνδέονται 4 μίνι υπολογιστές (mini computers 12k): του πανεπιστημίου της Καλιφόρνια στην Σάντα Μπάρμπαρα του πανεπιστημίου της Καλιφόρνια στο Λος Άντζελες, το SRI στο Στάνφορντ και το πανεπιστήμιο της Γιούτα. Η ταχύτητα του δικτύου έφθανε τα 50 kbps και έτσι επιτεύχθηκε η πρώτη dial up σύνδεση μέσω γραμμών τηλεφώνου. Μέχρι το 1972 οι συνδεδεμένοι στο ARPANET υπολογιστές έχουν φτάσει τους 23, οπότε και εφαρμόζεται για πρώτη φορά το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail).

Παράλληλα δημιουργήθηκαν και άλλα δίκτυα, τα οποία χρησιμοποιούσαν διαφορετικά πρωτόκολλα(όπως το x.25 και το UUCP) τα οποία συνδέονταν με το ARPANET. Το πρωτόκολλο που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους υπολογιστών. Έτσι, δημιουργήθηκε η ανάγκη στις αρχές του 1970 για ένα πρωτόκολλο που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε. Το 1974 λοιπόν, δημοσιεύεται η μελέτη των Βιντ Σερφ (Vint Cerf) και Μπομπ Κάαν (Bob Kahn) από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol) που αργότερα το 1978 έγινε TCP/IP,

προσετέθη δηλαδή το Internet Protocol (IP), ώσπου το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET.

Το 1984 υλοποιείται το πρώτο DNS (Domain Name System) σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών. Ένα ακόμη σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο δημιούργησε την πρώτη διαδικτυακή πανεπιστημιακή ραχοκοκκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet.

Ο όρος Διαδίκτυο/Ίντερνετ ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το ARPANET με το NSFNet και Internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε TCP/IP. Η μεγάλη άνθιση του Διαδικτύου όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Τιμ Μπέρνερς-Λι στο ερευνητικό ίδρυμα CERN το 1989, ο οποίος είναι στην ουσία, η "πλατφόρμα", η οποία κάνει εύκολη την πρόσβαση στο Ίντερνετ, ακόμη και στη μορφή που είναι γνωστό σήμερα.

2.4 Επιφανειακός Ιστός (Surface Web)

Ο Επιφανειακός Ιστός (επίσης γνωστός και ως Surface Web, Surface Net, ορατός ιστός, Clearnet, καταλογοποιημένος ιστός, καταλογοποιήσιμος ιστός ή Lightnet) αντιπροσωπεύει εκείνο το τμήμα του παγκόσμιου ιστού που είναι διαθέσιμο στο κοινό, αναζητήσιμο με κοινές μηχανές αναζήτησης. Είναι το αντίθετο του βαθέος ιστού.

Σύμφωνα με μία πηγή στις 14/06/2015 ο κατάλογος της Google για τον ιστό επιφανείας περιείχε 14,5 δις σελίδες.

2.5 Βαθύς Ιστός (Deep Web)

Ο Βαθύς Ιστός (επίσης γνωστός και ως Deep Web, Deepnet, Undernet, το αόρατο Web ή το κρυμμένο Web), αναφέρεται στο περιεχόμενο του World Wide Web που δεν ανήκει στον Επιφανειακό Ιστό (Surface Web), το οποίο ευρετηριάζεται από μία συνηθισμένη μηχανή αναζήτησης.

Ο Mike Bergman, ιδρυτής του BrightPlanet, που επινόησε την φράση, είχε πει πως το να ψάχνει κανείς στο Internet σήμερα είναι σαν να σέρνει ένα δίχτυ στην επιφάνεια του ωκεανού: πολλά μπορεί να πιαστούν στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκονται βαθιά και επομένως δεν μπορούν να πιαστούν. Οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες, και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Οι παραδοσιακές μηχανές αναζήτησης δεν μπορούν να ανακτήσουν το περιεχόμενο του Deep Web. Αυτές οι σελίδες δεν υπάρχουν μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Το Deep Web είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό Web.

Μέγεθος του Deep Web:

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο της Καλιφόρνιας, Μπέρκλεϋ (University of California, Berkeley) το 2001, το Deep Web αποτελούταν περίπου από 91.000 terabytes. Αντίθετα με τον επιφανειακό Web (που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης) να είναι περίπου στα 167 terabytes. Η Βιβλιοθήκη του Κογκρέσου, υπολογίστηκε πως το 1997 είχε 3.000 terabytes. Το 2011, το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200 εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes. Ο υπολογισμός του μεγέθους του Web διαφέρει από πηγή σε πηγή και έτσι υπάρχει ένα μεγάλο περιθώριο λάθους και κανένας αριθμός δε μπορεί να θεωρηθεί ως ακριβής. Ωστόσο σχετικά με τον αριθμό των πηγών του deep Web υπάρχουν πιο ακριβείς εκτιμήσεις: Το 2004 ο He ανακάλυψε 300.000 Deep Web sites σε ολόκληρο το Web, και σύμφωνα με τον Shestakov, περίπου 14.000 deep web sites υπήρχαν στο Ρώσικο τμήμα του Web το 2006.

Πληροφορίες του Deep Web:

Οι πληροφορίες του Deep Web ανήκουν σε μία ή περισσότερες από τις παρακάτω κατηγορίες:

1. Δυναμικά παραγόμενο περιεχόμενο: δυναμικές ιστοσελίδες οι οποίες δημιουργούνται ως αποτέλεσμα της εκτέλεσης κάποιας επερώτησης (query) ή προσπελαύνονται μόνο μέσω κάποιας φόρμας.

2. Μη συνδεδεμένο περιεχόμενο: ιστοσελίδες οι οποίες δεν περιέχουν συνδέσμους από άλλες ιστοσελίδες, εμποδίζοντας έτσι τα προγράμματα που κάνουν Web Crawling να επισκεφθούν το περιεχόμενό τους.

3. Ιδιωτικό Web: ιστότοποι που απαιτούν εγγραφή (registration) και κωδικό πρόσβασης.

4. Περιεχόμενο περιορισμένης πρόσβασης: ιστότοποι που περιορίζουν την πρόσβαση στις σελίδες τους με τεχνικό τρόπο (π.χ. χρησιμοποιώντας το Robots Exclusion Standard, CAPTCHAs, ή το no-cache Pragma στις επικεφαλίδες του πρωτοκόλλου HTTP, τα οποία απαγορεύουν στις μηχανές αναζήτησης να πλοηγούνται στις ιστοσελίδες τους).

5. Περιεχόμενο που δεν είναι σε μορφή HTML: κείμενα που συμπεριλαμβάνονται σε multimedia αρχεία (εικόνες ή video) ή που έχουν συγκεκριμένη μορφή την οποία δεν μπορούν να χειριστούν οι μηχανές αναζήτησης.

6. Κείμενα που χρησιμοποιούν το παλαιότερο πρωτόκολλο Gopher και αρχεία που βρίσκονται σε διακομιστές FTP και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης. Οι μηχανές αναζήτησης όπως η Google δεν δεικτοδοτούν ιστοσελίδες που βρίσκονται έξω από το πρωτόκολλο HTTP.

Προσπέλαση:

Οι μηχανές αναζήτησης ανακαλύπτουν περιεχόμενο στο Web, χρησιμοποιώντας Web Crawlers που ακολουθούν συνδέσμους. Αυτή η τεχνική είναι ιδανική για να ανακαλύψει κανείς πληροφορίες στο Επιφανειακό Web (Surface Web) αλλά είναι αναποτελεσματική στην εύρεση πληροφοριών από το Deep Web. Για παράδειγμα, αυτοί οι Crawlers δεν προσπαθούν να βρουν δυναμικές ιστοσελίδες που προέρχονται από ερωτήματα σε βάσεις δεδομένων επειδή τα ερωτήματα αυτά θα ήταν θεωρητικά άπειρα.

Το 2005, η Yahoo! έκανε ένα μικρό κομμάτι του Deep Web ερευνήσιμο με τη χρήση των Yahoo! Subscriptions. Αυτή η μηχανή αναζήτησης ψάχνει μόνο μέσω λίγων συνδρομητικών ιστοτόπων. Κάποιοι τέτοιοι ιστότοποι εμφανίζουν όλο τους το περιεχόμενο στα robots των μηχανών αναζήτησης, έτσι ώστε να εμφανίζονται στις αναζητήσεις των χρηστών, αλλά μετά εμφανίζουν στους χρήστες μία σελίδα για login ή συνδρομή.

2.6 Σκοτεινός Ιστός (Dark Web)

Ο Σκοτεινός Ιστός (Dark Web όπως είναι ευρέως γνωστός) είναι ένας ανώνυμος διαδικτυακός ιστός, στον οποίο σκιώδεις χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες. Μπορεί να χρησιμοποιηθεί είτε για θετικούς είτε για αρνητικούς σκοπούς. Αποτελείται από τα αποκαλούμενα σκοτεινά δίκτυα ή darknet, συνήθως δίκτυα επικάλυψης, που προσεγγίζονται

με συγκεκριμένο λογισμικό και άδειες συχνής χρήσης πρωτοκόλλων και θυρών που απαντώνται σε μη τυποποιημένες επικοινωνίες. Χαρακτηριστικοί τύποι σκοτεινών δικτύων είναι τα δίκτυα F2F , που χρησιμοποιούνται για ανταλλαγές αρχείων με σύνδεση peer-to-peer.

Χαρακτηριστικά του Dark Web:

Το Διαδίκτυο λειτουργεί ως ιδανική μέθοδος ενημέρωσης και προπαγάνδας. Η διάδοση της επικοινωνίας μέσω υπολογιστή προσφέρει ένα γρήγορο, φθηνό σχετικά και ανώνυμο μέσο επικοινωνίας για πολιτικούς και κοινωνικούς ακτιβιστές αφενός, για ομάδες που δραστηριοποιούνται σε διάφορους τομείς του κοινού εγκλήματος αφετέρου. Αυτή η προβληματική πτυχή του Διαδικτύου συχνά αναφέρεται ως Dark Web ή Σκοτεινός Ιστός.

Χαρακτηριστικό στοιχείο του Dark Web είναι διάφορα fora ή σκοτεινά δίκτυα κρυμμένα βαθιά στο διαδίκτυο που φιλοξενούν ακραίες απόψεις και συμπεριφορές. Αρκετοί ερευνητές θεωρούν πως υπάρχει ανάγκη για συλλογή και ανάλυση των σκοτεινών δικτύων του Παγκόσμιου Ιστού, καθώς η παρουσία τους σηματοδοτεί ενίοτε σημαντικές συνέπειες σε ό,τι αφορά στην ασφάλεια της πληροφορικής που σχετίζεται με διάφορες εφαρμογές. Η συλλογή των εν λόγω περιεχομένων φέρεται ότι είναι σημαντική για την μελέτη και την κατανόηση των διαφόρων κοινωνικών και πολιτικών απόψεων που υπάρχουν στις διαδικτυακές κοινότητες, αλλά και για τον επιδιωκόμενο έλεγχό τους από διάφορους κυβερνητικούς και μη, οργανισμούς και φορείς.

Άλλο χαρακτηριστικό γνώρισμα του σκοτεινού διαδικτύου είναι και τα δίκτυα ανωνυμίας, όπως το Tor, που λειτουργεί μέσω μιας σειράς ανώνυμων συνδέσεων. Το Tor είναι ουσιαστικά μηχανισμός δρομολόγησης, που σχεδιάστηκε για τη διατήρηση της ανωνυμίας του χρήστη του διαδικτύου, δημιουργώντας εναλλακτικά μονοπάτια για τη δρομολόγηση της κυκλοφορίας. Ο μηχανισμός που χρησιμοποιεί το Tor ονομάζεται onion routing (δρομολόγηση κρεμμύδι) και δημιουργήθηκε για πρώτη φορά από το Εργαστήριο Ναυτικών Ερευνών των ΗΠΑ.

Διαφορές Deep και Dark Web:

Το Deep Web συντίθεται από ιστοσελίδες προσβάσιμες μεν στο κοινό του Διαδικτύου, αλλά όχι μέσω των μηχανών αναζήτησης, όπως είναι για παράδειγμα η Google. Οι μηχανές αναζήτησης ανιχνεύουν το διαδίκτυο χρησιμοποιώντας στην αναζήτησή τους bots (spiders, crawlers) που καταλογογραφούν δεδομένα, χρησιμοποιώντας αρχεία robots.txt ως οδηγούς, που τα κατευθύνουν τι είδους στοιχεία να ευρετηριάσουν, υπό την Οδηγία Αποκλεισμού Ρομπότ του 1994.

Το διαδικτυακό ρομπότ (αράχνη, μποτ κ.ά.) δεν μπορεί να ευρετηριάσει βαθύ περιεχόμενο στον Παγκόσμιο Ιστό. Συνήθως τέτοιο υλικό είναι προσβάσιμο μόνο όταν ένας χρήστης αναζητά μια συγκεκριμένη βάση δεδομένων, πράγμα που σημαίνει ότι δεν υπάρχει διαθέσιμος φανερός σύνδεσμος.

Το σκοτεινό διαδίκτυο, από την άλλη, είναι συχνά διαθέσιμο στο κοινό –απλά πρέπει να γνωρίζει κανείς πώς να το βρει- γιατί υπάρχει σε ένα εναλλακτικό στρώμα του διαδικτύου. Αυτό το εναλλακτικό στρώμα συχνά κατασκευάζεται από κάποια κοινότητα, που θέλει να διατηρήσει την ανωνυμία, την αυτονομία ή πιθανώς την ιδεολογία της.

Τέτοιες κοινότητες είναι δυνατόν να χρησιμοποιήσουν το σκοτεινό διαδίκτυο για ποικίλες δραστηριότητες θετικές ή αρνητικές. Το σκοτεινό διαδίκτυο έχει χρησιμοποιηθεί για εγκληματικές δραστηριότητες, όπως η διανομή υλικού παιδικής πορνογραφίας, το hacking, το ξέπλυμα βρώμικου χρήματος και οι πωλήσεις όπλων και ναρκωτικών.

Ωστόσο, έχει επίσης χρησιμοποιηθεί ως εργαλείο βοήθειας πολιτών, προκειμένου να αποφύγουν μέτρα λογοκρισίας που εφαρμόζονται από διάφορα καθεστώτα, όπως η Κίνα πιθανώς κατά την περίοδο των Ολυμπιακών Αγώνων.

Η περίπτωση Silk Road:

Η ανωνυμία κάνει εξαιρετικά δύσκολη την επιβολή του νόμου σε όσους χρησιμοποιούν το σκοτεινό διαδίκτυο ή domain.onion, όπως το Hidden Wiki, για παράνομους σκοπούς. Ίσως η διασημότερη περίπτωση εκμετάλλευσης του σκοτεινού διαδικτύου ήταν το Silk Road, ιστοσελίδα μαύρης αγοράς για προμηθευτές και πελάτες παράνομων εμπορευμάτων και υπηρεσιών, συμπεριλαμβανομένων ναρκωτικών και εκτελεστών προς ενοικίαση. Το Silk Road, που ιδρύθηκε το 2011, διαχειριζόταν ο Ross William Ulbricht, πολίτης των ΗΠΑ, ο οποίος φέρεται ότι είχε έσοδα εκατοντάδων εκατομμυρίων δολαρίων.

ΚΕΦΑΛΑΙΟ 3:

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 Ορισμός του ηλεκτρονικού εγκλήματος

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. 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 crimes) και σε Κυβερνοεγκλήματα (cyber crimes), εάν τελέσθηκε μέσω του Διαδικτύου.

Ως παραδείγματα εγκλημάτων που τελούνται με την χρήση Η/Υ (computer crimes) η ελληνική νομοθεσία ορίζει την παράνομη αντιγραφή απόρρητων δεδομένων, την παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ και την απάτη. Στο βαθμό που τα εγκλήματα αυτά διαπράτονται και σε περιβάλλον διαδικτύου (κυβερνοεγκλήματα), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

3.2 Χαρακτηριστικά γνωρίσματα του ηλεκτρονικού εγκλήματος

Το Ηλεκτρονικό Έγκλημα, ανεξάρτητα από το εάν προσεγγιστεί από την στενή ή την ευρεία έννοια του, εμπεριέχει ορισμένα χαρακτηριστικά γνωρίσματα που το διαχωρίζουν από το παραδοσιακό έγκλημα.

Τέτοια σημεία είναι τα εξής :

1. Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε πραγματικό χρόνο, ακόμα και σε δευτερόλεπτα, και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

2. Είναι εύκολο στη διάπραξή του για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
3. Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις.

4. Οι κυβερνο-εγκληματίες πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλοντας ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.

5. Μπορεί να διαπραχθεί από οποιοδήποτε μέρος, καθώς δεν απαιτείται η μετακίνηση του δράστη, και τα αποτελέσματά του μπορούν να γίνονται ταυτόχρονα αισθητά σε πολλούς

στόχους ανεξαρτήτου εδαφικού περιορισμού. Για αυτό, άλλωστε, και το αποκαλούν «έγκλημα χωρίς πατρίδα».

6. Ο εντοπισμός ενός ψηφιακού εγκληματία, κατά κανόνα, είναι πολύ δύσκολος (αλλά όχι ακατόρθωτος) να προσδιοριστεί καθώς επίσης και ο (πραγματικός) τόπος τέλεσής του και αυτό γιατί μπορεί ο δράστης να εντοπιστεί σε ένα συγκεκριμένο τόπο, τα αποδεικτικά στοιχεία, όμως, να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

7. Καθώς ο κίνδυνος ανακάλυψης του ηλεκτρονικού δράστη είναι μικρός, το ηλεκτρονικό έγκλημα αποδίδει μεγάλα κέρδη.

8. Ο αριθμός των θυμάτων τους σε σύγκριση με εκείνων των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

9. Οι οικονομικές απώλειες που προξενούνται στα «ψηφιακά» εγκλήματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.

10. Καθώς για την διάπραξή του δεν απαιτείται φυσική μετακίνηση του δράστη, δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες, όπως για παράδειγμα παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται μαζί στις ίδιες ομάδες συζήτηση (π.χ. Newsgroups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (π.χ. Internet Relay Chat).

11. Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα γιατί ελάχιστες περιπτώσεις κυβερνο-εγκλημάτων καταγγέλλονται διεθνώς με άμεση συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του διαδικτύου να χαρακτηρίζεται ακόμα πιο «σκοτεινό» από ότι το έγκλημα του πραγματικού κόσμου.

12. Η αστυνομική διερεύνηση του είναι πολύ δύσκολη και απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

13. Οι οποίες εξειδικευμένες γνώσεις απαιτούνται και σε όσους, εκτός αστυνομίας, ασχολούνται με τη συγκεκριμένη μορφή εγκλήματος, όπως είναι οι εισαγγελείς, οι δικαστές, και οι δικηγόροι.

14. Για την διερεύνησή του ηλεκτρονικού εγκλήματος απαιτείται συνεργασία τουλάχιστον δύο κρατών: του κράτους που γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.

3.3 Μορφές ηλεκτρονικού εγκλήματος

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με την συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για αυτό το λόγο ρυθμίζονται και τιμωρούνται ξεχωριστά από άλλα ειδικότερα νομοθετήματα τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση και στο εξωτερικό γενικότερα. Ειδικότερα, θα αναφέρουμε και θα αναλύσουμε τις εξής μορφές: Κυβερνοσφετερισμός, Spamming, Η Χωρίς Νόμιμη Εξουσιοδότηση Είσοδος σε Η/Υ (hacking ή cracking), Διασπορά Κακόβουλων Προγραμμάτων, Τηλεχειρισμός (Κατασκοπεία) του Υπολογιστή, τα Cookies, Υποκλοπή αρχείων Η/Υ, Πειρατεία Λογισμικού, Πλαστογραφία, Διακίνηση ναρκωτικών - Εμπόριο οργάνων – Αυτοκτονία, Κυβερνοπόλεμος – Κυβερνοτρομοκρατία και Παιδική πορνογραφία. Παρακάτω θα γίνει ανάλυση για τους παραπάνω ορισμούς.

3.4 Συνέπειες του ηλεκτρονικού εγκλήματος για τον καταναλωτή

Οι δυσμενείς κοινωνικές και οικονομικές συνέπειες του ηλεκτρονικού εγκλήματος είναι πολλαπλές για τους πολίτες, ιδιαίτερα για τους ανηλίκους. Καθημερινά σχεδόν γίνεται λόγος στα ελληνικά και διεθνή ΜΜΕ για περιπτώσεις σεξουαλικής εκμετάλλευσης παιδιών και εφήβων που προσελκύονται μέσω φόρουμ συζήτησης του διαδικτύου και καταλήγουν να υφίστανται σοβαρές προσβολές της προσωπικότητας, της τιμής, της γενετήσιας αξιοπρέπειας, ακόμα και της ζωής τους.

Η παρότρυνση των καταναλωτών, μέσω παραπλανητικών διαφημίσεων και απαγορευμένων εμπορικών πρακτικών, ήτοι αποστολής, χωρίς τη συναίνεση του χρήστη, ανεπιθύμητων μηνυμάτων (γνωστών ως spam) να αγοράσουν άγνωστης προέλευσης, διατροφικής αξίας και αμφίβολης ποιότητας προϊόντων και υπηρεσιών, μπορεί να βλάψει την υγεία, την ασφάλεια και τα οικονομικά συμφέροντα των καταναλωτών.

Η αθέμιτη πρόσβαση τρίτων εισβολέων σε κωδικούς τραπεζικών λογαριασμών μέσω web banking συνεπάγεται την υπεξαίρεση των ποσών των καταθέσεων και τη μεταφορά αποταμιευτικών κεφαλαίων του καταναλωτή σε τράπεζες του εξωτερικού και στη συνέχεια στις τσέπες των εγκληματιών.

Η υποκλοπή μέσω διαδικτύου στοιχείων πιστωτικών καρτών των γονέων παιδιών και εφήβων έχει ως συνέπεια την αθέμιτη χρέωση των γονέων, της οποίας όμως οι γονείς ανακαλύπτουν πολύ αργότερα μαζί με τον εκκαθαριστικό τους λογαριασμό που λαμβάνουν από την τράπεζα.

Είναι γεγονός ότι ο κάτοχος της κάρτας, βάσει της νομοθεσίας, μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας. Συνεπώς, σε περίπτωση online συναλλαγής με κλεμμένα στοιχεία καρτών, ο νόμιμος κάτοχος μπορεί να αρνηθεί την καταβολή του αντίτιμου, οπότε η τράπεζα κανονικά δεν θα καταβάλει το ποσό στον πωλητή αλλά κανονικά θα χρεώσει το κατάστημα με τα έξοδα ακύρωσης της συναλλαγής.

Η συλλογή στοιχείων επικοινωνίας και προσωπικών δεδομένων των χρηστών, τα οποία χρησιμοποιούνται συχνά χωρίς τη συναίνεση των υποκειμένων, είτε από τους ίδιους τους προμηθευτές είτε διαβιβάζονται έναντι αντίτιμου σε τρίτους για προωθητικές ενέργειες μέσω αποστολής μαζικών SMS και MMS, έρευνες αγοράς, direct marketing, απαγορεύεται από τη νομοθεσία καθότι προσβάλλει την ιδιωτική ζωή του ατόμου.

ΚΕΦΑΛΑΙΟ 4:

ΕΠΙΚΙΝΔΥΝΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΜΕΡΟΣ 1

4.1 Η μη νόμιμη εξουσιοδοτημένη είσοδος σε Η/Υ (Hacking & Cracking)

Η μορφή αυτή του Ηλεκτρονικού Εγκλήματος έχει να κάνει με την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα, με παράνομους σκοπούς. Αυτούς τους «εγκληματίες του Κυβερνοχώρου» μπορούμε να τους διακρίνουμε σε δύο κατηγορίες ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα: στους hackers και στους crackers (criminal hackers).

4.2 Ορισμοί Hacking & Cracking

Με τον όρο hacker χαρακτηρίζεται το άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές αλλά και προχωρημένες γνώσεις προγραμματισμού, μπορεί να εντοπίσει αδυναμίες σε συστήματα υπολογιστών, να λύνει τεχνικά προβλήματα, να βελτιώνει εφαρμογές αλλά και να συνεργάζεται μ' άλλους όμοιους του για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά.»

Ο ορός Hacking αναφέρεται στις καταστροφές δικτύων υπολογιστών με προώθηση ιών, με «σπάσιμο» μυστικών κωδικών, με τρομοκρατία στο ίντερνετ. Με τον όρο αυτό αναφερόμαστε στον τρόπο που κάποιος ασχολείται φανατικά με τους ηλεκτρονικούς υπολογιστές σκορπώντας την καταστροφή.

Στόχος των crackers είναι η πρόκληση ζημιάς σε δίκτυα υπολογιστών, η εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, η δημιουργία ιών, η παραβίαση κωδικών ασφαλείας, η καταστροφή ή και η αλλοίωση διαφόρων sites, η δημιουργία πειρατικών αντιγράφων προγραμμάτων, τραγουδιών ή και βίντεο.

Για τους λόγους αυτούς μπορούν πολύ εύκολα να καταστρέψουν ολόκληρα συστήματα υπολογιστών απλά και μόνο για να κάνουν το κέφι τους, όταν βρουν βέβαια την κατάλληλη ευκαιρία. Είναι συνήθως άτομα με έντονη ανάγκη για επίδειξη και αφήνουν περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους μετά από κάθε εγκληματική τους πράξη. Γενικά διεισδύουν σε συστήματα και προκαλούν ζημιές και έτσι έχουν κατακτήσει μια θέση στον χώρο του εγκλήματος.

4.3 Είδη και εργαλεία επιθέσεων

Αρχικά θα κάνουμε μία επιγραμματική αναφορά στους κυριότερους τρόπους με τους οποίους εκδηλώνεται παρανόμως η δράση των hackers και με ποιο σκοπό.

1. Απόκτηση πρόσβασης σε ένα σύστημα υπολογιστή/ών με το «σπάσιμο» του κωδικού πρόσβασης.

2. Καταστροφή - διαγραφή στοιχείων και κλοπή εμπιστευτικών αρχείων και πληροφοριών.

3. Απόκτηση ελέγχου συστήματος και μεταβολή δεδομένων πρόσβασης με σκοπό τον αποκλεισμό χρηστών.

4. Χρησιμοποίηση – διαχείριση ενός συστήματος υπολογιστή/ων για αποστολή δεδομένων σε τρίτο σύστημα.

5. Παρεμπόδιση ομαλής λειτουργίας συστήματος με την επιβολή πρόσθετων εργασιών ή με την υπερφόρτωση με υπερβολικές ποσότητες δεδομένων.

Μετά από αυτή την απαρίθμηση σκόπιμο θα ήταν να διερευνήσουμε και τους τρόπους και τα μέσα που χρησιμοποιούν οι hackers για να επιτύχουν αυτούς τους στόχους.

1. Denial of service (DoS attack): οι hackers τρέχουν πολλαπλά προγράμματα με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών τα οποία βομβαρδίζουν το δίκτυο με δεδομένα και έτσι το υπερφορτώνουν ώστε να αδυνατεί να ανταποκριθεί.

2. Distributed denial of service (DDoS attack): Οι hackers με τη χρήση δουρείων ίππων αποκτούν τον έλεγχο πολλών υπολογιστών ανυποψίαστων χρηστών. Σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο και φυσικά μετά από την υπερβολική ζήτηση που αντιμετωπίζει, καταρρέει.

3. DNS Spoofing: Στην περίπτωση αυτή ο hacker τροποποιεί το Domain Name Code το οποίο είναι η αριθμητική, δυαδικά ψηφιοποιημένη διεύθυνση του site, έτσι ώστε να την αντιλαμβάνεται και ο υπολογιστής και να ανταποκρίνεται στην εντολή. Οπότε οι χρήστες ζητώντας μία ιστοσελίδα με αλλοιωμένη την αριθμητική της διεύθυνση (numerical address), θα βρεθούν σε άλλη ιστοσελίδα αυτόματα. Αυτο μπορεί να σημαίνει απώλεια εσόδων για την ιστοσελίδα που δεν κατόρθωσε να επισκεφθεί ο χρήστης τελικά αλλά και με τη δημιουργία ενός ακριβούς αντιγράφου κάποιας ιστοσελίδας (mirror site) να εκμαιεύσει ο hacker ευαίσθητα προσωπικά δεδομένα που ο χρήστης πιστεύει ότι δίνει στην αληθινή ιστοσελίδα που ζήτησε.

4. Packet Sniffers: στην ουσία είναι προγράμματα που επιτρέπουν στο χρήστη να προσλαμβάνει και να ερμηνεύει πακέτα πληροφοριών που διακινούνται στο διαδίκτυο. Κάθε πληροφορία που κοινοποιείται σε ένα δίκτυο υπολογιστών (όνομα χρήστη, κωδικός εισόδου, e-mail κλπ.) μεταφράζεται σε πακέτα, τα οποία στέλνονται στο δίκτυο. Το Internet λειτουργεί κυρίως με το Ethernet πρωτόκολλο μετάδοσης. Όταν λοιπόν κάποιος στείλει ένα πακέτο στο Ethernet, κάθε μηχάνημα στο δίκτυο βλέπει το πακέτο. Κάθε πακέτο που αποστέλλεται μέσω διαδικτύου έχει μία Ethernet κεφαλή-μία αριθμητική διεύθυνση, ώστε να είναι βέβαιο ότι η σωστή μηχανή παίρνει τη σωστή πληροφορία. Κάθε μηχάνημα υποτίθεται ότι εντοπίζει τα πακέτα δεδομένων με τη δική της διεύθυνση. Όμως το Ethernet packet sniffer είναι λογισμικό που επιτρέπει στον hacker ή τον διαχειριστή του δικτύου κανονικά να υποκλέπτει πληροφορίες, οι οποίες δεν προορίζονται για τη διεύθυνσή του.

5. Δούρειοι Ίπποι: Τα προγράμματα αυτά είναι κερκόπορτες σε ένα σύστημα υπολογιστή. Ο hacker μεταμφιέζει τον ίππο σε ένα άλλο πρόγραμμα, όπως για παράδειγμα σε ένα παιχνίδι, ώστε να ξεγελαστεί ο χρήστης και να κατεβάσει και να εγκαταστήσει το πρόγραμμα. Μόλις ο ίππος εγκατασταθεί στον υπολογιστή του θύματος, ο hacker αποκτά πρόσβαση στο σκληρό δίσκο ή στο e-mail του χρήστη. Κρύβοντας προγράμματα ώστε να τρέξουν αργότερα ο hacker μπορεί να αποκτήσει πρόσβαση και σε άλλα συστήματα ή και να πραγματοποιήσει DDoS επιθέσεις. Ο απλούστερος ίππος αντικαθιστά τα μηνύματα που εμφανίζονται όταν ζητείται ένα συνθηματικό από τον χρήστη. Οι χρήστες παρέχουν τα ονόματα χρήστη και κωδικούς πρόσβασης τους θεωρώντας ότι συνδέονται στο σύστημα, ενώ στην ουσία αυτά καταγράφονται από τον ίππο προς χρήση του hacker. Ο διασημότερος ίππος είναι ο Black Orifice που δημιουργήθηκε από το hacker group: Cult of the Dead Cow και που προσφέρει πρόσβαση και έλεγχο σε κάθε προσωπικό υπολογιστή που λειτουργεί με το λειτουργικό σύστημα Windows 95/98 και επόμενα, εκμεταλλευόμενο ένα ελάττωμα σε ένα πρόγραμμα για αποστολή e-mail.

6. Ιοί και σκουλήκια: Τα σκουλήκια και οι ιοί είναι αυτο-αναπαραγόμενα προγράμματα, τα οποία μπορούν να εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο. Συνήθως οδηγούν στην καταστροφή και δυσλειτουργία συστημάτων και αρχείων. Τα σκουλήκια αντιγράφονται από υπολογιστή σε υπολογιστή χωρίς να απαιτούν τη συμβολή κανενός άλλου προγράμματος ή αρχείου. Το διασημότερο σκουλήκι ILOVEYOU υπολογίζεται ότι επηρέασε περίπου 45 εκατ. Υπολογιστές.

4.4 Spamming

Με τον όρο spam εννοούμε την απρόκλητη, εμπορική και μαζική αποστολή μεγάλου αριθμού ηλεκτρονικών μηνυμάτων, τα οποία απευθύνονται σε ένα σύνολο χρηστών του διαδικτύου, χωρίς αυτοί να έχουν ζητήσει ή να επιθυμούν κάτι τέτοιο και χωρίς να έχουν συνειδητά προκαλέσει την επικοινωνία με τον αποστολέα των μηνυμάτων. Τα μηνύματα των spam e-mails είναι συνήθως ενημερωτικού ή διαφημιστικού περιεχομένου για προϊόντα και υπηρεσίες αμφίβολης ποιότητας. Οι εταιρείες που στέλνουν μαζικά διαφημιστικά e-mails αποκαλούνται spammers και μερικές από αυτές διακινούν το 90% των spam emails. Επίσης, έχουν την δυνατότητα να στείλουν εκατομμύρια e-mails με μια κίνηση ενώ οι εταιρείες που διαφημίζονται μέσω τέτοιων μηνυμάτων πληρώνουν βάσει συμφωνίας κάποια ποσά για κάθε παραγγελία που δέχονται.

4.5 Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό είναι ίσως ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του διαδικτύου. Η διασπορά του κακόβουλου κώδικα έχει σκοπό να διεισδύσει σε έναν ηλεκτρονικό υπολογιστή με σκοπό να του προκαλέσει ζημιά διαγράφοντας ή αλλοιώνοντας δεδομένα και προγράμματα, υποκλέπτοντας δεδομένα ή παρεμποδίζοντας τη λειτουργία ενός συστήματος.

Σύμφωνα με τον Sinrod ο κακόβουλος κώδικας διακρίνεται στους ιούς, στα σκουλήκια και στους δούρειους ίππους. Οι ιοί είναι ο πιο συνήθης κακόβουλος κώδικας. Ένας ιός δεν είναι τίποτα περισσότερο από ένα πρόγραμμα που τοποθετείται σε σημεία τέτοια ώστε να μην γίνεται αντιληπτός εκτελώντας την επίθεση του. Το πρόγραμμα αυτό είναι μια σειρά από εντολές που εκτελούν κακόβουλες ενέργειες σε έναν υπολογιστή. Σημαντικό είναι, όπως αναφέρθηκε και προηγουμένως, να εγκατασταθεί σε τέτοια θέση στον υπολογιστή – θύμα ώστε να μην γίνει αντιληπτό από τον χρηστή. Ο χρηστής επομένως άθελα του γίνεται φορέας του ιού που θα μεταδώσει με την σειρά του σε άλλον υπολογιστή. Έτσι επιδιώκεται η συνέχειά του ενώ παράλληλα προκαλεί ζημιές και αλλοιώσεις σε κάθε υπολογιστικό σύστημα.

Η ζημιά που κάνει ένας ιός μπορεί να κυμαίνεται από την εμφάνιση ενός ενοχλητικού μηνύματος στην οθόνη του υπολογιστή μέχρι και την διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολύνει. Ο συνηθέστερος τρόπος μόλυνσης ενός υπολογιστή είναι μέσω e-mail με απατηλά μηνύματα από έναν άγνωστο, τις περισσότερες φορές, αποστολέα που περιέχει ένα συνημμένο αρχείο με το πρόγραμμα του ιού, το οποίο εκτελείται αυτόματα και μολύνει τον υπολογιστή του χρήστη. Γνωστοί ιοί υπολογιστών που άφησαν εποχή είναι ο Melissa, ο Michelangelo, ο I Love You, ο Blaster κ.α.

Οι βασικότεροι ιοί είναι οι:

1. File-infectors ή Parasitic viruses: ο ιός αυτός ενεργεί μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο όποιο προσθέτουν το κακόβουλο κώδικα. Μολύνει αρχεία με επεκτάσεις .com, .exe, .sys, .old.

2. Boot Sector Virus: ο ιός αυτός προσβάλει εκτελέσιμο κώδικα συστήματος, τον οποίο εντοπίζει σε συσκευές βοηθητικής μνήμης, στον τομέα εκκίνησης ή στο MBR (Master Boot Record) του δίσκου. Ο Boot Sector Virus ενεργεί μολύνοντας κάθε δίσκο ή δισκέτα που θα χρησιμοποιηθεί από τον υπολογιστή.

3. Multi-partite viruses: Δρουν συνδυάζοντας επιμέρους χαρακτηριστικά των δύο παραπάνω κατηγοριών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία αλλά και τομείς εκκίνησης.

4. Companion viruses: ο ιός εκμεταλλεύεται μια ευπάθεια του λειτουργικού συστήματος DOS. Μεταδίδεται με αποσπώμενα αποθηκευτικά μέσα και πολλές φόρες το αρχείο αυτό παραμένει κρυφό στη μνήμη του υπολογιστή.

5. Ιοί Link και Flash Bios: οι Ιοί Link δε μολύνουν το πρόγραμμα αυτό καθ' αυτό αλλά δρουν τροποποιώντας το αρχείο FAT (File Allocation Table). Αυτό έχει ως αποτέλεσμα να αλλάζει ο σύνδεσμος που δείχνει προς ένα πρόγραμμα του υπολογιστή με τρόπο ώστε να «δείχνει» στο σημείο που βρίσκεται ο ιός και να εκτελείται αυτός αντί για το πρόγραμμα. Οι Flash Bios αντικαθιστούν το λογισμικό BIOS στην μητρική πλακέτα με απρόβλεπτες συνέπειες, όπως αδυναμία εκκίνησης του υπολογιστή.

6. Macro viruses: οι Ιοί αυτοί βρίσκονται σε αρχεία προγράμματος αυτοματισμού γραφείου. Τα σκουλήκια είναι παρόμοια με τους ιούς μονό που πολλαπλασιάζονται χωρίς κάποια συγκεκριμένη ενέργεια από τον χρηστή. Η διάδοσή τους γίνεται μέσω διαδικτύου χωρίς να χρειάζεται να επισυναφτούν σε κάποιο αρχείο. Αυτά μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία ενός υπολογιστή και στην συνέχεια στέλνουν αντίγραφα του εαυτού τους σε υποψήφια θύματα. 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.

7. Στην κατηγορία του κακόβουλου λογισμικού περιλαμβάνονται επίσης οι Δούρειοι ίπποι, Adware, Spyware, Dialers (Dialers είναι εκείνα τα προγράμματα που καλούν τηλεφωνικούς αριθμούς για την πρόσβαση σε ορισμένες υπηρεσίες υψηλής χρέωσης) οι λογικές και ωρολογιακές βόμβες, οι φάρσες και οι τεχνικές απόκρυψης ιών. Αναλυτικότερα, στον τρωικό

πόλεμο ο Οδυσσέας κατάφερε να εξαπατήσει τους Τρώες με τον Δούρειο Ίππο. Αυτό που έκανε ήταν να «δωρίσει» στους Τρώες τον Δούρειο Ίππο για να έχουν καλή τύχη. Οι Τρώες πέρασαν τον Ίππο μέσα από τα τείχη και τότε εμφανίστηκαν οι Έλληνες μέσα από αυτόν ξεκινώντας την άλωση της πόλης. Έτσι λοιπόν δίνουμε αυτή την ονομασία και στο κακόβουλο λογισμικό αφού κι αυτό φαινομενικά είναι ένα «αθώο» πρόγραμμα το όποιο κρύβει λειτουργίες που δεν είναι εύκολο να εντοπιστούν από το χρηστή. Τα προγράμματα αυτά φορτώνονται στο σκληρό δίσκο του υπολογιστή. Ο επιτιθέμενος με αυτό τον τρόπο καταφέρνει τον εξ' αποστάσεως έλεγχο του συστήματος και μπορεί έτσι να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή ακόμα και να εξαπολύσει άρνηση εξυπηρέτησης.

8. Τα Ad-ware και Spyware είναι προγράμματα που περιέχουν κακόβουλο κώδικα και θεωρούνται υποκατηγορία των Δούρειων Ίππων. Χρησιμοποιούνται για την διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων που προσφέρονται μέσω του διαδικτύου. Σε περίπτωση που η λειτουργία τους ορίζεται στους όρους χρήσης που αποδέχεται ο χρήστης, δεν χαρακτηρίζεται ως κακόβουλο λογισμικό. Τα Ad-ware και Spyware συνεργάζονται για τη δημιουργία προφίλ χρηστών με σκοπό την αποστολή στοχευμένων διαφημίσεων αλλά μπορούν να προκαλέσουν και ανεπιθύμητα αποτελέσματα όπως είναι η καταστροφή αρχείων, οι αποσυντονισμοί του συστήματος και η επιβράδυνση της περιήγησης στο διαδίκτυο και της εν γενεί λειτουργίας του υπολογιστή.

9. Όσον αφορά τους Dialers αποτελούν υποκατηγορία των Spyware. Είναι μικρά προγράμματα κι έχουν τη δυνατότητα να αποσυνδέουν την τηλεφωνική γραμμή από το internet και να συνδέονται με άλλες κλήσεις μεγαλύτερης χρέωσης. Επομένως το αποτέλεσμα αυτής της λειτουργίας είναι ο πλουτισμός συγκεκριμένων κατόχων δικτυακών τόπων από τα τεράστια αυτά ποσά. Οι dialers κρύβονται σε συγκεκριμένες ιστοσελίδες οι οποίες πιθανόν περιέχουν πειρατικό λογισμικό ή οποιοδήποτε άλλο αμφιλεγόμενο λογισμικό.

10. Η λογική βόμβα είναι ένα πρόγραμμα που ενεργοποιείται με ένα συγκεκριμένο γεγονός. Το πρόγραμμα αυτό μπορεί να σταματήσει την λειτουργία του υπολογιστή και να απελευθερώσει έναν ιό διαγράφοντας αρχεία και προκαλώντας γενικότερες ζημιές σε αυτόν. Το εν λόγω πρόγραμμα ενεργοποιείται είτε από τον χρηστή, είτε σε χρόνο και ημερομηνία που έχει εκ των προτέρων προγραμματισθεί, όπως συμβαίνει και με τις ωρολογιακές βόμβες.

11. Οι φάρσες ίσως να μην ανήκουν στο κακόβουλο λογισμικό αλλά είναι κακόβουλη η πρόθεση του επιτιθέμενου, αφού το μόνο που καταφέρνει είναι να προκαλέσει πανικό στον χρήστη προειδοποιώντας τον για έναν ιό που δεν υπάρχει. Ο χρήστης ωστόσο στην προσπάθεια του να προστατέψει τα δεδομένα του καταφεύγει στην διαγραφή αυτών.

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

4.6 Διακίνηση ναρκωτικών - Εμπόριο οργάνων – Αυτοκτονία

Η διακίνηση παράνομων ουσιών, το εμπόριο οργάνων ή ακόμα και παιδιών και η αυτοκτονία αποτελούν μορφές ηλεκτρονικού εγκλήματος οι οποίες έχουν παρατηρηθεί εντονότερα τα τελευταία χρόνια καθώς αποκτάται όλο και περισσότερη τεχνογνωσία μεταξύ των πληθυσμών. Μέσω διαφόρων sites ή ομάδων συζήτησης (newsgroups) γίνονται γνωριμίες μεταξύ των ανθρώπων που αναζητούν κάτι από τα παραπάνω και οι συναλλαγές τους γίνονται ηλεκτρονικά και μη. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση ενός ανήλικου μαθητή ο οποίος αυτοκτόνησε κάνοντας λήψη ενός πολύ τοξικού γεωργικού φαρμάκου αφού πρωτίστως είχε λάβει πληροφορίες σχετικά με το φάρμακο αυτό από έναν 25άχρονο που είχε γνωρίσει σε chat room. Μάλιστα, τα τελευταία χρόνια, όπως πληροφορούμαστε από τα αρμόδια όργανα της αστυνομίας, οι περιπτώσεις αυτοκτονίας και διακίνησης ναρκωτικών στο διαδίκτυο έχουν αυξηθεί κατά ένα πολύ μεγάλο ποσοστό από τα πρώτα χρόνια λειτουργίας του τμήματος (2000).

4.7 Κυβερνοσφετερισμός

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από την χρήση του Διαδικτύου με την επωνυμία τους.

Η προστασία των domain names παρέχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους τους. Αν την διαδικτυακή διεύθυνση αποτελεί ένα όνομα, τότε παρέχεται η προστασία των άρθρων 57 και 58 του ΑΚ. Αν πρόκειται για εμπορική επωνυμία, δηλαδή ένα όνομα με το οποίο ο έμπορος διεξάγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την προστασία

του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 1146/1914. Το άρθρο 13 του νόμου 1146/1914 εφαρμόζεται και όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων.

4.8 Κυβερνοπόλεμος – Κυβερνοτρομοκρατία

Ο Κυβερνοπόλεμος δεν αποτελεί απαραίτητα «θερμό επεισόδιο» αλλά περιλαμβάνει πολεμικές επιθέσεις ενάντια στο στρατιωτικό σώμα ενός έθνους, ένα παράδειγμα μιας τέτοιας επίθεσης μπορεί να είναι η διακοπή κρίσιμων τηλεπικοινωνιακών δίαυλων, και οι επιθέσεις ενάντια σε άμαχο πληθυσμό. Οι Κυβερνοεπιθέσεις έχουν ως στόχο την υποδομή, που αυτή αφορά τις πληροφορίες γενικότερα και τα αποτέλεσμα των οποίων μπορεί να είναι πιο επιζήμια για τις χώρες που διαθέτουν σημαντικές υποδομές δικτύων Η/Υ, ή δίκτυα κοινά σε όλους τους πολίτες ενός κράτους, όπως για παράδειγμα δίκτυα ενέργειας, μεταφορών, επικοινωνιών κ.τ.λ.

Η Κυβερνοτρομοκρατία είναι μια μορφή ηλεκτρονικού εγκλήματος, σύμφωνα με την οποία, χρησιμοποιείται ο κυβερνοχώρος για τη διάπραξη τρομοκρατικών ενεργειών. Παραδείγματα κυβερνοτρομοκρατίας αποτελούν η εισβολή σε υπολογιστικό σύστημα προκαλώντας τη διάλυση ενός εργοστασίου πυρηνικής ενέργειας, ή η καταστροφή του ηλεκτρονικού συστήματος ενός φράγματος, ή η σύγκρουση δύο αεροσκαφών.

ΚΕΦΑΛΑΙΟ 5:

ΕΠΙΚΙΝΔΥΝΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΜΕΡΟΣ 2

5.1 Τηλεχειρισμός (κατασκοπεία) του υπολογιστή

Υπάρχουν ειδικά προγράμματα που δίνουν την δυνατότητα σε έναν χρήστη του Internet να τηλεχειρίζεται τον υπολογιστή ενός άλλου χρήστη που είναι ταυτόχρονα συνδεδεμένος στο διαδίκτυο, όταν ο πρώτος καταφέρνει να υποκλέψει την IP διεύθυνση του δευτέρου. Αυτή η δυνατότητα σημαίνει την υποκλοπή αρχείων και προγραμμάτων, την διαγραφή του σκληρού δίσκου του υπολογιστή ή ακόμα και την ενεργοποίηση περιφερειακών συσκευών, όπως για παράδειγμα Web Camera. Η κατασκοπεία είναι μια ανερχόμενη μορφή ηλεκτρονικού

εγκλήματος που μπορεί να φύγει από τη σφαίρα της επίθεσης σε μεμονωμένους χρήστες και να λάβει σοβαρότερη έννοια εάν χρησιμοποιηθεί εναντίων κρατών, στρατών κ.τ.λ.

5.2 Cookies

Τα cookies αποτελούν ένα από τα ακανθώδη θέματα του Internet που έχουν να κάνουν με τα προσωπικά δεδομένα και το προσωπικό απόρρητο των χρηστών του Διαδικτύου. Τα cookies είναι ένα είδος αρχείων, τα οποία δημιουργούνται και αποθηκεύονται στον σκληρό δίσκο του υπολογιστή μας από τα Web sites που επισκεπτόμαστε στο Internet, με απώτερο σκοπό την αναγνώρισή μας από τα ίδια Web sites την επόμενη φορά που θα βρεθούμε στις ιστοσελίδες τους. Υποτίθεται ότι εξυπηρετούν χρήσιμους σκοπούς για τους χρήστες του Internet, καθώς συγκεντρώνουν πληροφορίες σχετικά με τις καταναλωτικές τους συνήθειες, τις οποίες μπορούν να αξιοποιήσουν sites μεγάλων εταιρειών για να εξειδικεύσουν έτσι ή και να βελτιώσουν τα προϊόντα ή τις υπηρεσίες τους.

Η σημαντικότερη χρήση των cookies είναι να παρακολουθούν και να καταγράφουν (κατασκοπεύουν) τις κινήσεις μας στο Internet, συνήθως τις καταναλωτικές, όπως σε ποια sites περιηγούμαστε και πόσο χρόνο μένουμε σ' αυτά, πόσο συχνά τα επισκεπτόμαστε κ.ά. Ακόμη και μέσα στο ίδιο το site μπορούν να καταγράψουν σε ποιες ιστοσελίδες έχουμε προτίμηση. Μπορούμε από τις κατάλληλες επιλογές του φυλλομετρητή μας να εμποδίσουμε όποτε θέλουμε την αποθήκευση των cookies στον σκληρό μας δίσκο αλλά δεν πρέπει να ξεχνάμε ότι πολλά Web sites είτε θα αρνηθούν να μας φανερώσουν τις ιστοσελίδες τους είτε δεν θα λειτουργήσουν σωστά αν δεν τους δώσουμε την δυνατότητα να διαχειριστούν τα cookies όπως αυτά γνωρίζουν.

Αυτό που έχει ανησυχήσει πολλούς χρήστες σχετικά με τα cookies είναι ο κίνδυνος να διαρρεύσουν οι πληροφορίες αυτές σε τρίτα άτομα ή και η πιθανότητα τα προσωπικά τους δεδομένα να διατίθενται σε τρίτους χωρίς την δική τους συναίνεση. Οι διαχειριστές ενός Web site που χρησιμοποιεί κατά κόρον τα cookies έχουν την δυνατότητα να χρησιμοποιήσουν τις πληροφορίες που συγκεντρώνουν σχετικά με τις προσωπικές προτιμήσεις των επισκεπτών (χρηστών) τους είτε για να βελτιώσουν την εικόνα του site τους ή για να προμηθεύσουν αυτά τα πολύτιμα στοιχεία σε τρίτους και κυρίως σε διαφημιστικές εταιρείες.

Μιλάμε συνεπώς για ένα νέο είδος marketing, το e-marketing. Τα cookies αποτελούν παντοδύναμα εργαλεία marketing, καθώς μπορούν να χρησιμοποιηθούν για να δημιουργηθούν λεπτομερή καταναλωτικά προφίλ για τους χρήστες του Internet. Οι δημιουργοί των δικτυακών

τόπων που χρησιμοποιούν cookies προβάλλουν το επιχείρημα ότι η χρήση των cookies εξυπηρετεί και τους ίδιους τους καταναλωτές – χρήστες του Internet, καθώς μπορούν έτσι να αποκτήσουν ενημέρωση και πληροφόρηση κομμένη και ραμμένη στα μέτρα τους.

Ισχυρίζονται επίσης ότι η μεγάλη πλειοψηφία των χρηστών του Internet δεν απενεργοποιεί τα cookies στο πρόγραμμα φυλλομετρητή που χρησιμοποιεί, παρόλη την ενημέρωση που έχει γίνει για το θέμα αυτό.

5.3 Υποκλοπή αρχείων Η/Υ

Αποκτώντας πρόσβαση σε ένα δίκτυο ο ψηφιακός εγκληματίας έχει τη διακριτική ευχέρεια να κλέψει, να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων και γενικά να κάνει οποιαδήποτε άλλη ενέργεια που θα τα αχρηστεύσει μόνιμα ή προσωρινά, επιφέροντας με τον τρόπο αυτό ανυπολόγιστες οικονομικές ζημιές στα θύματά του. Αν μάλιστα τα αρχεία αυτά περιέχουν οικονομικές πληροφορίες τα πράγματα είναι ιδιαίτερα επικίνδυνα. Στην περίπτωση αυτή το θύμα είναι κατά κύριο λόγο χρηματοπιστωτικό ίδρυμα, συνήθως Τράπεζα. Ο ψηφιακός εγκληματίας με την είσοδό του στο σύστημα επιδιώκει είτε το σπάσιμο των κωδικών λογαριασμών των πελατών με σκοπό τη μεταφορά του περιεχομένου τους στο δικό του λογαριασμό είτε την με αντίστοιχο τρόπο επιβάρυνση των λογαριασμών των κατόχων πιστωτικών καρτών με αγορές που οι ίδιοι δεν έχουν κάνει.

5.4 Πλαστογραφία

Η πλαστογραφία αποτελεί, ένα από τα πιο συνήθη εγκλήματα που δικάζεται στα δικαστήρια καθώς οι άνθρωποι για τις δικαιοπραξίες και τις συναλλαγές τους, χρησιμοποιούν καθημερινά πληθώρα εγγράφων. Σημαντικό είναι να γίνει κατανοητή η έννοια του εγγράφου**,** καθώς η πλαστογραφία τελείται με δημιουργία εγγράφου εξ' αρχής ή με αλλοίωση του περιεχομένου, ενός εγγράφου που ήδη υπάρχει.

Στο άρθρο 13 του Ποινικού Κώδικα ορίζεται πως έγγραφο, είναι όχι μόνο το γραπτό σε ένα φύλλο χαρτί που φέρει ημερομηνία και υπογραφή, αλλά κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή, καθώς επίσης και κάθε υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία όπως σύμβολο, ήχος ή εικόνα, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.

Παρακάτω παρατίθεται μία συνοπτική λίστα εγγράφων, σύμφωνα με τη νομολογία με τα οποία οι περισσότεροι έχουμε έρθει σε επαφή στη καθημερινότητα μας.

α) το όνομα τόσο του αποστολέα όσο και του παραλήπτη σε μια επιστολή,
β) τα εισιτήρια της συγκοινωνίας,
γ) ο αριθμός πλαισίου του κινητήρα του αυτοκινήτου,
δ) οι εγγραφές στη συσκευασία των φαρμάκων,
ε) τα τεχνικά σχέδια των μηχανικών,
στ) το φαξ,
ζ) ο σκληρός δίσκος του υπολογιστή,
η) η υπογραφή του ζωγράφου πάνω στο πίνακα ζωγραφικής του,
θ) οι τιμές που αναγράφονται στα εμπορεύματα, η ημερομηνία παρασκευής, λήξης ή οτιδήποτε δηλώνει προέλευση.

Οι περιπτώσεις αυτές είναι ενδεικτικές, και υπάρχουν πολλά περισσότερα παραδείγματα εγγράφων. Το σημαντικό είναι να γίνει κατανοητό πως οποιαδήποτε πληροφορία έχει ή μπορεί να έχει έννομη σημασία και είναι αποτυπωμένη σε οποιοδήποτε υλικό ή τεχνολογικό μέσο αποτελεί έγγραφο. Ποιοι είναι όμως η τρόποι τέλεσης του εγκλήματος της πλαστογραφίας, σύμφωνα με το νόμο;

Η πλαστογραφία τελείται με δύο τρόπους: α) με κατάρτιση πλαστού εγγράφου που σημαίνει πως το πρόσωπο που φέρεται ως εκδότης του εγγράφου, δεν είναι ο πραγματικός εκδότης του, δεν του ανήκει λοιπόν η υπογραφή του εγγράφου και β) με νόθευση εγγράφου η οποία αναφέρεται στο περιεχόμενο του εγγράφου, όταν δηλαδή υπάρχει ουσιώδης επέμβαση στο έγγραφο που αλλοιώνει το αληθινό του περιεχόμενο όπως για παράδειγμα η αλλαγή της ημερομηνίας, η αφαίρεση ή η προσθήκη μιας σελίδας σε συμβόλαιο, η προσθήκη ή η αφαίρεση λέξεων σε έγγραφο κ.α

Πέρα όμως από την αντικειμενική υπόσταση της πλαστογραφίας, δηλαδή την κατάρτιση και την νόθευση εγγράφου απαραίτητο είναι και το υποκειμενικό στοιχείο του αδίκου, στο πρόσωπο του δράστη που είναι ο σκοπός παραπλάνησης για γεγονός που έχει έννομες συνέπειες και χωρίς αυτόν δεν υφίσταται το εν λόγο έγκλημα. Σημειώνεται δε, πως ο σκοπός του δράστη για παραπλάνηση πρέπει να υπάρχει κατά τη στιγμή της κατάρτισης ή της νόθευσης, ενώ η πραγματοποίηση του σκοπού δεν είναι απαραίτητη.

Η χρήση του πλαστού εγγράφου από τον ίδιο τον πλαστογράφο, ενέχει μια ιδιαίτερη απαξία και θεωρείται επιβαρυντική περίσταση, ωστόσο και η χρήση του πλαστού εγγράφου από

κάποιον άλλον πλην του πλαστογράφου τιμωρείται αυτοτελώς, εφόσον φυσικά γνωρίζει το πρόσωπο που χρησιμοποιεί στις συναλλαγές το έγγραφο πως είναι πλαστό.

5.5 Πειρατεία λογισμικού

Ως πειρατεία λογισμικού ορίζεται η μη εξουσιοδοτημένη αντιγραφή ή η διανομή λογισμικού, η οποία πραγματοποιείται με την λήψη, αντιγραφή, κοινή χρήση, πώληση ή εγκατάσταση πολλαπλών αντιγράφων σε προσωπικούς ή εταιρικούς υπολογιστές. Αυτό που οι περισσότεροι δεν κατανοούν όταν αγοράζουν λογισμικό, είναι ότι στην πραγματικότητα αγοράζουν την άδεια χρήσης του και όχι το ίδιο το λογισμικό. Η άδεια θα πρέπει να διαβάζεται πολύ προσεκτικά γιατί καθορίζει σε πόσους υπολογιστές επιτρέπεται η εγκατάσταση του λογισμικού. Επομένως, η δημιουργία περισσοτέρων αντιγράφων από όσα ορίζει η άδεια αποτελεί πειρατεία.

Η πειρατεία λογισμικού είναι ένα πολύ σοβαρό θέμα. Εκτός από την παραβίαση του νόμου και των δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών του λογισμικού, το πλαστό λογισμικό μπορεί να βλάψει σοβαρά το PC και να υπονομεύσει την ασφάλεια του. Το πλαστό λογισμικό πωλείται συνήθως σε ψεύτικες ιστοσελίδες ή μέσω ταξινομημένων διαφημίσεων. Το πλαστό λογισμικό μπορεί να είναι καλό αντίγραφο του πρωτοτύπου, είναι όμως περισσότερο πιθανό να είναι ελαττωματικό, ακόμα και επικίνδυνο. Το πειρατικό λογισμικό μπορεί να φαίνεται καλή περίπτωση, αλλά μπορεί να αποβεί ιδιαίτερα δαπανηρό.

Ορίστε μερικοί από τους λόγους:

α) Το πειρατικό λογισμικό μπορεί να προκαλέσει ολικές βλάβες του υπολογιστή σας. Χάνετε χρόνο. Μπορεί να χάσετε αναντικατάστατα αρχεία ή δεδομένα. Μπορεί ακόμα και να καταστρέψετε το PC σας και όλο σας το άλλο λογισμικό,

β) Το πλαστό λογισμικό μπορεί να περιέχει spyware που φορτώνεται στον υπολογιστή σας και αναφέρει προσωπικά δεδομένα χωρίς να το γνωρίζετε, όπως αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, κωδικούς πρόσβασης και βιβλία διευθύνσεων. Οι κλεμμένες πληροφορίες μπορεί να γίνουν αμέσως αντικείμενο εκμετάλλευσης από κλέφτες ταυτότητας.

Οι κυβερνοκλέφτες ανακαλύπτουν κατά περιόδους ευπάθειες σε λογισμικό και οι προμηθευτές λογισμικού παρέχουν διορθωτικές εκδόσεις που αντιμετωπίζουν την ευπάθεια. Αν έχετε πλαστό λογισμικό, δεν θα μπορείτε να του ενσωματώνετε τις νομότυπες ενημερώσεις

κι έτσι θα είστε ευάλωτοι σε επιθέσεις. Ένας πωλητής που προτείνει να παραβιάσετε το νόμο ίσως να μη σταματήσει στο πειρατικό λογισμικό. Οποιαδήποτε δεδομένα πιστωτικών καρτών ή προσωπικά δεδομένα που παρέχετε μπορεί να τύχουν εκμετάλλευσης από κλέφτες ταυτότητας.

Για να αποφύγετε να γίνετε θύμα των πειρατών λογισμικού, ακολουθήστε αυτά τα απλά βήματα:

1) Αγοράζετε λογισμικό μόνο από αξιόπιστες εταιρείες.

2) Όταν κάνετε αγορές online, να βεβαιώνεστε ότι η ιστοσελίδα είναι νομότυπη. Στη σελίδα πραγματοποίησης αγοράς της ιστοσελίδας, κάντε κλικ στο εικονίδιο με το λουκέτο στο παράθυρο του προγράμματος περιήγησης και δείτε το πιστοποιητικό ασφαλείας. Αν δεν υπάρχει λουκέτο, πιθανότατα η ιστοσελίδα δεν είναι ασφαλής.

3) Πριν δώσετε στοιχεία πιστωτικής κάρτας, ελέγξτε τη διεύθυνση URL της ιστοσελίδας. Πρέπει να περιλαμβάνει την ένδειξη "https:" όχι μόνο "http:". Αν δεν υπάρχει "s", μην κάνετε την αγορά. (Το γράμμα "s" σημαίνει μόνο ότι οι πληροφορίες είναι κρυπτογραφημένες όταν στέλνονται μέσω του Internet. Δεν σημαίνει ότι η ιστοσελίδα είναι νομότυπη).

4) Αν σας φαίνεται ότι μια τιμή φαίνεται πολύ καλή για να είναι αληθινή, μάλλον έτσι είναι. Προσέχετε τις εξαιρετικά μειωμένες τιμές και διπλοελέγξτε τη γνησιότητα της ιστοσελίδας.

5) Αν το λογισμικό σας καταφθάσει σε μια λευκή θήκη ή σε έναν απλό φάκελο, πιθανότατα είναι πλαστό. Το νομότυπο λογισμικό διατίθεται σε συσκευασίες με πλαστικό κάλυμμα, με τυπωμένες οδηγίες και κάρτες δήλωσης στοιχείων.

6) Αν πιστεύετε ότι ίσως να αγοράσατε πλαστό λογισμικό, θα πρέπει να επικοινωνήσετε με τον νόμιμο κατασκευαστή του δημιουργού του λογισμικού και ταυτόχρονα να ζητήσετε επιστροφή των χρημάτων σας από τον πωλητή.

Το συμπέρασμα: Το πλαστό λογισμικό είναι βλαπτικό για όλους και μπορεί να είναι πολύ δαπανηρό για όλους όσους το χρησιμοποιούν. Προσέχετε όταν αγοράζετε λογισμικό online και αναφέρετε όποιο λογισμικό υποπτεύεστε ότι μπορεί να είναι πλαστό. 7 στους 10 χρήστες ηλεκτρονικών υπολογιστών στην Ελλάδα παραδέχονται ότι έχουν αποκτήσει πειρατικό λογισμικό, σύμφωνα με τα στοιχεία της Business Software Alliance (BSA) που ανακοινώθηκαν στο πλαίσιο της Διεθνούς Έρευνας της BSA για την Πειρατεία Λογισμικού

2011. 38% των χρηστών ηλεκτρονικών υπολογιστών που συμμετείχαν στην έρευνα, δήλωσαν ότι λαμβάνουν πειρατικό λογισμικό «περιστασιακά», «πάντα» ή «τις περισσότερες φορές», ενώ το 32% δήλωσαν «σπάνια».

Ως αποτέλεσμα, το ποσοστό της πειρατείας λογισμικού στην Ελλάδα για το 2011 άγγιξε το 61%, το οποίο σημαίνει ότι κατά προσέγγιση 2 στα 3 προγράμματα που εγκαταστάθηκαν από τους χρήστες ήταν χωρίς άδεια (παράνομα). Το ποσοστό αυτό είναι αυξημένο κατά 2% σε σύγκριση με το 59% που καταγράφηκε το 2010, και αντικατοπτρίζει τη σταθερά ανοδική τάση της πειρατείας λογισμικού που καταγράφεται στην Ελλάδα κάθε χρόνο από το 2007. Η δε εμπορική αξία της πειρατείας για το 2011 αντιστοιχεί σε €247 εκατομμύρια.

Με το ποσοστό του 61%, η Ελλάδα κατατάσσεται 3η ανάμεσα στις πρώτες πέντε χώρες της Ευρωπαϊκής Ένωσης με τα μεγαλύτερα ποσοστά πειρατείας, μετά τη Βουλγαρία (64%) και την Ρουμανία (63%), και ακολουθούμενη από τη Λετονία και τη Λιθουανία (με ποσοστό 54% και οι δύο), και την Πολωνία (53%). Σε Πανευρωπαϊκό επίπεδο, το ποσοστό πειρατείας για το 2011 κυμαίνεται στο 33%, καταγράφοντας μια μείωση της τάξης του 2% σε σύγκριση με την προηγούμενη χρονιά.

5.6 Απάτη μέσω Διαδικτύου

Αναμφισβήτητα το διαδίκτυο έχει γίνει πολύτιμος σύμμαχος για τους εγκληματίες, οι όποιοι επιδιώκουν με κάθε τρόπο την απόσπαση χρηματικών ποσών από ανυποψίαστα θύματα. Ένας τέτοιος εύκολος και ανέξοδος τρόπος είναι η αποστολή e-mail. Ο εγκληματίας αποστέλλει μαζικά e-mails σε θύματα με περιεχόμενο παραπλανητικό αλλά αρκετά έξυπνο και καλά οργανωμένο. Ο επιτιθέμενος συντάσσει ένα e-mail παράκλησης στο όποιο αναφέρει πως προέρχεται από αφρικανική χωρά κι έχει σκοπό να μετακινηθεί στη χωρά του θύματος προφασιζόμενος αιτίες που θα συγκινήσουν το θύμα (πόλεμος, φυσικές καταστροφές κτλ).

Ζητάει λοιπόν από το θύμα να ανοίξει ένα τραπεζικό λογαριασμό με συνδικαιούχο τον ίδιο, υποσχόμενος πως όταν η διαδικασία μεταφοράς χρημάτων ολοκληρωθεί, θα ανταμείψει το θύμα. Ο σκοπός είναι να αποσπάσει το χρηματικό πόσο που κατέθεσε το θύμα για τα έξοδα κίνησης και ύστερα να καταργήσει το λογαριασμό. Ένα ακόμα παράδειγμα τέτοιας απάτης είναι και το ισπανικό ΛΟΤΤΟ. Αφρικανοί υπήκοοι κάτοικοι Ισπανίας, αποστέλλουν e-mails με τα οποία αναφέρουν πως το θύμα κέρδισε στο ισπανικό ΛΟΤΤΟ. Ζητούν τα προσωπικά στοιχειά και τον αριθμό του τραπεζικού λογαριασμού του θύματος για να καταθέσουν το

υποτιθέμενο ποσό όσο και την κατάθεση χρηματικού ποσού για τα διαδικαστικά έξοδα από το ίδιο το θύμα.

Τα εγκλήματα με πιστωτικές κάρτες αυξηθήκαν με τη βελτίωση και εξάπλωση του ηλεκτρονικού εμπορίου, ιδιαίτερα τώρα που αρκεί ο τραπεζικός λογαριασμός ώστε ο χρήστης να μπορεί να διεκπεραιώσει κάθε είδους εμπορική συναλλαγή εξ αποστάσεως. Επομένως έχουμε την διάθεση αριθμών τραπεζικών λογαριασμών στο διαδίκτυο, διαδικασία όχι ιδιαίτερα δύσκολη, αφού με την τεχνολογία «web sniffer» παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα οι αριθμοί αυτοί.

Από την σκοπιά του ποινικού δικαίου κατά την χρήση του διαδικτύου είναι δυνατόν να τελεστούν απάτες μέσω υπολογιστή, όπου ο υπολογιστής είναι απλώς το μέσο τέλεσης της κοινής απάτης αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή η ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή, στα προγραμματα και στα δεδομένα του.

Οι μορφές των πλέον διαδεδομένων απατών που τελούνται τα τελευταία χρόνια μέσω του διαδικτύου είναι οι ακόλουθες:

1. Η απάτη με τα Νιγηριανά μηνύματα του ηλεκτρονικού ταχυδρομείου (Nigerian e-mail fraud). Στην περίπτωση αυτή το υποψήφιο θύμα λαμβάνει ένα e-mail στο οποίο ο απατεώνας του υπόσχεται μεγάλη χρηματική αμοιβή αν τον βοηθήσει να μεταφέρει χρήματα από τον τραπεζικό του λογαριασμό στον λογαριασμό του θύματος. Οι λόγοι τους οποίους επικαλείται ο απατεώνας για την μεταφορά αυτή ποικίλλουν κατά περίπτωση συνήθως, όμως, αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή γόνους πλούσιων οικογενειών που θα πρέπει να εγκαταλείψουν τη χώρα τους εξαιτίας πολιτικών συγκρούσεων. Προτού, όμως, το θύμα να εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο απατεώνας, θα πρέπει να καταβάλλει ορισμένα χρήματα για τα έξοδα μεταφοράς ή να δώσει για το λόγο αυτό τα στοιχεία του τραπεζικού του λογαριασμού. Στην πρώτη περίπτωση, μετά την αποστολή των χρημάτων θα διακοπεί η επικοινωνία με τον απατεώνα, ενώ στη δεύτερη το θύμα είναι πολύ πιθανό να χάσει όλα τα χρήματα του τραπεζικού του λογαριασμού, έχοντας ο απατεώνας στην διάθεση του τα στοιχεία της ταυτότητας του θύματος με την δυνατότητα να τον χρεώνει μεγάλα χρηματικά ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης και «419» από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

2. Η απάτη με το phishing mail (ηλεκτρονικό μήνυμα «ψαρέματος»). Στην περίπτωση αυτή, ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει, να αποσπάσει από το θύμα του προσωπικά του οικονομικά δεδομένα. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email,

αποστολέας του οποίου φαίνεται να είναι η τράπεζα με την οποία συναλλάσεται. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του τραπεζικού του λογαριασμού που διακινεί μέσω του διαδικτύου (Web Banking). Η σχετική αιτιολογία αναφέρεται σε προβλήματα στους Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δεν γίνει η επιβεβαίωση του θα κλειδωθεί. Το e-mail αυτό έχει σύνδεσμο (link) προς τον δικτυακό τόπο της εν λόγω τράπεζας, ο οποίος όμως δεν είναι πραγματικός και μιμείται απλά τον αυθεντικό και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα.

3. Άλλος ένας τρόπος ψηφιακής απάτης είναι εκείνος που αφορά την λήψη από το υποψήφιο θύμα ενός e-mail ή ενός pop-up window που του εμφανίζεται κατά την περιήγηση του στον Ιστό, με τον οποίο του γνωστοποιείται ότι κέρδισε ένα σημαντικό χρηματικό ποσό σε κάποια κλήρωση. Για να το πάρει αυτό, θα πρέπει να καταβάλλει ένα χρηματικό ποσό σε συγκεκριμένο λογαριασμό. Φυσικά, μετά την καταβολή των χρημάτων ο απατεώνας εξαφανίζεται και τα θύματα τους δεν λαμβάνουν κανένα νέο e-mail το οποίο θα τους γνωστοποιεί τον τρόπο με τον οποίο θα εισπράξουν το χρηματικό έπαθλο.

4. Η απάτη με τις ιστοσελίδες – μαϊμούδες. Σε αυτήν την περίπτωση ο απατεώνας προσπαθεί να οδηγήσει το θύμα του να κάνει μια οικονομική συναλλαγή στο πιστό αντίγραφο της τράπεζας του ή του ηλεκτρονικού καταστήματος που επισκέπτεται, το οποίο το έχει δημιουργήσει ο ίδιος και το ελέγχει απόλυτα. Το ανυποψίαστο θύμα, νομίζοντας ότι βρίσκεται στην ιστοσελίδα της τράπεζας του ή ενός υπεράνω πάσης υποψίας ηλεκτρονικού καταστήματος δίνει όλα τα απαιτούμενα για την συναλλαγή στοιχεία (αριθμό πιστωτικής κάρτας, λογαριασμού, κωδικούς πρόσβασης κ.τ.λ.), τα οποία ο απατεώνας μπορεί να τα χρησιμοποιήσει στη συνέχεια είτε για να αδειάσει τον τραπεζικό λογαριασμό του θύματος είτε για να επιβαρύνει την πιστωτική του κάρτα με αγορές που ποτέ δεν πραγματοποίησε το ίδιο το θύμα.

5. Η απάτη με τις επιταγές. Στη συγκεκριμένη περίπτωση, ένας απατεώνας αγοραστής σε μια δικτυακή δημοπρασία είναι δυνατό να συμφωνήσει με τον πωλητή να πληρώσει με επιταγή. Το υποψήφιο θύμα καταθέτει την επιταγή και ο πωλητής στέλνει το εμπόρευμα, όμως στις περισσότερες περιπτώσεις οι τράπεζες εμφανίζουν τα χρήματα στο λογαριασμό του θύματος προτού να ελεγχθεί η γνησιότητα της επιταγής. Λίγες μέρες μετά η τράπεζα διαπιστώνει ότι η επιταγή είναι ακάλυπτη ή πλαστή και αφαιρεί το αντίστοιχο χρηματικό ποσό από το λογαριασμό του θύματος.

ΚΕΦΑΛΑΙΟ 6:

ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ

6.1 Ιστορική αναδρομή

Όσο πιο προς τα πίσω πηγαίνει η ιστορία όλο και πιο ογκώδη βρίσκει κανείς την παραμέληση και τη σκληρότητα και όλο και περισσότερα παιδιά έχουν σκοτωθεί, απορριφθεί, χτυπηθεί, τρομοκρατηθεί και σεξουαλικά κακοποιηθεί από τους υπεύθυνους για την φροντίδα τους.

Ο ψυχοϊστορικός Lloyd deMause έχει γράψει εκτενώς για την κακοποίηση παιδιών. Στην «Ιστορία Της Παιδικής Ηλικίας», απαριθμεί την εμπειρία παιδιών στην Ινδία και την Κίνα ως ιδιαίτερα καταχρηστική. Στην Ινδία, τα παιδιά αυνανίζονταν από τις μητέρες τους και οι ενήλικοι τα χρησιμοποιούσαν σεξουαλικά πολύ πριν φθάσουν στην ηλικία των δέκα. Το να μεγαλώνει κανείς στην Κίνα ήταν εξίσου σκληρό. Και στα αρσενικά και στα θηλυκά παιδιά είχαν επιτεθεί σεξουαλικά και τα είχαν αναγκάσει να βγουν στη πορνεία. Τα αρχαία ελληνικά και ρωμαϊκά κορίτσια βιάζονταν συχνά, και ηλικιωμένοι χρησιμοποιούσαν συχνά μικρά αγόρια για την ικανοποίηση των σεξουαλικών τους ορέξεων. Μέχρι πρόσφατα, από τις αρχές

μέχρι και τα μέσα του 20ου αιώνα, στις δυτικές χώρες τα παιδιά θεωρούνταν μικροί ενήλικοι καθώς εργάζονταν από πολύ μικρά σε ιδιαίτερα βαριές δουλειές.

Η παιδική εκμετάλλευση υπήρξε πολύ πριν από το Διαδίκτυο, και τα δίκτυα των παραβατών που επικοινωνούσαν πριν από την ανακάλυψη των προσωπικών υπολογιστών ήταν μέρος της καθημερινής ζωής αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης παιδιών. Η αυξανόμενη χρήση του Διαδικτύου από τους έφηβους και από τα πιο μικρά παιδιά δημιούργησαν την πιθανότητα δίωξης τους από τους ενήλικους παραβάτες. Καθώς όλο και περισσότερα παιδιά συγκεντρώθηκαν στο Διαδίκτυο στη δεκαετία του '90, οι ενήλικες που επιθυμούσαν να τους δελεάσουν για σεξουαλικές σχέσεις, τους υποδέχθηκαν με χαρά. Τι συνέβαινε πριν από την ευρεία χρήση του Διαδικτύου; Εάν ένας ενήλικος ενδιαφερόταν να έρθει σε σεξουαλική επαφή με ένα παιδί, θα επιδίωκε την επαφή με την εύρεση της απασχόλησης όπου θα υπήρχε έκθεση στα παιδιά, ή θα προσφερόταν εθελοντικά να συνεργαστεί με παιδιά, ή αποκτώντας με τον ένα ή τον άλλο τρόπο δικά του ή γίνονταν φιλικός με τα παιδιά της γειτονιάς.

Φανταστείτε την απέραντη διαφορά στην τεχνολογία επικοινωνιών που έχει εμφανιστεί κατά τη διάρκεια του προηγούμενου τετάρτου του αιώνα. Οποτεδήποτε πριν από το 1995, ένα πρόσωπο που επιδίωκε τη σεξουαλική επαφή με ένα παιδί είτε θα γινόταν ιερέας, ή δάσκαλος, ή κλόουν, ή πατέρας, ή θείος, ή οδηγός λεωφορείων ή θα κρυβόταν γύρω από την παιδική χαρά γειτονιάς.

6.2 Ορισμός

Σαν παιδική πορνογραφία ορίζεται η καταγραφή της σεξουαλικής κακοποίησης παιδιών κάτω της ηλικίας των 18 ετών σε φωτογραφίες ή βιντεοσκοπήσεις. Ο όρος ‘‘Παιδική Πορνογραφία’’ περιλαμβάνει πορνογραφικό υλικό το οποίο περιγράφει ορατά: Ανήλικο ή πρόσωπο που φαίνεται να είναι ανήλικο που εμπλέκεται σε σεξουαλική συμπεριφορά.

Ως βασικότερη αιτία προώθησης της σεξουαλικής εκμετάλλευσης των παιδιών θεωρείται μεταξύ άλλων το παγκόσμιο εμπόριο πορνογραφικού υλικού. Ως δραστηριότητα, αποτελεί μια ανθούσα βιομηχανία με εκτιμώμενα κέρδη αρκετών δισεκατομμυρίων ευρώ που υλοποιείται μέσω εξαιρετικά πολύπλοκων δικτύων και κυκλωμάτων. Η παραγωγή και το εμπόριο παιδικής πορνογραφίας οργανώνεται και παράγεται κυρίως από άτομα διαταραγμένης προσωπικότητας που ανήκουν κατά κανόνα στην κατηγορία των παιδεραστών.

Τα άτομα αυτά αποσκοπούν στην αξιοποίηση του πορνογραφικού υλικού ως μέσου σεξουαλικής ικανοποίησης τόσο των ίδιων όσων και άλλων που είναι αναμεμειγμένοι σε τέτοιες δραστηριότητες κακοποίησης. Συγκεκριμένα, μέσα από αστυνομικά δεδομένα, έχουν καταγραφεί πέντε βασικοί λόγοι για τους οποίους οι παιδεραστές προβαίνουν στην παραγωγή παιδικής πορνογραφίας.

Αυτοί είναι:

1. Ως μόνιμη καταγραφή του παιδιού από αυτόν που το κακοποιεί
2. Για να χρησιμοποιηθεί σαν μέρος της διαδικασίας αποπλάνησης
3. Για να ενισχύσουν και να επιβεβαιώσουν τα πιστεύω τους
4. Για να εκβιάσουν τα θύματα
5. Για εμπορικούς σκοπούς

Η πορνογραφία ως υλικό μπορεί να περιλαμβάνει περιοδικά, βιντεοταινίες, κινηματογραφικές ταινίες ή φωτογραφίες. Αν και η διαφήμιση του υλικού αυτού συχνά είναι καλυμμένη και κωδικοποιημένη εν τούτοις, οι αστυνομικές εκθέσεις δείχνουν αύξηση των περιπτώσεων ανταλλαγής υλικού και παιδιών μεταξύ παιδεραστών. Η παραγωγή και το εμπόριο πορνογραφικού υλικού με πρωταγωνιστές μικρά παιδιά και η σεξουαλική εκμετάλλευση των παιδιών κρίνεται ότι είναι πράξεις που κακοποιούν, εκμεταλλεύονται και προκαλούν σοβαρές ζημιές στα παιδιά. Από αυτή την άποψη, η ύπαρξη παιδικής πορνογραφίας αποτελεί συνεπώς, σαφές και κατηγορηματικό στοιχείο παιδικής κακοποίησης.

6.3 Διαδίκτυο και πορνογραφικό υλικό

Η συνήθης έκφραση της παιδικής πορνογραφίας είναι αυτή της παρουσίασης ανηλίκων μέσω φωτογραφικού υλικού ως συμμετεχόντων σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Σήμερα με τις δυνατότητες που οι νέες τεχνολογίες προσφέρουν, είναι πολύ εύκολο και σχετικά γρήγορο, να ‘‘ανεβάσει’’ κάποιος ψηφιακό υλικό σεξουαλικού περιεχομένου στο Διαδίκτυο. Αυτό επιτυγχάνεται δημιουργώντας βίντεο ή σκανάροντας φωτογραφίες, υλικό το οποίο εύκολα μπορεί να αποθηκεύσει σε κάποιο αρχείο, και μετά είτε να το διαβιβάσει μέσω του ηλεκτρονικού ταχυδρομείου ή να το προωθήσει μέσω κινητής τηλεφωνίας, είτε να το δημοσιεύσει σε κάποια ιστοσελίδα, με παραλήπτες σε όλο τον κόσμο.

Το φαινόμενο της παιδικής πορνογραφίας στο Διαδίκτυο έχει λάβει ανησυχητικές διαστάσεις. Συγκλονιστικά στοιχεία γύρω από την παιδική πορνογραφία έρχονται στο φως με ανατριχιαστικές αποκαλύψεις. Στην Ελλάδα από το 2001 έως σήμερα έχουν εξιχνιαστεί 50 αντίστοιχες υποθέσεις, έχουν κατηγορηθεί 119 άτομα και έχουν πραγματοποιηθεί 93 συλλήψεις. Ήδη το 2005 εντοπίστηκαν 20 κυκλώματα διακίνησης υλικού παιδικής πορνογραφίας μέσω διαδικτύου.

Σύμφωνα με την τελευταία έκθεση του Ευρωβαρομέτρου το 2005, (ΕΕ-Ευρωβαρόμετρο, 2005) υπολογίζεται ότι η παιδική πορνογραφία στην Ελλάδα αυξάνεται ετησίως κατά 150%. Αυτό αποδεικνύεται και από στοιχεία της Ελληνικής Αστυνομίας, όπου γίνεται λόγος για ύπαρξη κυκλωμάτων που διακινούν απίστευτο πορνογραφικό υλικό με πρωταγωνιστές μαθητές, μέχρι και νήπια σε κτηνώδεις σεξουαλικές δραστηριότητες, ακόμα και με ζώα ενώ στον τελευταίο ενάμιση χρόνο σημειώθηκε αυτοκτονία και 5 απόπειρες. Τα στοιχεία που κατατέθηκαν στην Κυπριακή Βουλή σε σχέση με την παιδική πορνογραφία δείχνουν ότι οι περιπτώσεις αυξήθηκαν σημαντικά κατά τους τελευταίους 20 μήνες προκαλώντας δέος και δίνοντας την πραγματική διάσταση του προβλήματος.

Το πρόβλημα φαίνεται να λαμβάνει ακόμα πιο συγκλονιστικές διαστάσεις αν λάβει κανείς υπόψη του ανάλογες παραμέτρους όπως είναι για παράδειγμα, ο βαθμός προσβασιμότητας των παιδιών στο διαδίκτυο αλλά και ο βαθμός συνειδητής επίγνωσης και ενημέρωσης των κινδύνων που διατρέχουν τα ίδια τα παιδιά κατά την πλοήγησή τους στο διαδίκτυο.

Σε σχετικά πρόσφατη έρευνα του Πανευρωπαϊκού Δικτύου Εθνικών Κόμβων Ασφαλούς Διαδικτύου Insafe, που τελείται υπό την αιγίδα της Ευρωπαϊκής Επιτροπής, που διεξήχθη μεταξύ 6 Δεκεμβρίου 2006 και 7 Φεβρουαρίου 2007 σε 37 χώρες του κόσμου στο ερωτηματολόγιο της οποίας απάντησαν συνολικά 21.825 παιδιά και έφηβοι, μεταξύ των οποίων και 322 Ελληνόπουλα, αποκαλύπτεται ότι:

Τα παιδιά κάτω των 10 ετών φαίνεται να έχουν ελάχιστη γνώση των κινδύνων που ελλοχεύουν στις συναντήσεις με άτομα που γνώρισαν μέσα από δωμάτια ανοιχτής επικοινωνίας, τα λεγόμενα chat rooms. Περισσότερα από το 1/3 των παιδιών αυτών δήλωσαν ότι θα συναντούσαν μόνα τους έναν τέτοιον άγνωστο και δεν θα ενημέρωναν τους γονείς τους. 8 στα 10 ελληνόπουλα δηλώνουν ότι έχουν δικό τους υπολογιστή, 6 στα 10 παιδιά σερφάρουν έως 5 ώρες εβδομαδιαίως, ενώ 2 στα 10 είναι online πάνω από 10 ώρες.

Επιπλέον 7 στα 10 Ελληνόπουλα δηλώνουν ότι δεν συνομιλούν με αγνώστους στο διαδίκτυο και δεν θα πήγαιναν ποτέ μόνα τους σε συνάντηση με άγνωστο που γνώρισαν μέσα από το

διαδίκτυο. Όμως 1 στα 2 παιδιά δηλώνει ότι δίνει πολλές προσωπικές πληροφορίες γύρω από τον εαυτό του και τη ζωή του μέσα από τους ιδιαίτερα δημοφιλείς ιστοχώρους κοινωνικής δικτύωσης, τα λεγόμενα social networking sites, όπως το MySpace ή το Bebo.

Αναφορικά με τα προσωπικά δεδομένα, δηλώνεται ότι 1 στα 4 παιδιά θα έδινε χωρίς πρόβλημα τα στοιχεία του τραπεζικού του λογαριασμού μέσα από το διαδίκτυο. και μόνο 4 στα 10 παιδιά θα συμπλήρωναν σε φόρμες ιστοχώρων όπου ερωτώνται για τη διεύθυνσή τους, το τηλέφωνό τους και για άλλες προσωπικές τους πληροφορίες, μόνο τα βασικά στοιχεία τους.

Σχετικά με το εάν λάμβαναν από κάποιο διαδικτυακό τους φίλο φωτογραφία με πορνογραφικό περιεχόμενο, δηλώνεται ότι μόνο 1 στα 2 παιδιά θα το έλεγε στους γονείς του ή στον δάσκαλό του. Από την άλλη πλευρά 8 στα 10 παιδιά μας δηλώνουν ότι θα άκουγαν προσεκτικά τους δασκάλους τους σχετικά με συμβουλές γύρω από την ασφαλή χρήση του διαδικτύου.

6.4 Το προφίλ των παιδιών-θυμάτων

Από τα 229 παιδιά που εντοπίσθηκαν ως θύματα κακοποίησης, τα 165 (72,1%) ήταν κορίτσια και τα 64 (27,9%) αγόρια. Το εύρος των ηλικιών των παιδιών που μελετήθηκαν κυμαίνονται από 3 μήνες έως και 17 έτη, με μέσο όρο ηλικίας 11,25 έτη. Ειδικότερα, για τα αγόρια ο μέσος όρος ηλικίας είναι 9 έτη, ενώ για τα κορίτσια 12 έτη. Ο μεγαλύτερος αριθμός των θυμάτων (49,8%) αφορά σε παιδιά εφηβικής ηλικίας (13-18 ετών), ενώ το (36,3%) και το (13,9%) αφορά σε παιδιά σχολικής ηλικίας, 6-12 ετών και προσχολικής ηλικίας (5 ετών ή μικρότερα), αντίστοιχα. Θα μπορούσε να συμπεράνει κανείς, ότι τα αγόρια θυματοποιούνται συχνότερα σε μικρότερη ηλικία, σε σχέση με τα κορίτσια. Επίσης, τα αγόρια φαίνεται, ότι όταν θυματοποιηθούν μία φορά, συχνότερα επαναλαμβάνεται η κακοποίηση (57,5%), σε αντίθεση με τα κορίτσια, τα οποία συχνότερα γίνονται θύματα μεμονωμένων συμβάντων (60,7%).

6.5 Το προφίλ όσων κακοποιούν παιδιά

Στη συντριπτική πλειοψηφία τα παιδιά γνώριζαν τον δράστη (93,0%) και μόνο στο (7,0%) των περιπτώσεων ο δράστης τους ήταν άγνωστος. Στο (38,2%) των καταγγελιών ο υπαίτιος της κακοποίησης φαίνεται να είχε σχέση συγγένειας με το παιδί. Ειδικότερα, ως δράστης παρουσιάζεται ο πατέρας του παιδιού (15,1%) και στο (19,6%) κάποιος άλλος συγγενής του (θείος, ξάδερφος κ.ά.). Ορισμένες καταγγελίες κακοποίησης αφορούν στη μητέρα του παιδιού ως δράστη (1,5%). Στο σύνολό τους οι δράστες είναι άντρες (98%) και σε (14,6%) περιπτώσεις ο υπαίτιος της κακοποίησης είναι ανήλικος. Οι καταγγελίες αφορούν σε δράστες ενήλικες, που

είχαν αναπτύξει σχέσεις φιλίας και εμπιστοσύνης με το παιδί (41,7%) και μόνο (7,5%) των καταγγελιών σχετίζονται με ενήλικα άτομα, τα οποία ήταν άγνωστα στο παιδί. Σε (17,6%) περιπτώσεις οι δράστες είναι περισσότεροι του ενός, ενώ σε (13,1%) η πληροφορία αυτή είναι άγνωστη.

6.6 Συνηθέστεροι τρόποι προσέγγισης των παιδιών-θυμάτων

Συχνότερος τρόπος προσέγγισης του θύματος αποτελεί η εκμετάλλευση της εμπιστοσύνης του παιδιού (47,3%) από συγγενικά του άτομα (πατέρας, θείος, νονός) ή άτομα του στενού οικογενειακού περιβάλλοντός του (πατριός, φίλος γονέων). Άλλος τρόπος, που φαίνεται να εφαρμόζουν οι δράστες είναι η αρχική γνωριμία του παιδιού με οποιονδήποτε τρόπο και στην συνέχεια η κακοποίησή του με την άσκηση σωματικής βίας ή με τη χρήση κατασταλτικών ουσιών, όπως είναι η αλκοόλη και οι ναρκωτικές ουσίες (18,8%). Ο βιασμός του παιδιού με την άσκηση σωματικής βίας παρατηρήθηκε λιγότερο συχνά, ενώ σε (11,8%) και (5,4%) περιπτώσεις η συναίνεση του θύματος εξασφαλίσθηκε με τη σύναψη σχέσης και την εξαγορά του, αντίστοιχα. Τέλος, υπάρχουν και (18,8%) περιπτώσεις, στις οποίες δεν υπάρχουν πληροφορίες σχετικά με τον τρόπο προσέγγισης των δραστών. Παιδιά τα οποία κακοποιούνταν κατ' επανάληψη φαίνεται να καθυστερούσαν να αποκαλύψουν το συμβάν, σε σχέση με εκείνα που κακοποιήθηκαν μία φορά. Επίσης, τα περισσότερα παιδιά, που δεν γνώριζαν και δεν είχαν αναπτύξει προηγουμένως σχέσεις με τον δράστη, κατήγγειλαν άμεσα το γεγονός (76,9%).

6.7 Grooming

Διαδικασία κατά την οποία τα "αρπακτικά", προσποιούμενα ότι είναι έφηβοι, χρησιμοποιούν τα δωμάτια ανοικτής επικοινωνίας (chat rooms), τις ιστοσελίδες διαδικτυακής επικοινωνίας για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα θύματα του Grooming μπορεί να υποστούν σοβαρά τραύματα που έχουν ψυχολογικό και συναισθηματικό αντίκτυπο, με πολύ βλαβερές επιπτώσεις στην υγεία τους. Η κακοποίηση που δέχεται ένα παιδί το οποίο εμπλέκεται σε Grooming, δεν είναι μόνο σεξουαλικής φύσεως, αλλά και συναισθηματικής, καθώς τα παιδιά βρίσκουν πολύ δύσκολο να ανταπεξέλθουν στις απαιτήσεις και την πίεση των "αρπακτικών".

Επισημαίνεται ότι, κατά την περίοδο της εφηβείας, τα νεαρά άτομα κάνουν την "προσωπική τους επανάσταση". Αυτή η στάση ανεξαρτησίας και η αναζήτηση νέων γνωριμιών μέσω

Διαδικτύου καθιστούν τους εφήβους την πιο ευαίσθητη ομάδα στο ζήτημα της παιδικής πορνογραφίας, αλλά και της σεξουαλικής παρενόχλησης.

Συχνά τέτοιου είδους ιστοχώροι θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο διαδίκτυο, εξαιτίας τόσο της δημόσιας φύσης της συζήτησης όσο και της λανθασμένης εκτίμησης των παιδιών, ότι διατηρείται η ανωνυμία τους. Τα "αρπακτικά" ξεκινούν συζητήσεις με τα πιθανά θύματα, με σκοπό να αναπτύξουν μια φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντά τους, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Οι συζητήσεις μπορεί να διαρκέσουν ημέρες, εβδομάδες, ακόμα και μήνες, μέχρι το αρπακτικό να αποκτήσει την εμπιστοσύνη του παιδιού. Στη συνέχεια, προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και τους στέλνουν φωτογραφίες ως κάτι το αποδεκτό και το φυσιολογικό. Αυτή η τακτική αποσκοπεί στο να υπονομεύσει την απροθυμία των παιδιών να λάβουν μέρος σε σεξουαλική επαφή, αλλά και αποτρέψει το θύμα από το να ζητήσει βοήθεια από γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

Συνήθως τα "αρπακτικά" είναι άτομα υπεράνω πάσης υποψίας, που πιθανόν έχουν και τη δική τους οικογένεια: φιλήσυχοι, ευυπόληπτοι, μορφωμένοι , επιφανείς, οικονομικά ευκατάστατοι, π.χ. επιστήμονες, δάσκαλοι, επιχειρηματίες κ.α. Δεν διστάζουν να εκμεταλλευτούν τη θέση τους, αλλά και τη σχέση τους (συγγενείς) για να ικανοποιήσουν το αρρωστημένο τους πάθος.

Συνήθως, τα "αρπακτικά" έχουν παιδοφιλικές τάσεις. Οι παιδόφιλοι που δεν μπορούν να έχουν πρόσβαση σε ανήλικα παιδιά ικανοποιούν τις ανάγκες και το πάθος τους μέσα από το Διαδίκτυο, που τους δίνει πρόσβαση σε παιδικό πορνογραφικό υλικό το οποίο ικανοποιεί τις σεξουαλικές τους ανάγκες.

Πως λειτουργούν τα κυκλώματα;

Πρόκειται για "κλειστές ομάδες", οι οποίες επικοινωνούν μέσω ομάδων συζήτησης (new groups), μέσω δωματίων επικοινωνίας (chat rooms) ή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails).

Πάγια τακτική των κυκλωμάτων που διακινούν υλικό, είναι η χρήση παραπλανητικών φωτογραφιών στην αρχική σελίδα των ιστοσελίδων. Οι ιστοσελίδες στις οποίες "ανεβάζουν" πορνογραφικό υλικό ανηλίκων είναι "καμουφλαρισμένες" ώστε να μην εντοπίζονται (είναι

αδύνατον με τη χρήση μιας μηχανής αναζήτησης). Δημιουργούν βίντεο στα οποία αναμειγνύουν πορνογραφία ενηλίκων μαζί με ανηλίκων, για να δυσκολεύουν τον εντοπισμό τους.

6.8 Πορνογραφία ανηλίκων

Αποτελεί αδιαμφισβήτητα μια ειδεχθή εγκληματική δραστηριότητα, η οποία τα τελευταία χρόνια λαμβάνει έντονη δραστηριότητα και στη χώρα μας εντείνοντας την προσπάθεια των διωκτικών αρχών για τον περιορισμό του φαινομένου.

Το υλικό πορνογραφίας ανηλίκων, που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή και οποιασδήποτε άλλης μορφής πολυμέσων.

Οι πιο διαδεδομένοι τρόποι προμήθειας - διακίνησης του συγκεκριμένου υλικού είναι οι εξής:

α) Με την χρήση ειδικών Peer-to-Peer (P2P) προγραμμάτων τα οποία καθιστούν δυνατή την ανταλλαγή αρχείων μέσω διαδικτύου.

β) Αποστολή σεσημασμένου υλικού πορνογραφίας ανηλίκων μέσω ηλεκτρονικής αλληλογραφίας (email), ως επισυναπτόμενα αρχεία.

γ) Τέτοιου είδος υλικό φιλοξενείται και σε διάφορους δικτυακούς ιστοτόπους (forum) περιορισμένης πρόσβασης καθόσον απαιτείται συνήθως από τον εκάστοτε χρήστη η δημιουργία λογαριασμού για να εισέλθει.

δ) Με την χρήση ειδικών πλατφόρμών που εξυπηρετούν τον διαμοιρασμό αρχείων, μεταξύ υπολογιστών.

Κάθε χρήστης διαδικτύου κατά την προμήθεια - διακίνηση υλικού πορνογραφίας ανηλίκων μέσω διαδικτύου, αφήνει το ψηφιακό του στίγμα με την μορφή της IP διεύθυνσης, προσδιορίζοντας έτσι μοναδικά την ταυτότητα του, ενώ το τελευταίο διάστημα παρατηρούνται φαινόμενα τεχνικής απόκρυψης της ψηφιακής ταυτότητας των χρηστών με την χρήση εξειδικευμένων προγραμμάτων.

Στην ελληνική έννομη τάξη, ως υλικό πορνογραφίας ανηλίκων νοείται η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση, σε ηλεκτρονικό ή άλλο υλικό φορέα, κατά τρόπο που

προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

Σε βάρος των δραστών της συγκεκριμένης παραβατικής συμπεριφοράς στη χώρα μας, τυγχάνουν εφαρμογής οι γενικές διατάξεις του Π.Κ., ήτοι τα άρθρα 337 «Προσβολή της γενετήσιας αξιοπρέπειας», 339 «Αποπλάνηση παιδιών», 342 «Κατάχρηση ανηλίκων σε ασέλγεια», 348Α «Πορνογραφία ανηλίκων», 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους», 348Γ «Πορνογραφικές παραστάσεις ανηλίκων» και 351Α Π.Κ. «Ασέλγεια με ανήλικο έναντι αμοιβής» στα πλαίσια της αντιμετώπισης της εν γένει εγκληματικότητας.

Ειδικότερα: Το άρθρο 348Α Π.Κ ορίζει ότι:

1) Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πουλάει 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, πουλάει 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) Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ:

α. αν τελέστηκαν 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 της ηλικίας του».

γ. 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.».

Επιπροσθέτως, ποινικοποιήθηκε και η ζωντανή θέαση σε πραγματικό χρόνο υλικού πορνογραφίας ανηλίκων, μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών. Στο άρθρο 348Β Π.Κ., τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων εώς διακοσίων χιλιάδων ευρώ, 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. Στο άρθρο 348 Γ Π.Κ., τιμωρείται η εξώθηση ή παράσυρση ανηλίκου, προκειμένου να συμμετάσχει σε πορνογραφικές παραστάσεις ή η διοργάνωση αυτών. Ως πορνογραφική παράσταση νοείται η οργανωμένη απευθείας έκθεση, που προορίζεται για θέαση ή ακρόαση, μεταξύ άλλων και με χρήση της τεχνολογίας των πληροφοριών και επικοινωνιών α) ανηλίκου που επιδίδεται σε πραγματική ή εικονική πράξη γενετήσιου χαρακτήρα και β) των γεννητικών οργάνων ή του σώματος εν γένει, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση.

Επισημαίνεται δε ότι, τα αδικήματα που προβλέπονται στο άρθρο 348Α «Πορνογραφία ανηλίκων», 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους», 348Γ «Πορνογραφικές παραστάσεις ανηλίκων», 339 «Αποπλάνηση παιδιών» παρ.1α,1β, και 342 «Κατάχρηση ανηλίκων σε ασέλγεια» παρ.1,2 έχουν συμπεριληφθεί στον κατάλογο των αδικημάτων για τα οποία επιτρέπεται η άρση του απορρήτου (άρθρο 4 του Ν. 2225/1994).

6.9 Cyber-bullying

Ο εκφοβισμός μέσω διαδικτύου (Cyber-bullying) είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, Tablets, κινητών τηλεφώνων).

Ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό, αφού υπάρχει θύτης, θύμα και παρατηρητές. Έχει όμως και μερικές σημαντικές διαφορές, όπως:

- μπορεί να φτάσει σε πολύ λίγο χρόνο σε πολλούς παραλήπτες.
- ο θύτης νιώθει ότι μπορεί να παραμείνει ανώνυμος.

- η έλλειψη προσωπικής επαφής με το θύμα κάνει το δράστη σκληρότερο.
- το θύμα πλήττεται στο σπίτι και στον προσωπικό του χώρο.

Τα μέσα που χρησιμοποιούνται για την παρενόχληση μέσω διαδικτύου είναι:

- το ηλεκτρονικό ταχυδρομείο (e-mail)
- τα γραπτά μηνύματα (sms)
- μέσα κοινωνικής δικτύωσης (social media)
- δωμάτια επικοινωνίας (chat rooms)
- ιστολόγια (blogs)
- διαδικτυακά παιχνίδια (internet games)

Πως εκδηλώνεται το Cyber-bullying.

Αυτοί που ασκούν εκφοβισμό, χρησιμοποιούν τις νέες τεχνολογίες για να παρενοχλήσουν, να απειλήσουν, να εκφοβίσουν, να εκβιάσουν, να δυσφημήσουν και, σε μερικές περιπτώσεις, να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο (σε instant messengers ή chatrooms).

- Η κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση.

- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση σε τρίτους, σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λ.π.

- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή.

- Χρήση του ονόματος ξένου χρήστη με σκοπό την διάδοση φημών για κάποιον τρίτο (κλοπή ταυτότητας).

- Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

- Η αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών.

- Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

6.10 Παιδική πορνογραφία και επιπτώσεις του προβλήματος

Από ότι ως τώρα έχει αναδειχθεί, γίνεται γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Ότι αφορά τα παιδιά-θύματα η παραγωγή και εμπορία τέτοιου υλικού είναι άμεσα συνδεδεμένη με την κακοποίηση των παιδιών αυτών. Τα παιδιά βρίσκονται σε κίνδυνο σεξουαλικής κακοποίησης είτε από τις δραστηριότητες των δικτύων παιδεραστών είτε και από εκείνους που επιδιώκουν κέρδος από την εκμετάλλευσή τους.

Το πρόβλημα τόσο της σεξουαλικής κακοποίησης και εκμετάλλευσης όσο και της διαταραγμένης σεξουαλικής συμπεριφοράς, είναι ιδιαίτερα έντονο ιδίως όταν πρόκειται για ευάλωτες ομάδες παιδιών. Στις περιπτώσεις αυτές, η παιδική πορνεία, οι απαγωγές και η παρακίνηση σε σεξουαλικές δραστηριότητες προς εκμετάλλευση, παραμένουν υπαρκτοί κίνδυνοι, όταν συνδυάζονται με παραμέτρους όπως είναι για παράδειγμα, η αύξηση του αριθμού άστεγων νέων παιδιών και αυτών που ζουν στα όρια της φτώχειας. Σε αυξημένο κίνδυνο κακοποίησης εκτίθενται επίσης παιδιά με κάποια αναπηρία. Τα παιδιά αυτά είναι ακόμη πιο ευάλωτα σαν αποτέλεσμα της εξάρτησής τους σε ορισμένες περιπτώσεις και σε άλλες εξαιτίας της διαβίωσής τους μέσα σε ιδρύματα.

Ανεξάρτητα από όλα αυτά, αποδεικνύεται ότι στα παιδιά που εμπλέκονται σε τέτοιες δραστηριότητες δημιουργούνται επικίνδυνες επιρροές, κινδυνεύοντας έτσι ως ενήλικες πλέον να παρουσιάσουν συμπτώματα διαταραγμένης σεξουαλικής συμπεριφοράς. Σύμφωνα με μελετητές ακόμα και η διαρκής έκθεση τους στην επονομαζόμενη "πορνογραφία ενηλίκων" μπορεί να δημιουργήσει προβλήματα σεξουαλικής συμπεριφοράς ως ενήλικες, η οποία τα απευαισθητοποιεί και τα αποπλανά με τις προτροπές για σεξουαλικές δραστηριότητες που περιέχει.

Αναφορικά με την συνάφεια του πορνογραφικού υλικού και του ρόλο του στην διάπραξη σεξουαλικού αδικήματος γενικότερα, θα πρέπει το σημείο αυτό να αναδειχθεί ότι υπάρχουν αμφιλεγόμενες απόψεις. Η επισκόπηση της σχετικής βιβλιογραφίας φαίνεται να αποκαλύπτει ότι αν και μια μειονότητα παραβατών που σχετίζονται με σεξουαλικά αδικήματα αναφέρουν χρήση πορνογραφίας, εντούτοις δεν φαίνεται να υπάρχει κάποια θετική συνάφεια μεταξύ των

πορνογραφικών εμπειριών - ανεξάρτητα αν οι ίδιες συνέβησαν στην παιδική ηλικία ή αργότερα - ανάμεσα σε παραβάτες αυτού του είδους και σε μη παραβάτες.

Στο ίδιο μήκος κύματος, αν και οι περιπτώσεις των βιαστών δεν σχετίζονται με την διακίνηση πορνογραφικού υλικού, βρέθηκαν όμως αμφιλεγόμενες συσχετίσεις. Με άλλα λόγια και σύμφωνα με τα ερευνητικά δεδομένα αποκαλύπτεται ότι το πορνογραφικό υλικό δομεί μορφές κοινωνικής μάθησης, δεν σχετίζεται το ίδιο κατά κανόνα με σεξουαλικά αδικήματα. Στην προσπάθεια μείωσης των σεξουαλικών αδικημάτων αυτό που φαίνεται να παίζει σημαντικό ρόλο είναι το είδος αυτών των εμπειριών και το σχετικό background των παραβατών γενικότερα.

6.11 Παιδική πορνογραφία και πρόληψη του προβλήματος

Πέρα από την παιδική πορνογραφία που αποτελεί ξεκάθαρα ποινικό αδίκημα ενδιαφέρον παρουσιάζει από παιδαγωγική σκοπιά εκείνο το υλικό το οποίο ή είναι επιβλαβές ή κινείται στην γκρίζα ζώνη και επηρεάζει μακροπρόθεσμα και κάτω από ειδικές συνθήκες (μιντιακή κοινωνικοποίηση) τους νέους διαμορφώνοντας στάσεις και κοινωνικές αξίες.

Σε επίπεδο ευαισθητοποίησης των πολιτών έχουν δραστηριοποιηθεί παγκοσμίως άτομα και φορείς και κατά καιρούς έχουν προταθεί και παρθεί διάφορα μέτρα. Όσον αφορά την Ελλάδα και την ασφαλή χρήση του Διαδικτύου συναντά κανείς δύο βασικές ιδιωτικές δράσεις. Η πρώτη είναι η Safeline του Ελληνικού όργανου αυτορρύθμισης Safenet με την υποστήριξη του Ευρωπαϊκού προγράμματος "Σχέδιο Δράσης για την Ασφαλέστερη Χρήση του Διαδικτύου" (http://europa.eu.int/saferinternet/Action Plan). Ο βασικός ρόλος της Safeline είναι μιας Ανοικτής Γραμμής επικοινωνίας, ένας ρόλος μεσολαβητή με άλλα λόγια μεταξύ των πολιτών και των ελληνικών αστυνομικών αρχών, λαμβάνοντας τις καταγγελίες των πρώτων και προωθώντας τις στις αστυνομικές αρχές.

Η δεύτερη δράση είναι της ελληνικής οργάνωσης καταναλωτών ΕΚΑΤΟ. Η ΕΚΑΤΟ λειτουργεί ως επίσημη ιστοσελίδα που έχει σαν στόχο την ασφαλή πλοήγηση των παιδιών στο Διαδίκτυο. Τα παιδιά μπορούν μεταξύ άλλων να βρούν εύχρηστες και κατανοητές πληροφορίες για να προστατευτούν από τους κινδύνους που κρύβονται στο Διαδίκτυο, να δηλώσουν και να αξιολογήσουν τις αγαπημένες τους ιστοσελίδες, να στείλουν τις ερωτήσεις και τα σχόλιά τους. Η ΕΚΑΤΟ έχει πραγματοποιήσει μια σειρά από έρευνες, μέσα από τις οποίες καταγράφεται η σχέση των μαθητών με το Διαδίκτυο. http://www.ekato.org/gr/.

Επιπλέον το υπουργείο Παιδείας σε συνεργασία με το Παιδαγωγικό Ινστιτούτο έχει εντάξει στους στόχους του την αξιοποίηση του Διαδικτύου στην εκπαίδευση. Το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ) καλύπτει τα σχολεία της Πρωτοβάθμιας Εκπαίδευσης και Δευτεροβάθμιας Εκπαίδευσης, παρέχοντας υπηρεσίες ασφάλειας προς τους χρήστες της εκπαιδευτικής κοινότητας, όπως είναι ο Έλεγχος Περιεχομένου (Web-Filtering). Πρακτικά αυτό σημαίνει εγκατάσταση λογισμικών φίλτρων στους υπολογιστές που μπορεί να αποκλείσουν την προσπέλαση σε τόπους του κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο. Όμως, η αποτελεσματικότητα του φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού αλλά και από την επιθυμία των χρηστών να εγκαταστήσουν στους υπολογιστές τους οικειοθελώς αντίστοιχο λογισμικό φιλτραρίσματος.

Επιπρόσθετα, σε προληπτικό και συμβουλευτικό επίπεδο, εντείνεται η προσπάθεια της ενημέρωσης των εκπαιδευτικών, γονιών αλλά και των μαθητών για τη σωστή χρήση του διαδικτύου. Στο σημείο αυτό και ότι αφορά τους εκπαιδευτικούς και ιδιαίτερα την προσέγγιση των νέων μέσων από πλευράς διδακτικής απαιτείται ουσιαστική επιμόρφωση των εκπαιδευτικών. Μια πτυχή αποτελεί και η επιμόρφωση των εκπαιδευτικών στη δημιουργία νέων μαθησιακών περιβάλλοντων με στόχο τη χρήση των νέων μέσων. Αν και σε πρώτο επίπεδο προβάλλεται η ανάγκη για μάθηση με στόχο εργαλειακό ως προς την χρήση επιβάλλεται όμως το κοινό αυτών των χρηστών ¨να μυηθεί σε μορφές κριτικής και πραγματιστικής χρήσης των Νέων Μέσων¨.

Η παιδική πορνογραφία και κατ΄ επέκταση το φαινόμενο της σεξουαλικής κακοποίησης και εκμετάλλευσης των παιδιών στο διαδίκτυο παραμένει ένα παγκόσμιο και σοβαρό πρόβλημα. Αν και το ζήτημα της παιδικής πορνογραφίας στο διαδίκτυο διευκολύνεται με τις νέες τεχνολογίες δεν παύει όμως να αντανακλά επικρατούσες αντιλήψεις και κυρίαρχες συμπεριφορές.

Παρά ταύτα η αστυνόμευση του διαδικτυακού περιεχομένου παραμένει μια δύσκολη υπόθεση καθώς προσκρούει:

1. Σε θέματα προστασίας της ελευθερίας του λόγου και του προσωπικού απορρήτου.

2. Στο μέγεθος του διαδικτύου σε συνδυασμό με την έλλειψη αποτελεσματικού ελέγχου και την ανωνυμία την οποία προσφέρει το μέσο.

3. Η «αγορά» παιδοπορνογραφικού υλικού διεθνώς έχει τζίρο δεκάδων δισ. δολαρίων ετησίως.

4. Στην έλλειψη ενιαίου νομοθετικού πλαισίου διεθνώς για την αντιμετώπιση του φαινόμενου.

5. Στις τεχνολογικές εξελίξεις στους τομείς παραγωγής και διανομής περιεχομένου και της διασφάλισης ανωνυμίας.

Μια ευρύτερη προσέγγιση του προβλήματος που σχετίζεται με την προστασία των νέων στο διαδίκτυο αναδεικνύει το σημαντικό ρόλο που μπορεί να διαδραματίσει η μιντιακή αγωγή για την ευαισθητοποίηση των νέων αλλά και στην προώθηση της μιντιακής ικανότητας τους.

ΚΕΦΑΛΑΙΟ 7:

ΝΟΜΟΘΕΣΙΑ

7.1 Το πρόβλημα της νομικής προσέγγισης θεμάτων που αφορούν τον κυβερνοχώρο

Η προσέγγιση των νομικών θεμάτων που αφορούν τον κυβερνοχώρο ενέχει πολλές δυσκολίες καθώς προϋποθέτει όχι μόνο νομικές αλλά, μέχρι ένα βαθμό τουλάχιστον, και τεχνικές γνώσεις. Ένα εξίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με τη νομική πλευρά του θέματος από ποινική άποψη είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων και αυτή οφείλεται στο γεγονός πως το έγκλημα στον κυβερνοχώρο αποτελεί μια νέα μορφή εγκλήματος.

Ένα επιπλέον πρόβλημα έχει να κάνει με την ελληνική νομική ορολογία. Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη, κατά κανόνα, στην αγγλική γλώσσα και η αντίστοιχη μεταφορά αυτών των όρων στα ελληνικά δεν είναι ούτε εύκολη ούτε δόκιμη. Το πρόβλημα αυτό της ορολογίας παρουσιάζεται όχι μόνο στο πεδίο του ουσιαστικού ποινικού δικαίου αλλά και στον αντίστοιχο του ποινικού δικονομικού δικαίου. Αυτό που έχει αποφασισθεί από τα κρατικά νομικά μέσα για την αντιμετώπιση αυτού του θέματος είναι να ακολουθηθεί η παραδοσιακή δικονομική ορολογία και μόνο όπου και όταν κριθεί αναγκαίο να ακολουθηθεί μια μικτή, δηλαδή σε μια υπόθεση ηλεκτρονικού εγκλήματος να αναφερθούν τόσο οι παραδοσιακοί όροι όσο και οι τεχνικοί, για παράδειγμα οι όροι έρευνα ή παρόμοια πρόσβαση (search or similar access), κατάσχεση ή παρόμοια διαφύλαξη (seize or similar secure).

Τέλος, τα ηλεκτρονικά αποδεικτικά μέσα δεν μπορούν σε καμία περίπτωση να ταυτιστούν με τα παραδοσιακά αποδεικτικά μέσα και αυτό γιατί οι αποδείξεις ενός εγκλήματος που λαμβάνει χώρα στο «φυσικό» κόσμο έχουν, κατά κανόνα, υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, οι ηλεκτρονικές αποδείξεις, δεν είναι χειροπιαστές,

μπορεί να τις κατευθύνει ή να τις διαχειριστεί κάποιος από μακριά, να αλλάξει την μορφή και το περιεχόμενο τους ακόμα και να τις εξαφανίσει με το πάτημα ενός πλήκτρου.

7.2 Δικαιοδοσία στο Διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις.

Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες:

1. Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.

2. Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

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

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

7.3 Αρχές που εποπτεύουν την προστασία του Διαδικτύου στην Ελλάδα

Στην Ελλάδα, λειτουργούν τρεις ανεξάρτητες αρχές που εποπτεύουν σε ζητήματα ασφάλειας και προστασίας στο διαδίκτυο και στις επικοινωνίες γενικότερα και σε αυτές μπορούν να αναφερθούν σχετικά προβλήματα. Αυτές είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ), η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) . Και οι τρεις αυτοί φορείς έχουν το δικαίωμα να επιβάλλουν ιδιαίτερους όρους σχετικά με την τήρηση του απορρήτου των τηλεπικοινωνιών στις εταιρείες που διαθέτουν άδεια χρήσης τηλεπικοινωνιών δραστηριοτήτων και σε αυτές υπάγονται και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's).

1) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.).

Η Αρχή Προστασίας Δεδομένων προσωπικού Χαρακτήρα, λειτουργεί από το 1977 σύμφωνα με τις διατάξεις του ν.2472/1997 και έχει ως αποστολή την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδικτύου. Σύμφωνα με το νόμο για την «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», ν.2774/1999, οι ιστοσελίδες που συγκεντρώνουν προσωπικά στοιχεία των επισκεπτών τους, όπως για παράδειγμα ονόματα, τηλέφωνα, διευθύνσεις e-mail κ.α., έχουν νομική υποχρέωση να τους ενημερώνουν για τον σκοπό που συλλέγονται αυτά τα στοιχεία καθώς και για το αν αυτά τα στοιχεία διατίθενται σε τρίτους.

2) Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.).

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του ν.3115/2003. Σκοπός της Α.Δ.Α.Ε. είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Στις αρμοδιότητες της Α.Δ.Α.Ε. περιλαμβάνεται το δικαίωμα διενέργειας ελέγχων, αποδοχής και εξέτασης καταγγελιών αλλά και έκδοσης κανονιστικών κειμένων. Οι σημαντικότερες από αυτές είναι :

1. Να διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

2. Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.

3. Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.

4. Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

3) Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Ε.Τ.) αποτελεί σημαντική αρχή στον χώρο του διαδικτύου καθώς αποτελεί την εθνική ρυθμιστική αρχή σε θέματα τηλεπικοινωνιών. Είναι ανεξάρτητη διοικητική αρχή με έδρα την Αθήνα και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας. Τα μέλη της Ε.Ε.Ε.Τ. διορίζονται με απόφαση του Υπουργού Μεταφορών και Επικοινωνιών μετά από προηγούμενη επιλογή τους από την Διάσκεψη των Προέδρων της Βουλής με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της. Ως μέλη της Ε.Ε.Ε.Τ. επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαμβάνουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα. Κατά την εκτέλεση των καθηκόντων τους, τα μέλη της Ε.Ε.Ε.Τ. δεσμεύονται από τον νόμο, έχουν δε υποχρέωση τήρησης των αρχείων αντικειμενικότητας και αμεροληψίας. Επίσης, υποχρεούνται στην τήρηση εμπιστευτικότητας, εμπορικών πληροφοριών για τέσσερα χρόνια μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Ε.Τ.

Η Ε.Ε.Ε.Τ. χορηγεί άδειες σε Πάροχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's), ενώ ρυθμίζει τον τομέα των τηλεπικοινωνιών, ασκώντας παράλληλα και έλεγχο σε αυτόν, και εποπτεύεται την τηλεπικοινωνιακή αγορά.

7.4 Μέτρα προστασίας κατά την πρόσβαση στο Διαδίκτυο

Κατά την πλοήγηση των χρηστών στους χώρους του Διαδικτύου καλό είναι να λαμβάνονται κάποια μέτρα ασφάλειας. Έτσι, λοιπόν, θα πρέπει να αποφεύγεται:

1. Η αποκάλυψη των προσωπικών ευαίσθητων δεδομένων σε τρίτους.

2. Να μην υπάρχει εμπιστοσύνη σε e-mails ή ιστοσελίδες που δεν έχουν αποδείξει την ταυτότητα τους.

3. Να αποφεύγεται η συμπλήρωση φορμών με οικονομικά στοιχεία, αριθμό ταυτότητας, Α.Φ.Μ., ημερομηνία γέννησης και λοιπά προσωπικά στοιχεία και η αποστολή τους μέσω ηλεκτρονικού ταχυδρομείου χωρίς να είναι κρυπτογραφημένες.

4. Να αποφεύγεται η επίσκεψη σε ύποπτα sites.

5. Όσο για τις on-line συναλλαγές, οι χρήστες θα πρέπει να βεβαιώνονται ότι το ηλεκτρονικό κατάστημα που συναλλάσσονται είναι αξιόπιστο (ψηφιακά υπογεγραμμένο από κάποιο ανεξάρτητο φορέα ή αρχή πιστοποίησης), έχει καλή φήμη και εφαρμόζει μηχανισμούς ασφαλείας όπως κρυπτογραφημένη επικοινωνία μέσω του πρωτοκόλλου SSL (Secure Socket Layer).

6. Εφόσον κριθεί αναγκαία η χρησιμοποίηση κάποιας οικονομικής κάρτας, καλό είναι αυτή η χρήση να γίνεται μέσω χρεωστικών καρτών ή προπληρωμένων πιστωτικών καρτών.

7. Οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί όσον αφορά τις πληροφορίες που αποκαλύπτουν. Υπάρχουν μέθοδοι υποκλοπής προσωπικών δεδομένων που δεν στηρίζονται σε τεχνολογικές αδυναμίες αλλά στην ικανότητα ενός επίδοξου hacker να αντλήσει προσωπικά στοιχεία από έναν ανυποψίαστο χρήστη. Ο πιο διάσημος hacker που χρησιμοποίησε τέτοιες μεθόδους είναι ο Kevin Mitnick ο οποίος μέσω τις πειθούς κατάφερνε να αποκαλύπτει ονόματα χρήσης (user names) και κωδικούς (passwords) από ανυποψίαστους χρήστες όπως γραμματείς και τεχνικούς.

7.5 Μέτρα προστασίας των επιχειρήσεων

Τίποτα δεν μπορεί να εξασφαλίσει απόλυτη προστασία από τις απειλές που υπάρχουν στο Internet κάνοντας κάθε μέρα την αναζήτηση ασφάλειας μια όλο και πιο περίπλοκη υπόθεση όχι μόνο για τους απλούς μεμονωμένους χρήστες του διαδικτύου αλλά ακόμα και για τις επιχειρήσεις, ανεξαρτήτου μεγέθους. Τα μέτρα, λοιπόν, που μπορούν να πάρουν οι επιχειρήσεις για να αντιμετωπίσουν τους κινδύνους του διαδικτύου είναι:

1. Ενημέρωση: Παρακολούθηση δικτυακών τόπων με προγράμματα προστασίας και εγγραφή σε mailing list που ενημερώνουν μέσω ηλεκτρονικού ταχυδρομείου για τις νέες απειλές. Είναι βασικό να γνωρίζουν οι χρήστες τις απειλές πριν διαδοθούν ευρέως. Έτσι μπορούν να τις αντιμετωπίσουν καλύτερα.

2. Επιλογή «δύσκολων» συνθημάτων: Τα προγράμματα των hacker στο Διαδίκτυο περιλαμβάνουν δεκάδες χιλιάδες πιθανών συνθημάτων. Με αυτά τα προγράμματα, όταν το σύνθημα είναι συνηθισμένο και απλό να βρεθεί, οι hacker μπορούν εύκολα να εισβάλουν στα συστήματα των υπολογιστών. Ένα ιδανικό σύνθημα μπορεί να είναι ο συνδυασμός συμβόλων και αριθμών.

3. Συχνή εναλλαγή συνθήματος: Με το να εναλλάσσονται περιοδικά τα συνθήματα, ακόμα και να το βρουν οι hackers, ήδη η επιχείρηση θα χρησιμοποιεί ένα καινούργιο.

4. Βεβαίωση ότι το υπάρχον πρόγραμμα προστασίας που υπάρχει έχει ενημερωθεί: Πολλές εταιρείες λογισμικού προσφέρουν ανανεώσεις και συμπληρώματα στα προγράμματα ασφαλείας που παρέχουν, για να μπορούν αυτά να ανταποκρίνονται στις νέες απειλές. Οι επιχειρήσεις θα πρέπει να ελέγχουν τακτικά το πρόγραμμα ασφαλείας που διαθέτουν και να το ανανεώνουν για να μπορεί να αντιμετωπίζει τις απειλές που εμφανίζονται.

5. Προστασία συστημάτων ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί η επιχείρηση: Επιλογή συστήματος e-mail που μπορούν να «μπλοκάρουν» ιούς που μπορεί να περιέχονται σε mail που λαμβάνει μια επιχείρηση. Οι υπάλληλοι της επιχείρησης θα πρέπει να εκπαιδευθούν για να μην ανοίγουν συνημμένα αρχεία (file attachments) από πηγές που δεν γνωρίζουν, και που είναι ο συνηθέστερος τρόπος για να εισέλθει ένας ιός στον υπολογιστή.

6. Δοκιμή υπάρχοντος συστήματος για αδυναμίες: Η πραγματοποίηση τακτικών τεστ για τυχόν αδυναμίες του συστήματος μπορούν να γίνουν τόσο μέσα από το δίκτυο της εταιρείας όσο και με εργαλεία που μπορούν να βρεθούν στο διαδίκτυο. Για παράδειγμα, είναι δυνατόν με ένα

πρόγραμμα που «σπάει» συνθήματα να φανεί αν πρέπει να αλλαχθούν τα συνθήματα πρόσβασης των χρηστών της εταιρείας.

7. Εκπαίδευση υπαλλήλων: Οι υπάλληλοι της εταιρείας πρέπει να κατανοήσουν πόσο σημαντικό είναι εταιρικά στοιχεία και πληροφορίες να παραμένουν εμπιστευτικά και κυρίως να μην κυκλοφορούν ευρέως στο Διαδίκτυο.

8. Ενημέρωση των προγραμμάτων και του λειτουργικού συστήματος: Η ενημέρωση του λειτουργικού συστήματος και των προγραμμάτων και η εγκατάσταση των τελευταίων ενημερώσεων κάνουν το σύστημα πιο σταθερό και οι νέες συμπληρώσεις στα προγράμματα ασφαλείας θα λειτουργούν καλύτερα.

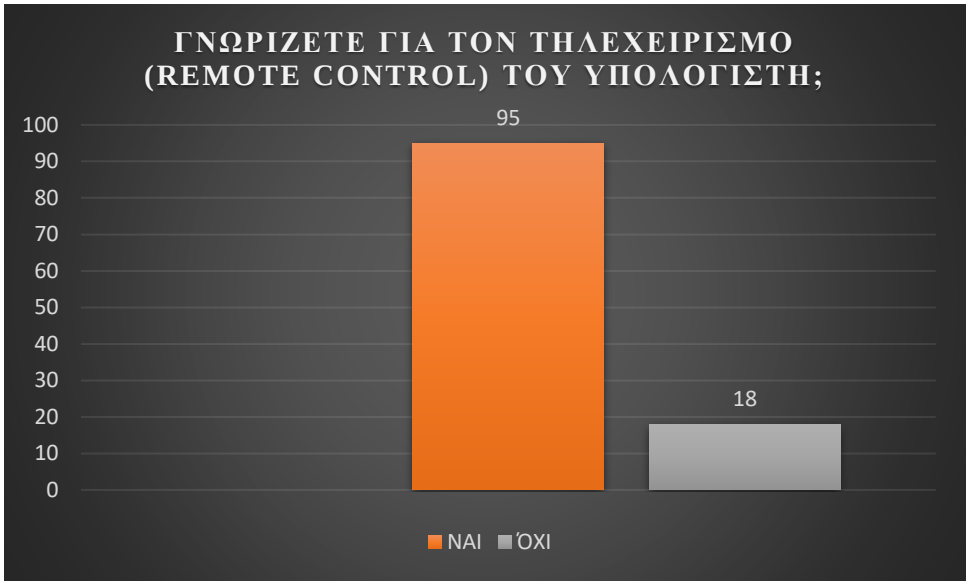
9. Αντι-ιϊκά παντού: Όλα τα συστήματα, από φορητούς υπολογιστές μέχρι τους εξυπηρετητές (servers) της επιχείρησης θα πρέπει να προστατεύονται από ιούς.

10. Δημιουργία Εταιρικής Πολιτικής Ασφάλειας: Η καταγραφή της πολιτικής ασφάλειας της επιχείρησης και η ανανέωση της ανά τακτά χρονικά διαστήματα μπορεί να ανταποκρίνεται καλύτερα σε νέες απειλές που προκύπτουν.

ΚΕΦΑΛΑΙΟ 8:

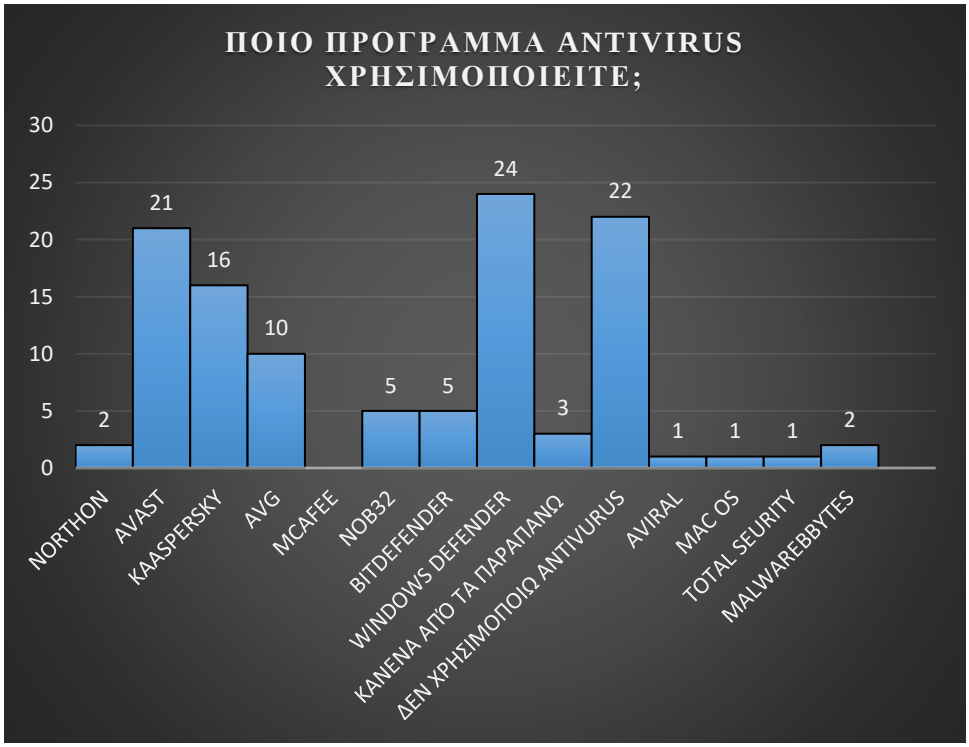
ΔΙΑΓΡΑΜΜΑΤΑ ΕΡΕΥΝΑΣ

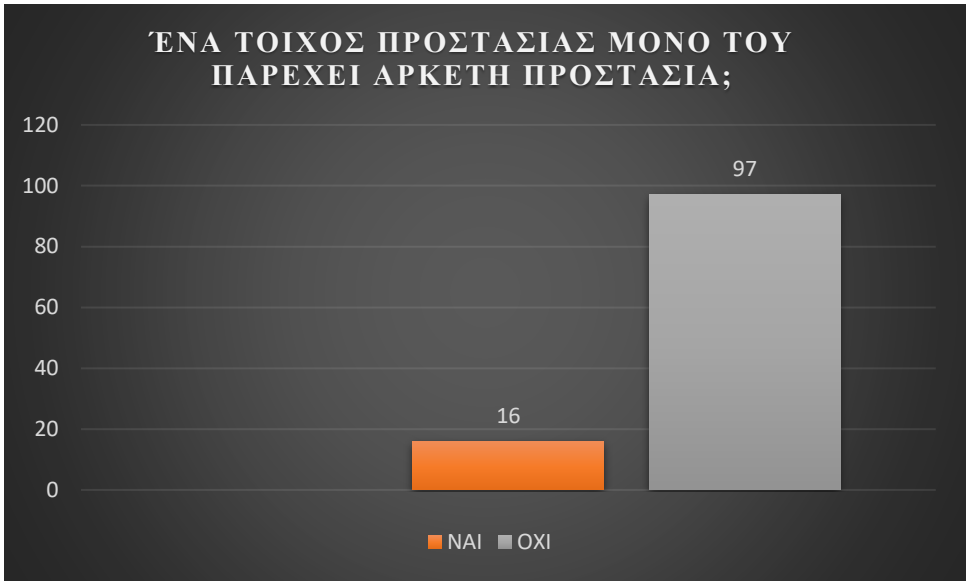
8.1 Διαγράμματα έρευνας


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΟΝ ΤΗΛΕΧΕΙΡΙΣΜΟ (REMOTE CONTROL) ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ;
100
90
80
70
60
50
40
30
20
10
0
95
18
ΝΑΙ
ΟΧΙ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΗΝ ΔΙΑΚΙΝΗΣΗ ΝΑΡΚΩΤΙΚΩΝ, ΕΜΠΟΡΙΟ ΟΡΓΑΝΩΝ, ΑΥΤΟΚΤΟΝΙΕΣ;
120
100
80
60
40
20
0
110
3
ΝΑΙ
ΟΧΙ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΗΝ ΠΛΑΣΤΟΓΡΑΦΙΑ;
120
100
80
60
40
20
0
111
2
ΝΑΙ
ΟΧΙ

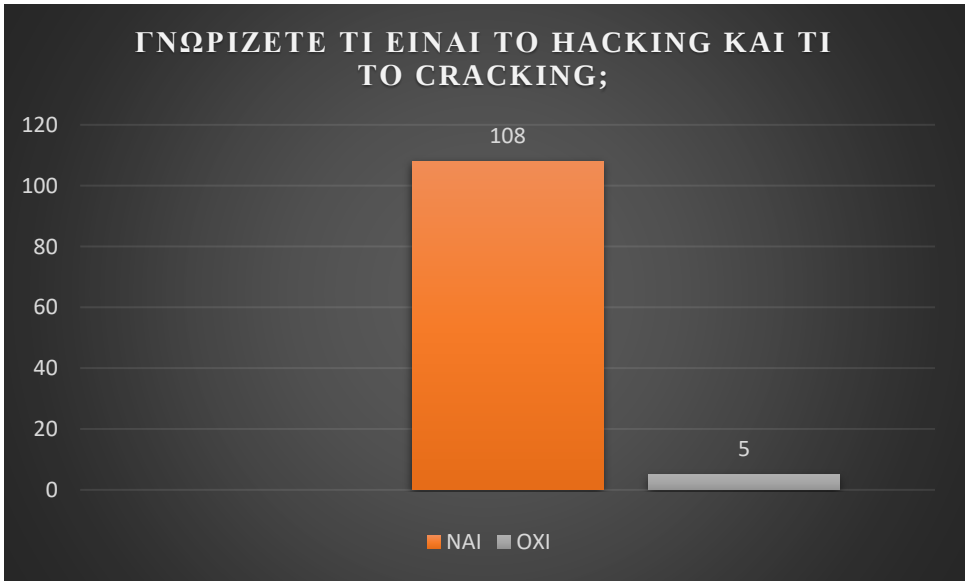

ΠΟΙΟ ΠΡΟΓΡΑΜΜΑ ANTIVIRUS ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ;
30
25
20
15
10
5
0
2
21
16
10
5
5
24
3
22
1
1
1
2
NORTHON
AVAST
KAASPERSKY
AVG
MCAFEE
NOB32
BITDEFENDER
WINDOWS DEFENDER
ΚΑΝΕΝΑ ΑΠΟ ΤΑ ΠΑΡΑΠΑΝΩ
ΔΕΝ ΧΡΗΣΙΜΟΠΟΙΩ ANTIVIURUS
AVIRAL
MAC OS
TOTAL SEURITY
MALWAREBBYTES


ΈΝΑ ΤΟΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ ΜΟΝΟ ΤΟΥ ΠΑΡΕΧΕΙ ΑΡΚΕΤΗ ΠΡΟΣΤΑΣΙΑ;
120
100
80
60
40
20
0
16
97
ΝΑΙ
ΟΧΙ


ΓΝΩΡΙΖΕΤΕ ΤΙ ΕΙΝΑΙ Ο ΕΠΙΦΑΝΕΙΑΚΟΣ ΙΣΤΟΣ (SURFACE WEB), ΒΑΘΥΣ ΙΣΤΟΣ (DEEP WEB) ΚΑΙ ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ (DARK WEB);
100
80
60
40
20
0
94
19
ΝΑΙ
ΟΧΙ

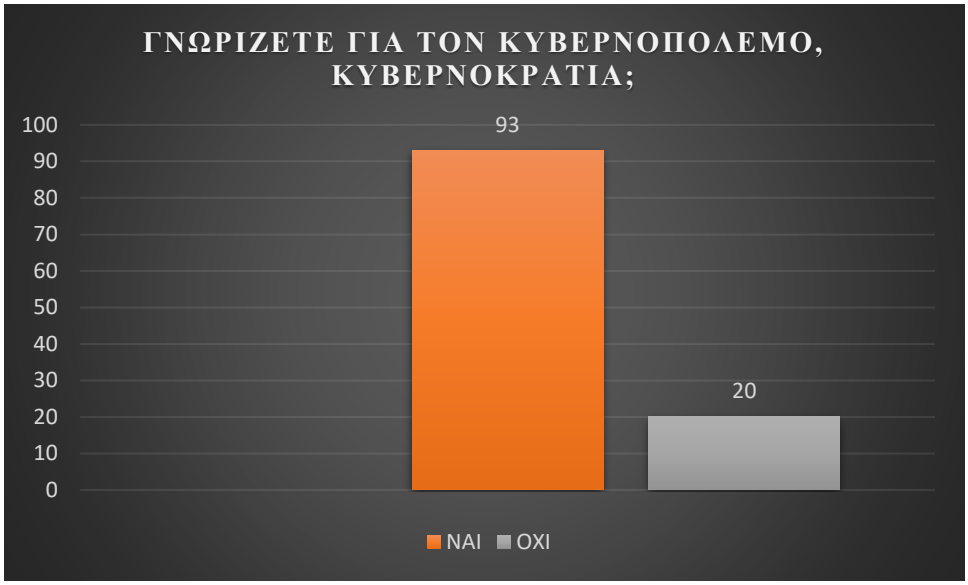

Ο ΣΩΣΤΟΣ ΤΡΟΠΟΣ ΣΥΝΤΑΞΗΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΠΡΕΠΕΙ ΝΑ ΠΕΡΙΛΑΜΒΑΝΕΙ:
120
100
80
60
40
20
0
9
103
1
ΑΡΙΘΜΟΥΣ ΚΑΙ ΓΡΑΜΜΑΤΑ
ΣΥΜΒΟΛΑ,ΑΡΙΘΜΟΥΣ,ΠΕΖΑ,ΚΕΦΑΛΑΙΑ
ΗΜΕΡΟΜΗΝΙΕΣ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΣΦΕΤΕΡΙΣΜΟ (CYBERSQUATTING) ΩΣ ΜΟΡΦΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ;
80
70
60
50
40
30
20
10
0
39
74
ΝΑΙ
ΟΧΙ

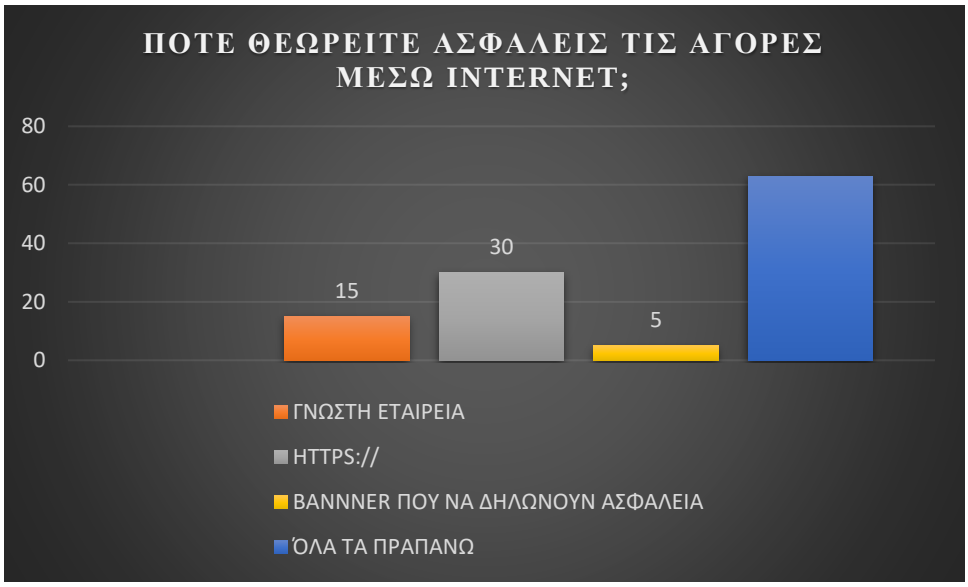

ΓΝΩΡΙΖΕΤΕ ΤΙ ΕΙΝΑΙ ΤΟ HACKING ΚΑΙ ΤΙ ΤΟ CRACKING;
120
100
80
60
40
20
0
108
5
ΝΑΙ
ΟΧΙ

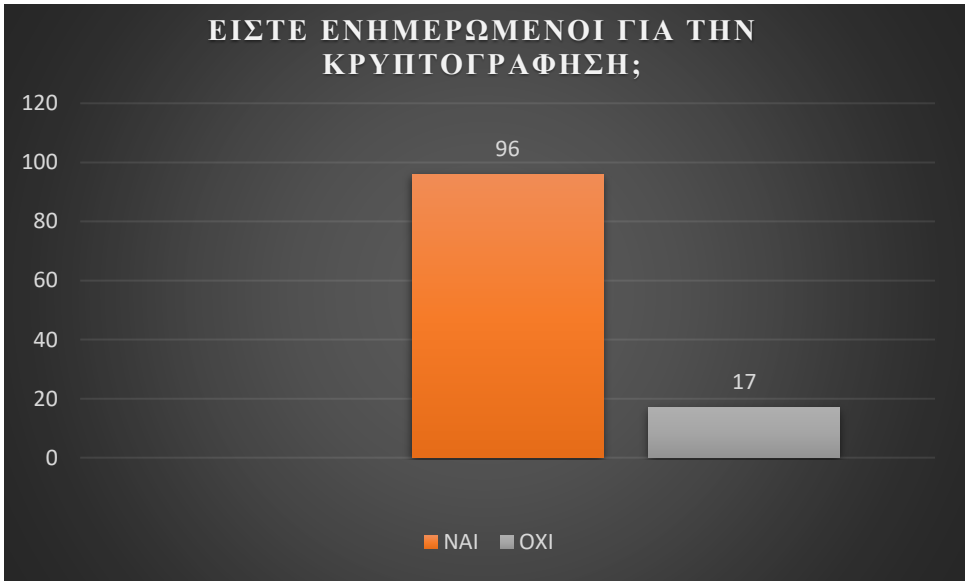

ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΑ COOKIES;
120
100
80
60
40
20
0
108
5
ΝΑΙ
ΌΧΙ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΗΝ ΥΠΟΚΛΟΠΗ ΑΡΧΕΙΩΝ Η/Υ;
120
100
80
60
40
20
0
110
3
1
ΝΑΙ
ΌΧΙ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΠΟΛΕΜΟ, ΚΥΒΕΡΝΟΚΡΑΤΙΑ;
100
90
80
70
60
50
40
30
20
10
0
93
20
ΝΑΙ
ΟΧΙ


ΓΝΩΡΙΖΕΤΕ ΓΙΑ ΤΗΝ ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ;
120
100
80
60
40
20
0
110
3
1
ΝΑΙ
ΌΧΙ





Συμπεράσματα Έρευνας

Τα βασικά συμπεράσματα της έρευνας είναι:

- Οι σπουδαστές ηλικίας 18-35 είναι ενημερωμένοι αρκετά καλά για την πλειοψηφία των διάφορων μορφών του Ηλεκτρονικού Εγκλήματος. Η πιο καλή ενημέρωση είναι για το Hacking, το Cracking, την υποκλοπή αρχείων, την διακίνηση ναρκωτικών, το εμπόριο οργάνων, τις αυτοκτονίες, τα Cookies, την πλαστογραφία και την παιδική

πορνογραφία (σε ποσοστά που κυμαίνονται από 95–97%). Δεν είναι επαρκώς ενημερωμένοι για τον Κυβερνοσφετερισμό (σε ποσοστό 65,6%).

- Από τα γνωστά antivirus προγράμματα το windows defender έχει την πρώτη θέση στις προτιμήσεις των σπουδαστών. Το 19,5% απάντησε ότι δεν χρησιμοποιεί antivirus. Ακολουθεί το avast, το kaspersky και το avg.
- Είναι καλά ενημερωμένοι για τον σωστό τρόπο σύνταξης κωδικών πρόσβασης και για την επιστήμη της Κρυπτογράφησης σε ποσοστό 84.96%, και για τον κυβερνοπόλεμο με ποσοστό 82,3%.
- Οι περισσότεροι σπουδαστές (ποσοστό 85,8%) γνωρίζουν για την λειτουργία των Firewalls.
- Το 26,5% νοιώθει ασφάλεια για τις αγορές τους μέσω internet όταν βλέπει μπροστά από το url της σελίδας το πρόθεμα (http://) ενώ το 13,3% όταν γνωρίζουν την εταιρεία,
- Ένα 4,4% εμπιστεύεται σελίδες με απλά διαφημιστικά banners που υπόσχονται αξιοπιστία και πάνω από τους μισούς 55,8% θέλει όλα τα παραπάνω ως προϋποθέσεις για να πραγματοποιήσει ηλεκτρονική αγορά.

Συνοψίζοντας όλα τα παραπάνω θα λέγαμε ότι τα άτομα ηλικίας 18-35 που σπουδάζουν σε ΙΕΚ, ΤΕΙ και πανεπιστήμια είναι αρκετά καλά ενημερωμένοι στην πλειοψηφία των θεμάτων σχετικά με το Ηλεκτρονικό Έγκλημα και τις μορφές του. Ακόμα συμπεραίνουμε ότι η χρήση του Internet για αγορές έχει καταφέρει να ξεπεράσει το παραδοσιακό εμπόριο. Στα βασικά ζητήματα όμως, όπως είναι η παιδική πορνογραφία, η υποκλοπή δεδομένων, το παράνομο εμπόριο κ.λ.π. οι σπουδαστές είναι επαρκώς ενημερωμένοι.

Θα προτείναμε την διοργάνωση σεμιναρίων για τους φοιτητές των σχολών αυτών με θέματα όπως:

«Προστατεύστε τους υπολογιστές σας με χρήση Antivirus και Firewall», «Ενημερωθείτε για τους κινδύνους και τα οφέλη του Ηλεκτρονικού Εμπορίου» και «Τρεις μορφές Ηλεκτρονικού Εγκλήματος: Κυβερνοπόλεμος, Τηλεχειρισμός και Κυβερνοσφετερισμός ».

ΕΠΙΛΟΓΟΣ

Ανακεφαλαιώνοντας, λοιπόν, τα όσα προαναφέραμε κατανοούμε πλήρως τις δυνατότητες που μας προσφέρονται από τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο, καθώς και τις

επιπτώσεις που μπορούμε να έχουμε σε περίπτωση που πραγματοποιηθεί κατάχρηση αυτών. Είναι σαφές ότι η απεριόριστη χρήση των ηλεκτρονικών υπολογιστών και η λειτουργία του διαδικτύου δίνουν απεριόριστες δυνατότητες και συμβάλλουν στην οικονομική ανάπτυξη των κρατών. Ωστόσο, η δυναμική τους εισβολή ευνοεί την ανάπτυξη τεράστιων δυνατοτήτων χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων.

Η χρήση τους με δόλιο σκοπό έχει ως αποτέλεσμα την εμφάνιση του ηλεκτρονικού εγκλήματος, για το οποίο κάναμε εκτενής αναφορά, με ιδιαίτερη έμφαση στην παιδική πορνογραφία. Τα ποσοστά της ηλεκτρονικής εγκληματικότητας συνεχώς αυξάνονται, όπως και οι πιθανότητες εμφάνισης νέων μορφών της στο μέλλον. Επομένως, οι συνθήκες αυτές επιβάλλουν την συντομότερη αντιμετώπιση του θέματος, την πραγματοποίηση συλλογικής προσπάθειας και διασυνοριακής συνεργασίας καθώς και την κατάλληλη τεχνολογική υποδομή σε συνδυασμό με την αντίστοιχη νομοθεσία ούτως ώστε να υπάρχει πραγματική απονομή δικαιοσύνης.

ΚΕΦΑΛΑΙΟ 9:

ΑΝΑΦΟΡΕΣ

9.1 Αναφορές

https://newtech-pub.com › uploads › 2013/10 › kef-asf.plhr_.pdf

// Ιστορική αναδρομή

https://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα#Ορισμός_του_Ηλεκτρονικού_Εγκλήματος

// Ορισμός του ηλεκτρονικού εγκλήματος

https://sites.google.com/site/elektronikoenklema2012/charakteristika-tou-elektronikou

// Χαρακτηριστικά γνωρίσματα ηλεκτρονικού εγκλήματος

http://socialpolicy.gr/2015/09/ηλεκτρονικό-έγκλημα-κυβερνοέγκλημα.html

// Μορφές ηλεκτρονικού εγκλήματος

http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf

// Συνέπειες του ηλεκτρονικού εγκλήματος για τον καταναλωτή

https://sites.google.com/site/crimeics/selida/2-3cracking-kai-hacking

// Ορισμοί Hacking και Cracking

https://sites.google.com/site/elektronikoenklema2012/morphes-tou-elektronikou-enklematos/enklemata-me-ten-chrese-e-y-os-boethetiko-meso

// Απάτη μεσω διαδικτύου

https://sylviecom.com/δίκαιο-και-internet/

// Επικίνδυνη δραστηριότητα στο διαδίκτυο

http://isecurenet.sch.gr/portal/wp-content/uploads/2015/02/Η-ΑΝΑΣΦΑΛΗΣ-ΟΨΗ-ΤΟΥ-ΔΙΑΔΙΚΤΥΟΥ.pdf

https://www.kamouzis.gr/to-egklhma-ths-plastografias/

// Πλαστογραφία

http://1ogelasaferinternet.weebly.com/piepsiloniotarhoalphatauepsilon943alpha-lambdaomicrongammaiotasigmamuiotakappaomicron973.html
// Πειρατεία λογισμικού

http://www.saferinternet.gr/, Τεύχος 11ο: Μάρτιος 2007
// Έρευνες Δικτύου Εθνικών Κόμβων Ασφαλούς Διαδικτύου Insafe

https://www.infokids.gr/paidiki-seksoualiki-kakopoiisi-ellin/
// Το προφίλ των παιδιών θυμάτων

https://www.infokids.gr/paidiki-seksoualiki-kakopoiisi-ellin/
// Grooming

https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html
// Πορνογραφία ανηλίκων και Cyber-bullying

https://sites.google.com/site/elektronikoenklema2012/to-problema-tes-nomikes-prosengises-thematon-pou-aphoroun-ton-kybernochoro
// Το πρόβλημα της Νομικής Προσέγγισης Θεμάτων που αφορούν τον Κυβερνοχώρο

https://sites.google.com/site/elektronikoenklema2012/arches-pou-epopteuoun-ten-prostasia-tou-diadiktyou-sten-ellada
//Αρχές που Εποπτεύουν την Προστασία του Διαδικτύου στην Ελλάδα

https://sites.google.com/site/elektronikoenklema2012/asphaleia-sto-diadikty
//Μέτρα Προστασίας Κατά Την Πρόσβαση Στο Διαδίκτυο