ΠΑΝΕΠΗΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΑ – ΔΙΑΔΥΚΤΙΑΚΑ ΕΓΚΛΗΜΑΤΑ : ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΥΤΩΝ

Συντάκτης: Γιώργος Αλεξάκης **ΑΜ: Ε05205**

Επιβλέπων καθηγητής: Κωνσταντίνος Λαμπρινουδάκης **Επίκουρος καθηγητής Πανεπιστημίου Πειραιώς**

-Ηράκλειο , Μάρτιος 2015-

Περιεχόμενα

Εισαγωγή

Η πληροφορική, οι υπολογιστές, το διαδίκτυο και γενικότερα η σύγχρονη τεχνολογία έχουν εισβάλει στην καθημερινότητα του ανθρώπου, καθώς του παρέχουν μια σειρά δυνατοτήτων που βελτιώνουν την ποιότητα της ζωής του. Η απλοποίηση κάποιων εργασιών, η οργάνωση των πληροφοριών, η επιτάχυνση διαδικασιών όπως και ο ακριβής, άμεσος υπολογισμός και διαχείριση μεγάλου όγκου δεδομένων είναι λίγες μόνο από τις ωφέλειες που μπορεί να καρπωθεί ο σύγχρονος άνθρωπος από τη ραγδαίως αναπτυσσομένη πληροφορική τεχνολογία. Το διαδίκτυο αποτελεί το μεγαλύτερο υπολογιστικό σύστημα στον κόσμο. Η εξέλιξη του βασίστηκε στη φιλοσοφία ενός έκκεντρου, ανοιχτού συστήματος χωρίς ιδιαίτερο έλεγχο από κάποια αρχή και αυτό γιατί το διαδίκτυο δεν είναι ιδιοκτησία κανενός. Παρόλα αυτά όμως, μπορεί να γίνει εύκολα αντιληπτό, πως εξαιτίας του πολλαπλασιασμού των χρηστών, κρίνεται πλέον αναγκαία η οργάνωση καθώς και ο έλεγχος του, ώστε να εξασφαλίζεται η σωστή λειτουργία του. Μπορούμε να το φανταστούμε ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, που διασύνδεει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα διασκορπισμένα ανά τον κόσμο, παρέχοντας στους χρήστες τους μια τεράστια ποικιλία εργαλείων και υπηρεσιών. Από την άλλη, ένα από τα πλέον αρνητικά στοιχεία της πληροφορικής τεχνολογίας, είναι και η δημιουργία πρόσφορων συνθηκών για την ανάπτυξη και διάδοση νέων μορφών εγκλημάτων. Το ηλεκτρονικό έγκλημα είναι ένα φαινόμενο εξελισσόμενο με ταχύτατους ρυθμούς, καθώς συμβαδίζει με αυτούς της ανάπτυξης της τεχνολογίας. Υπάρχει επομένως κίνδυνος κάθε είδους απάτης, από κάλους γνώστες της τεχνολογίας, οι οποίοι προσπαθούν να πραγματοποιήσουν παράνομες πράξεις, μετατρέποντας την τεχνολογία κατά αυτόν τον τρόπο σε ένα καταστροφικό όπλο. Οι δυνατότητες δίωξης από τις αρμόδιες αρχές είναι περιορισμένες, καθώς υπάρχει έλλειψη εμπειρίας αλλά και εκπαίδευσης σε επαρκή βαθμό όπως επίσης και ασάφεια όσον αφορά τη νομοθεσία.

1 . Έγκλημα και Διαδίκτυο

Στο κεφάλαιο που ακλουθεί θα δούμε κάποιους ορισμούς - έννοιες του εγκλήματος και του διαδικτύου ξεχωριστά στην αρχή και στη συνέχεια ως δύο έννοιες που συναποτελούν το λεγόμενο ηλεκτρονικό διαδικτυακό έγκλημα. Έπειτα , παρουσιάζονται τα βασικά είδη του ηλεκτρονικού εγκλήματος, η ιστορική εξέλιξη καθώς και τα κυριότερα χαρακτηριστικά του γνωρίσματα.

1.1 Έγκλημα

Το έγκλημα έχει φύση σύνθετη, γιατί σε αυτήν συναντώνται και την καθορίζουν από την μία μεριά η κοινωνική, βιολογική και ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει στο πλαίσιο ορισμένης κοινωνίας την κοινωνική συμπεριφορά του. Έτσι το είναι έγκλημα τόσο οντολογικό όσο και αξιολογικό φαινόμενο. Δεν είναι ούτε μόνο το ένα ούτε μόνο το άλλο. Η σύνθετη φύση του εγκλήματος μπορεί να αποδοθεί από τον χαρακτηρισμό του ως ορισμένου, αρνητικά αξιολογούμενου, φαινομένου της πραγματικότητας. Το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας και συμπεριφέρεται ως ένας οργανισμός που συνεχώς μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης καθώς και το νομικό πλαίσιο που το καθορίζει. Με διαφορετική μάσκα αλλά και περιεχόμενο πολλές φορές, ανάλογα με τις κοινωνικοπολιτικές και ηθικές τάσεις κάθε εποχής και τόπου το έγκλημα παραμένει παρόν, κινούμενο πάντα σε τρείς βασικούς άξονες, τα απαραίτητα συστατικά στοιχεία του, αυτά που το ορίζουν. Ποια είναι όμως αυτά τα στοιχεία; Δογματικό ορισμό του εγκλήματος μας δίνει ο ίδιος ο Ποινικός Κώδικας μας στην διάταξη του άρθρου 14. Έτσι σύμφωνα με το άρθρο 14 Π.Κ. «πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο». Το ουσιαστικότερο περιεχόμενο του εγκλήματος συνίσταται στο ότι :είναι η πράξη εκείνη που θίγει τις αξίες της κοινωνική ζωής στις γενικότερης αποδοχής πλευρές της, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά απόλυτα αναγκαία. Το εγκληματικό φαινόμενο αποτελεί ιστορικό, κοινωνικό φαινόμενο καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Αυτό που έχει ιδιαίτερη σημασία να επισημάνουμε είναι η διαχρονικότητα του στο πέρασμα των αιώνων. Αν και σε κάθε έγκλημα (προσβολή), υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση), καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό. Αντίθετα αυτό που παρατηρείται είναι μια αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς. Σε κάθε κοινωνία υπάρχουν κανόνες οι οποίοι θεσπίστηκαν τυπικά ή άτυπα (έθιμα) προκειμένου να προστατευτούν κοινωνικά αγαθά και άνθρωποι οι οποίοι παραβαίνουν τους κανόνες αυτούς. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων (ποινών) στους παραβάτες, οι οποίες αποτελούν τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση,

καθώς και το είδος της ποινής, βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό. Τα βασικά στοιχεία του εγκληματικού φαινομένου, κανόνας, έγκλημα, κύρωση (ποινή), συναποτελούν έναν αδιάσπαστο κύκλο. Εδώ είναι ξεκάθαρη η αλληλεξάρτηση των στοιχείων. Αν δεν υπήρχε έγκλημα δεν θα υφίστατο η κύρωση. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή την παράβασή του. Ο κανόνας δημιουργήθηκε για να οργανώσει και να προστατέψει τα κοινωνικά αγαθά (υλικά και άυλα) από κάθε προσβολή τους μέσα στα πλαίσια της κοινωνικής συμβίωσης. Στη συνέχεια, και αφού επέλθει η προσβολή του έννομου αγαθού (αυτό που προστατεύεται από τον κανόνα-νόμο), έρχεται η κύρωση (ποινή). Είναι με λίγα λόγια η κύρωση (ποινή) συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Θα λέγαμε ότι η ποινή αποτελεί την εκτόνωση της κοινωνικής αντίδρασης στο έγκλημα. Μπορεί δε, να παρουσιαστεί με πολλούς διαφορετικούς τρόπους, όσο αφορά τη ιδεολογική της προσέγγιση, όπως ως αποκατάσταση της διαταραχθείσας από το έγκλημα κοινωνικής τάξης ή ως το μέσο για την ηθική βελτίωση του παραβάτη.

1.2 Διαδίκτυο

Το διαδίκτυο αποτελεί μία από τις βάσεις της σημερινής κοινωνίας. Έχει αλλάξει τον τρόπο με τον οποίο ο κόσμος επικοινωνεί, δουλεύει, μαθαίνει και το σπουδαιότερο ζει. Το διαδίκτυο (ιντερνέτ) μπορεί να περιγραφεί ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, το οποίο διασύνδεει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένε σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων. Αποτελεί την κύρια μηχανή με την οποία άτομα επικοινωνούν μεταξύ τους ταχύτερα πλέον από ποτέ. Στα σπουδαιότερα πλεονεκτήματα του έχουν περιληφθεί, η ταχύτητα και η άνεση. Τα πάντα μπορούν να πραγματοποιηθούν με το πάτημα ενός κουμπιού του πληκτρολογίου ή με ένα κλικ του ποντικιού. Στο διαδίκτυο ο τόπος χάνει την σημασία του. Η σωστή χρήση του διαδικτύου μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών του προσφέροντας τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης Το διαδίκτυο και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές (Η/Υ), έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητας μας, είτε ως μέσα ψυχαγωγίας- ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων. Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Στις μέρες μας, γίνεται σε μεγάλο βαθμό και η χρήση εφαρμογών κοινωνικής δικτύωσης (facebook, twitter, chat rooms).

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

δεδομένων εντός του συστήματος, δίνοντας έτσι την εντύπωση ενός ενιαίου πλέγματος. Ειδικότερα, όλοι οι συνδεδεμένοι με το διαδίκτυο ηλεκτρονικοί υπολογιστές συνεργάζονται για να μεταφέρουν πληροφορίες προς διάφορες κατευθύνσεις σε όλο τον κόσμο. Με την αποστολή μιας τέτοιας ηλεκτρονικής πληροφορίας αυτή χωρίζεται από το TCP (Transmission Control Protocol) και το IP (Internet Protocol) σε μικρότερα κομμάτια που ονομάζονται πακέτα (packets) και το καθένα αποκτά τη δική του ταυτότητα το κάθε μικρότερο κομμάτι της πληροφορίας (πακέτο) ακολουθεί διαφορετικό δρόμο, για να φτάσει στον προορισμό του. Όταν η ηλεκτρονική πληροφορία φτάσει στον προορισμό της, τότε όλα τα διασπασμένα κομμάτια (πακέτα) της πληροφορίας ενώνονται ξανά και υπεύθυνο για την ασφαλή και ορθή επανένωση αυτή είναι το TCP (Transmission Control Protocol) και το IP (Internet Protocol). Την κυκλοφορία μέσω του διαδικτύου διευθύνει ένας ειδικός υπολογιστής που ονομάζεται Router. Ένα πακέτο μπορεί να περάσει από πολλούς Routers ως τον προορισμό του. Για να αποκτήσει κάποιος πρόσβαση στο διαδίκτυο, ώστε να γίνει δέκτης του πλήθους των υπηρεσιών που προσφέρει, πρέπει να επιλέξει έναν από του εξής τρόπους σύνδεσης με το διαδίκτυο:

1. Διαρκής σύνδεση
2. Προσωρινή άμεση σύνδεση
3. Προσωρινή έμμεση σύνδεση

1.3 Ηλεκτρονικό-διαδικτυακό έγκλημα

Το ιντερνέτ και οι Η/Υ παρέχουν στους χρήστες αφενός μεν ασύλληπτες δυνατότητες και αφετέρου όμως εισαγάγουν νέες μορφές παραβατικής συμπεριφοράς. Επιπρόσθετα «γεννώνται» αξιόποινες πράξεις που υφίστανται μόνο με τη χρήση Η/Υ και του ιντερνέτ, όπως η διασπορά κακόβουλου λογισμικού σε Η/Υ και η παραβίαση ηλεκτρονικών αρχείων. Έτσι, παραδοσιακές εγκληματικές πράξεις όπως εξύβριση ή δυσφήμιση, μέσω μίας ιστοσελίδας (web site) ή ηλεκτρονικού ταχυδρομείου, διαπράττονται πλέον ταχύτερα, με το διαδίκτυο να αποτελεί το κύριο μέσο τέλεσης τους. Το καθεστώς της ανωνυμίας των δραστών, η δυσκολία των διωκτικών αρχών στην διαλεύκανση της ηλεκτρονικής εγκληματικότητας με αποτέλεσμα την ελαχιστοποίηση της τιμωρίας του δράστη είναι εκείνα τα στοιχεία που τους ωθούν στην τέλεση αξιόποινων πράξεων μέσω Διαδικτύου Στις μέρες μας, παρά την εξέλιξη και ανάπτυξη των διωκτικών μηχανισμών, η διαλεύκανση της ηλεκτρονικής εγκληματικότητας παραμένει μία δύσκολη υπόθεση. Είναι όμως το ηλεκτρονικό έγκλημα διαδικτυακό; Είναι πλέον αναγκαίο να γίνεται διάκριση μεταξύ του λεγόμενου ηλεκτρονικού εγκλήματος και του διαδικτυακού (cybercrime) το οποίο παρουσιάζει ποιοτικά σημαντικές διαφοροποιήσεις από το πρώτο λόγω των ιδιαίτερων χαρακτηριστικών του διαδικτύου, που συνοψίζονται στη δυνατότητα ανταλλαγής δεδομένων και προγραμμάτων μεταξύ όλων των συνδεδεμένων υπολογιστών. Επίσης πρέπει να σημειωθεί η δυσκολία στη διατύπωση ενός ενιαίου ορισμού που να περιλαμβάνει όλες τις εκφάνσεις του διαδικτυακού εγκλήματος, κάτι που παρατηρείται και αναφορικά με τον εννοιολογικό προσδιορισμό εν γένει της ηλεκτρονικής εγκληματικότητας. Τούτο συμβαίνει διότι οι παραβάσεις στο διαδικτύου παρουσιάζουν ποικιλομορφία ως προς τις μορφές εκδήλωσης τους και

κατατείνουν στην προσβολή διαφόρων κάθε φορά έννομων αγαθών. Συμφωνά με ορισμό που δόθηκε από τους Forester and Morrison (1994), είναι «Μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Ένας άλλος ορισμός, από τους πλέον διαδεδομένους, είναι αυτός που δόθηκε από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, αρκετά χρόνια πριν (1986). Έτσι λοιπόν, «Ηλεκτρονικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων». Απαραίτητο στοιχείο για την τέλεση ηλεκτρονικού εγκλήματος, θεωρείται η ύπαρξη συσκευής ηλεκτρονικής επεξεργασίας δεδομένων όπως είναι ο ηλεκτρονικός υπολογιστής, το κινητό τηλέφωνο κλπ. Σύμφωνα με τον Shinder (2002), ο ρόλος που διαδραματίζει ο Η/Υ στα πλαίσια του ηλεκτρονικού εγκλήματος είναι κυρίαρχος καθώς:

- Μπορεί να αποτελεί το στόχο κάποιας επίθεσης, στη συγκεκριμένη περίπτωση ο Η/Υ είναι το «θύμα» της επίθεσης.
- Δύναται να αποτελεί μέσο για τη διάπραξη κάποιας επίθεσης. Εδώ είναι το εργαλείο που χρησιμοποιείται από το δράστη για την πραγματοποίηση εγκληματικού σκοπού.
- Τέλος, υπάρχει και η περίπτωση που ο Η/Υ αποτελεί βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Μέχρι στιγμής έχουμε προσδιορίσει τον όρο «ηλεκτρονικό έγκλημα», ο οποίος διαφοροποιείται από τον όρο του διαδικτυακού εγκλήματος . Η παραπάνω παρατήρηση δεν παραβλέπει σε καμία περίπτωση τη σχέση που τις συνδέει, η οποία είναι σχέση γένους προς είδος. Το ηλεκτρονικό έγκλημα είναι έννοια γένους που περιλαμβάνει εννοιολογικά και το διαδικτυακό έγκλημα χωρίς όμως να ταυτίζεται με αυτό. Το διαδικτυακό έγκλημα είναι δηλαδή μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος Κατά τον ορισμό του Donn Parker «το διαδικτυακό έγκλημα λοιπόν ή αλλιώς κυβερνοέγκλημα (cyber-crime), είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, αυτό για την τέλεση του οποίου ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο. Σχετίζεται με την οποιανδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο». Αν λοιπόν θέλουμε να κατηγοριοποιήσουμε τις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων, σύμφωνα με τον Αργυρόπουλο (2001), θα διακρίνουμε τα παρακάτω ηλεκτρονικά εγκλήματα:

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.
- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για

την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσουμε τη διασπορά κακόβουλου λογισμικού.

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

1. Σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ , η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών
2. Σε εκείνα που υποστηρίζονται από Η/Υ και οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά.

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

1. Στην πρώτη κατηγορία ανήκουν τα παραδοσιακά εγκλήματα τα οποία τελούνται με χρήση Η/Υ και ως τέτοια αναφέρει την απάτη, την κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και την κλοπή της ηλεκτρονικής ταυτότητας.
2. Στην δεύτερη κατηγορία υπάγονται τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια ο συγγραφέας θεωρεί την επίθεση της άρνησης παροχής υπηρεσιών , την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.
3. Στην τρίτη κατηγορία τοποθετεί τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί
4. Στην τέταρτη κατηγορία ανήκουν τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

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

1. απάτη: Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή /συμπίεση/ ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς)
2. κλοπή: των δεδομένων, του λογισμικού
3. χρήση λογισμικού χωρίς άδεια: χρήση παράνομων αντιγράφων λογισμικού
4. ιδιωτική εργασία: μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποδοκιμή κέρδους ή για ίδιον όφελος
5. χάκινγκ: :ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας

6. σαμποτάζ: η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό
7. εισαγωγή: πορνογραφικού υλικού
8. ιοι: διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής.

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα:

Το πρώτο καταγεγραμμένο Ηλεκτρονικό έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μίας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία. Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών , οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται.

1.4 Κύρια χαρακτηριστικά γνωρίσματα διαδικτυακών εγκλημάτων

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

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

2. Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα. Βλάβες, φθορές καθώς και αλλοιώσεις που προκαλούνται σε ενσωματωμένα

αντικείμενα όπως σκληρούς δίσκους, μνήμες κλπ, είναι απλά δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά τα δεδομένα.

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

4. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (του κράτους στο οποίο γίνεται αντιληπτή η διάπραξη του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Αυτός ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος οδηγεί σε πολλές περιπτώσεις σε διαφορετική αξιολόγηση του περιεχομένου, αφού μπορεί να είναι νόμιμο στο κράτος που βρίσκεται ο δράστης ή που υπάρχουν αποθηκευμένα τα δεδομένα και να είναι παράνομο στο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους.

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

6. Το ηλεκτρονικό έγκλημα έχει εισάγει νέους περιορισμούς:

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

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

2. Κατηγορίες ηλεκτρονικών – διαδικτυακών εγκλημάτων

Σε αυτό το κεφάλαιο θα καταγράψουμε και θα αναλύσουμε διάφορα είδη ηλεκτρονικών - διαδικτυακών εγκλημάτων είτε αυτά εμφανίστηκαν παράλληλα με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο είτε προϋπήρχαν αλλά η εμφάνιση των ηλεκτρονικών υπολογιστών και του διαδικτύου ευνόησαν σε μεγάλο βαθμό την ανάπτυξη τους.

2.1 Hacking – Cracking

Hacker είναι ένας τεχνικά καταρτισμένος χρήστης υπολογιστή ο οποίος, είτε με αρνητικά είτε με θετικά κίνητρα, θα παραβιάσει ("σπάζοντας" την ασφάλεια, για αυτό κολλάει εδώ και ο όρος cracker) συστήματα υπολογιστών. Συνήθως είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής και έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Μερικές φορές η εισβολή σε κάποιον "στόχο" γίνεται για καλό σκοπό δηλαδή είναι ευγενής και ευεργετική άλλες πάλι φορές μπορεί να είναι κακόβουλη , για κλοπές και βανδαλισμό. θα δείτε μερικές φορές τον όρο "hacker" να γράφεται στην διαδικτυακή αργκό με διάφορους τρόπους, όπως "haxor", "Hax0r", ή "h4x0r".Ιστορικά, ένας hacker τη δεκαετίας του 1980 ήταν απολύτως κακός και ανέντιμος: ένας εγκληματίας που αναλάμβανε παράνομα και ανήθικα τον έλεγχο των ηλεκτρονικών υπολογιστών και δικτύων. Έτσι, ο ορισμός hackers εξακολουθεί να παραπέμπει σε κάτι παράνομο μέχρι και σήμερα στον 21ο αιώνα. Ωστόσο, ο όρος hacker έχει διευρυνθεί και συμπεριλάβει μη ποινικούς και ακόμα και ευγενείς χρήστες υπολογιστών. Σήμερα, ο όρος hacker διακρίνεται σε 3 κατηγορίες χρηστών υπολογιστών: "Black Hat", "White Hat", "Grey Hat.

1) Κλασικοί "Black Hat" Hackers = εγκληματίες – παραβάτες

Αυτός είναι ο κλασικός ορισμός ενός hacker: ένας χρήστης υπολογιστή που επιδιώκει εσκεμμένα να καταστρέψει ή να διαπράξει κλοπές σε δίκτυα άλλων ανθρώπων. Αυτό το κλασικό είδος hacker είναι γνωστό και ως "Black Hat hacker", λόγω των κακόβουλων κινήτρων του. Οι Black Hat είναι προικισμένοι τεχνικά χρήστες, αλλά κακόβουλοι και τα κίνητρα τους υποκινούνται από συναισθήματα δύναμης και μικροαστικής εκδίκησης. Πρόκειται για ηλεκτρονικούς κακοποιούς, με κάθε έννοια της λέξης, και έχουν τα ίδια χαρακτηριστικά προσωπικότητας, σαν τους έφηβους που σπάνε τα παράθυρα ενός λεωφορείου για προσωπική ικανοποίηση. Οι Black Hat hackers είναι γνωστοί για τα ακόλουθα κοινά εγκλήματα στον κυβερνοχώρο:

- Επιθέσεις DOS/DDOS που επιβαρύνουν τους διακομιστές στο Διαδίκτυο.
- Παραμόρφωση ιστοσελίδων με ανάληψη ελέγχου και η αντικατάσταση των κύριων φωτογραφιών της σελίδας με αγενή συνθήματα.

- Κλοπή ταυτότητας και κλοπή προσωπικών πληροφοριών.
- Botnetting: Τηλεχειρισμός δεκάδων προσωπικών υπολογιστών, και προγραμματισμός των “ζόμπι” για εκτέλεση spam

2) White Hat “Ethical Hackers” Ειδικοί Ασφαλείας Network Security

Μια διαφορετική κατηγορία hackers. Οι White Hat hackers έχουν έντιμα, ή τουλάχιστον καλοήθη κίνητρα. Ένας White Hat Ethical Hacker είναι ένας ταλαντούχος χρήστης στην ασφάλεια του υπολογιστή που χρησιμοποιείται για να βοηθήσει στην προστασία δικτύων υπολογιστών. Οι White HatEthical Hackers μπορεί να είναι και πρώην black hat που αναλαμβάνουν εργασία σαν φρουροί ασφαλείας μιας εταιρείας. Οι Ethical Hackers συνήθως υποκινούνται από ένα σταθερό μισθό, αλλά υπάρχουν και αυτοί που το κάνουν μόνο από χόμπι χωρίς καθόλου μισθό. Δεν είναι έκπληξη να δούμε ethical hackers να ξοδεύουν το μισθό τους για πολύ ακριβούς υπολογιστές στην προσωπική τους ζωή, ώστε να μπορούν να παίξουν online παιχνίδια μετά τη δουλειά. Αναφέραμε παραπάνω ότι οι White Hat μπορεί να ασχολούνται μόνο από χόμπι. Κάτι παραπλήσιο είναι και οι “Ακαδημαϊκοί Hackers” = οι Creative Artists Υπολογιστών

Ένα άλλο είδος White Hat είναι ο “academic hacker“: ένας τεχνικός υπολογιστών ο οποίος δεν ενδιαφέρεται για την προστασία συστημάτων, αλλά μάλλον στη δημιουργία έξυπνων προγραμμάτων. Αν είστε ένας ακαδημαϊκός hacker, για παράδειγμα, θα πάρετε έναν κώδικα, για να τον βελτιώσετε με έξυπνες μετατροπές και προσθήκες. Το “Ακαδημαϊκό hacking» είναι ακίνδυνο και δεν επιδιώκει να βλάψει δίκτυα άλλων ανθρώπων. Οι ακαδημαϊκοί White Hat hackers είναι συχνά μεταπτυχιακοί φοιτητές στον προγραμματισμό ηλεκτρονικών υπολογιστών.

3) Grey Hat Hackers = Δεν είναι σίγουρο από ποια πλευρά του νόμου στέκεται.

Οι Grey Hat Hackers είναι συχνά χομπίστες: είναι χρήστες με βασικές και ενδιάμεσες δεξιότητες τεχνολογίας που τους αρέσει να αποσυναρμολογούν και να τροποποιούν δικά τους συστήματα από χόμπι. Συχνά ανακατεύονται με μικρά εγκλήματα, όπως τη κοινή χρήση αρχείων ταινιών ή χρήση παράνομου (σπασμένου) λογισμικού. Τα εκατομμύρια p2p downloaders θεωρούνται χόμπι hackers. Έχετε τροποποιήσει ποτέ router και firewall για να σας επιτρέψει ταχύτερα p2p downloads; Θα μπορούσατε να περιγράψετε τον εαυτό σας σαν ένα “Grey Hat” χόμπι Hacker. Μόνο ένα μικρό ποσοστό από αυτούς τους hackers θα γίνουν Black Hat κάποια στιγμή.

2.2 Επιθέσεις άρνησης εξυπηρέτησης (DoS, Denial of Service)

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστή ιστοσελίδας (web server) ή ενός διακομιστή αρχείων(file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιότητα δεδομένων και τη γενικότερη λειτουργία του συστήματος. Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

- Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο.
- Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.
- Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

2.3 Κακόβουλο λογισμικό (Malware)

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα «ξενιστή» και σε αυτό που δεν χρειάζεται «ξενιστή» και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε δύο άλλες κατηγορίες. Το ιομορφικό λογισμικό και το μη ιομορφικό λογισμικό. Στο ιομορφικό λογισμικό ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο μη ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) καθώς και οι δούρειοι ίπποι (Trojan horses).

α) Ιοί (Viruses)

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

Ξεκίνησαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. ή εταιριών προϊόντων υψηλής τεχνολογίας όπως XEROX, BELL κλπ. Σύμφωνα με τον Kyas (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό :

1. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).
2. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).
3. Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).
4. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων Anti-Virus (Polymorphous Viruses).
5. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).
6. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).
7. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

β) Δούρειοι ίπποι (Trojan Horses)

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

δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall). Είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. 'Ετσι ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού , αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου. Στις περισσότερες των περιπτώσεων, ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης

γ) Σκουλήκι (Worm)

Σκουλήκι είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά του να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντάς το με άχρηστη δραστηριότητα.

δ) Άλλα είδη κακόβουλου λογισμικού

- Dialers .
- Λογική βόμβα.
- Rootkits.
- Ransomware.
- Bots – zombies.
- Scareware.
- Βακτήρια (bacteria).

2.4 Ανεπιθύμητη αλληλογραφία (Spamming)

Ως Ανεπιθύμητη Αλληλογραφία (spam) ορίζουμε την συνήθως ανώνυμη αποστολή ενός η περισσοτέρων μηνυμάτων ηλεκτρονικού ταχυδρομείου προς πολλαπλούς αποδέκτες. Ο βασικός λόγος ύπαρξης του spam είναι συνήθως η αποκομιδή κέρδους. Όταν το spam είναι ανώνυμο η πραγματική ταυτότητα του αποστολέα δεν είναι έγκυρη ή είναι πλαστογραφημένη ή μεταμφιεσμένη σε κάποια άλλη πραγματική διεύθυνση. Ο σκοπός του ανώνυμου spam είναι να αποκρύψει τον πραγματικό αποστολέα. Μαζική αποστολή μηνυμάτων σημαίνει συνήθως η αποστολή δεκάδων χιλιάδων έως και εκατομμυρίων μηνυμάτων. Ο βασικός λόγος για τον τεράστιο όγκο μηνυμάτων είναι το οικονομικό όφελος που έχουν οι αποστολείς των μηνυμάτων spam (γνωστοί ως spammers) και προέρχεται από ένα πολύ μικρό ποσοστό ανταπόκρισης από τους παραλήπτες των μηνυμάτων τους. Ανεπιθύμητη αλληλογραφία μπορεί να θεωρηθεί όμως από κάποιον και νόμιμη αλληλογραφία όπως για παράδειγμα διαφημιστικό υλικό το οποίο κάποιοι τελικοί αποδέκτες έχουν επιλέξει να λαμβάνουν από κάποιο αποστολέα. Ένα τέτοιο μήνυμα μπορεί να μοιάζει με spam, αλλά στην πραγματικότητα μπορεί να είναι νόμιμη αλληλογραφία. Με άλλα λόγια, το ίδιο μήνυμα μπορεί να χαρακτηριστεί ως spam η ως νόμιμη αλληλογραφία ανάλογα με το αν ή όχι ο χρήστης επιλέξει να το παραλάβει. Επομένως ο όρος διαφήμιση δεν πρέπει να χρησιμοποιείται ως το αποκλειστικό κριτήριο ορισμού του spam. Πολλά μηνύματα spam δεν είναι ούτε διαφήμιση, ούτε κάποιου είδους εμπορική πρόταση. Εκτός από την προσφορά αγαθών και υπηρεσιών, το spam μπορεί να περιλαμβάνει μεταξύ άλλων και τις ακόλουθες κατηγορίες:

- Μηνύματα πολιτικού περιεχομένου
- Οικονομικές απάτες
- Μηνύματα που προτρέπουν την προώθηση τους σε τρίτους (αλυσίδα)
- Μηνύματα που χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού (malware)

2.5 Ηλεκτρονικό ψάρεμα (phishing - pharming)

Το Phishing είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί . Αν ήταν εφικτό να αποδώσουμε τον όρο στα Ελληνικά, θα μπορούσαμε κάλλιστα να το αποκαλέσουμε 'Ηλεκτρονικό Ψάρεμα', κι αυτό γιατί αγγλικός όρος δεν απέχει πολύ από αυτό. Ο όρος Phishing, που πρωτοχρησιμοποιήθηκε από τον χάκερ Khan C Smith και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα των χάκερς, προέρχεται από το αγγλικό 'fishing' (ψάρεμα , καθώς η διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες, θυμίζει την διαδικασία του δολώματος στο ψάρεμα. Στην περίπτωση αυτή ο απατεώνας προσπαθεί

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

Pharming είναι η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν. Κατόπιν τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα.

2.5 Διαδικτυακή τρομοκρατία

Ο όρος , Διαδικτυακή τρομοκρατία, αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μιας τρομοκρατικής επίθεσης. Πιο συγκεκριμένα το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες». Η χρήση του διαδικτύου παρέχει στους τρομοκράτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.

2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του.

Με τη χρήση λοιπόν του διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων. Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή του καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία.

2.6 Διαδικτυακός εκφοβισμός (Cyberbullying)

Ο εκφοβισμός μέσω του Διαδικτύου είναι οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που θεσπίζεται και πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών επικοινωνίας, συγκεκριμένα του διαδικτύου και των κινητών τηλεφώνων και η οποία επαναλαμβάνεται ανά τακτά ή άτακτα χρονικά διαστήματα. Ο όρος cyber bulling δημιουργήθηκε από τον Καναδό Bill Belsey και έχει τις ρίζες του στον παραδοσιακό σωματικό ή ψυχολογικό εκφοβισμό όπου ο στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του. Μερικές από τις πιο κοινές μεθόδους διαδικτυακού εκφοβισμού είναι οι εξής

- Πειράγματα με στόχο τη διασκέδαση
- Διάδοση άσχημων-προσβλητικών φημών on-line
- Επαναλαμβανόμενη αποστολή ανεπιθύμητων μηνυμάτων (υβριστικά-προσβλητικά)
- Δυσφήμηση σε τρίτους (άλλους πλην του θύματος) μέσω του ηλεκτρονικού ταχυδρομείου, μηνυμάτων μέσω κινητού, φωτογραφίες και βίντεο στο διαδίκτυο, ιστοσελίδες, μπλογκς, chat rooms κ.ά.
- Παρέμβαση και παρενόχληση οποιασδήποτε διαδικτυακής δραστηριότητας του ατόμου
- Δημιουργία ψεύτικων διαδικτυακών προφίλ
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή αλλού είδους μαγνητοσκοπημένου υλικού

- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- Αποστολή απειλητικών μηνυμάτων σε αλλά άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

Σύμφωνα με τα στοιχεία της Γραμμής Βοήθειας 800 11 800 15 "ΥποΣΤΗΡΙΖΩ" του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, από τον Ιανουάριο 2011 έως και Ιούνιο 2012 πραγματοποιήθηκαν συνολικά 2440 αιτήματα. Τα 82% προήλθαν μέσα από τηλεφωνική επικοινωνία στον αριθμό χωρίς χρέωση 800 11 80015 ενώ ένα ποσοστό της τάξης του 18% επέλεξε να επικοινωνήσει ηλεκτρονικά μέσω email στη διεύθυνση help@saferinternet.gr. Όσον αφορά στα δημογραφικά στοιχεία, η πλειοψηφία των αιτημάτων (78%) προήλθε από ενήλικες (κυρίως γονείς), ενώ οι επαγγελματίες και οι ανήλικοι που απευθύνθηκαν στη γραμμή ακολουθούν με ποσοστό 10% και 12%, αντίστοιχα. Αναφορικά με τον τύπο του αιτήματος, η πλειοψηφία των αιτημάτων αφορούσε σε θέματα εξάρτησης (36%), ενώ στη δεύτερη θέση βρίσκονται τα αιτήματα αφορούσαν σε γενικές πληροφορίες για την ασφάλεια στο διαδίκτυο (30%).Στην τρίτη θέση, με ποσοστό 11%, αναδείχθηκε μια νέα κατηγορία που αφορά στα προβλήματα με τις σελίδες κοινωνικής δικτύωσης και ιδιαίτερα μέσω της διάσημης ιστοσελίδας "Facebook" (π.χ. ψευδή προφίλ). Σημειώνεται ότι πραγματοποιήθηκαν μόλις 9 αιτήματα για εκβιασμό και 8 για πρόθεση για αυτοκτονία. 407 περιπτώσεις παραπέμφθηκαν στη γραμμή καταγγελιών Safeline.gr και στη Δίωξη Ηλεκτρονικού Εγκλήματος για περιπτώσεις ηλεκτρονικού εγκλήματος, ή σε άλλους αρμόδιους φορείς αντίστοιχα με τη φύση της αναφοράς (π.χ. καταναλωτικές οργανώσεις κλπ). Σύμφωνα επίσης, με τα στοιχεία που λάβαμε επίσης από τη δίωξη ηλεκτρονικού εγκλήματος, τα εμπλεκόμενα μέρη είναι συνήθως ανήλικοι. Έφηβοι ηλικίας 12-16 ετών φαίνεται να αποτελούν την πιο ευαίσθητη κοινωνική ομάδα που επηρεάζεται από το φαινόμενο. Χαρακτηριστικά αναφέρεται ότι ένα στα πέντε παιδιά έχει πέσει θύμα διαδικτυακού εκφοβισμού.

2.7 Παιδική πορνογραφία

Σύμφωνα με το «Προαιρετικό Πρωτόκολλο της Σύμβασης για τα δικαιώματα του Παιδιού για την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία» και συγκεκριμένα στο άρθρο 2, «παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες, ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς». Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Οι εγκληματίες διακίνησης πορνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου

εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα εκμεταλλευόμενοι την παιδική αθωότητα . Με τη χρήση του διαδικτύου:

- Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του.
- Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος.
- Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων.
- διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη «επιχειρηματική» δραστηριότητα. Αποτελεί προϊόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά. Οι επιπτώσεις εις βάρος των ανηλίκων, μπορούν να ειδωθούν από πολλές οπτικές γωνίες. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων, αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε «μέσα» ικανοποίησης των σεξουαλικών τους ορέξεων. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους, που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική τους ωρίμανση. Ο ανήλικος από την πλευρά του, είναι ικανότατος χρήστης των υπολογιστών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου του χαρακτήρα του, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε δια μέσου του ιστού.

2.8 Οικονομικό έγκλημα

Με τη διενέργεια ενός οικονομικού εγκλήματος, επιδιώκεται μεγάλο και αδικαιολόγητο οικονομικό ή άλλο όφελος μέσω διάπραξης παρανομιών. Στο πλαίσιο των διαδικτυακών οικονομικών εγκλημάτων, η απάτη μέσω υπολογιστή περιλαμβάνει την παραποίηση κάποιων δεδομένων ή πληροφοριών που φιλοξενούνται στις βάσεις δεδομένων ή σε προγράμματα με σκοπό το οικονομικό κέρδος. Λεπτομερέστερα, αφορά κυρίως στην κλοπή, διαγράφη, αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος. Κεντρικό αντικείμενο- στόχος της συγκεκριμένης μορφής απάτης είναι τα δεδομένα που φιλοξενούνται στον υπολογιστή και αφορούν σε οικονομικά μεγέθη. Η συγκεκριμένη απάτη μετεξελίχθητε

στο πέρασμα του χρόνου από ένα ομοιογενές σύνολο αδικημάτων, της εποχής των κεντρικών πληροφορικών συστημάτων, σε μία διαφοροποιημένη ενότητα που περιγράφει ένα μεγάλο φάσμα διαφορετικών υποθέσεων στο πεδίο του οικονομικού εγκλήματος. Μερικές μορφές οικονομικών εγκλημάτων είναι τα εξής παρακάτω :

- **Παραποίηση λογιστικών λογαριασμών**

Η απάτη σε βάρος μιας επιχείρησης ή ενός ιδιώτη μέσω της παραποίησης, σε πληροφορίες και δεδομένα, τα οποία τους αφορούν άμεσα και έμμεσα, έχει να κάνει με τους άυλους πόρους, όπως χρηματικές καταθέσεις, οικονομικούς τίτλους, για παράδειγμα, ομόλογα, και λογιστικά μεγέθη, όπως ισολογισμούς. Συχνά, υπάρχουν περιπτώσεις βελτίωσης της πίστης (credit rating) μέσω της παραποίησης των δεδομένων που αναφέρονται σε ένα άτομο ή μία επιχείρηση, ώστε για παράδειγμα, να μπορεί να πάρει δάνειο ή να πάρει δάνειο με καλύτερους όρους, αλλά και χειροτέρευσης της φερεγγυότητας ενός ατόμου ή μιας επιχείρησης, για τους αντίθετους λόγους, που μπορεί να πραγματοποιηθούν από κάποιο άτομο ή επιχείρηση εχθρικά διακείμενων ή αντίθετων συμφερόντων.

- **Παραποιημένη εφαρμογή ηλεκτρονικών πληρωμών**

Η απάτη μέσω υπολογιστή με την παρέμβαση στο σύστημα επεξεργασίας δεδομένων ενός οργανισμού ή μιας επιχείρησης απαντάται συχνά σε ζητήματα μισθών, συντάξεων αλλά και των τραπεζικών καταθέσεων. Σε ένα «ανοχύρωτο» σύστημα, η δημιουργία ενός τραπεζικού λογαριασμού πολλών μηδενικών είναι ζήτημα λεπτών - και για έναν έμπειρο hacker, είναι ζήτημα δευτερολέπτων. Αν το πληροφορικό σύστημα διαθέτει έναν αμυντικό μηχανισμό προηγούμενης γενιάς και αν ο συγκεκριμένος hacker δε βιάζεται, αλλά αρκείται σε έναν αρχικό λογαριασμό ενός ή δύο μηδενικών, και κατόπιν εισάγει μία ρουτίνα προσθήκης πέντε μηδενικών σε κάποια συχνά μεν, αλλά άτακτα χρονικά διαστήματα, δεν έχει λόγους να φοβάται τις συνέπειες. Πέρα όμως, από τις περιπτώσεις παράνομης κατασκευής δεδομένων, συχνά εμφανίζονται στη διεθνή βιβλιογραφία και ειδησεογραφία, πολλές περιπτώσεις παραβίασης καρτών συναλλαγής (ATM cards) και ανάλογων μέσων πληρωμής. Ακόμη και αν τέτοιου είδους απάτες οδηγούν σε μικρές συνολικά ζημιές, οι στατιστικές δείχνουν πως η κακή χρήση των καρτών αποτελεί μία από τις πιο συχνές υποθέσεις πληροφορικού εγκλήματος. Μια παραποιημένη πληρωμή διαπράττεται μέσω τράπεζας, που διαθέτει σύστημα αυτόματης ανάληψης ή χορήγησης χρήματος. Με διάφορες μεθόδους, είναι δυνατή η παράνομη ανάληψη χρήματος από τερματικά των συστημάτων επεξεργασίας δεδομένων των τραπεζών

- **Ξέπλυμα χρήματος**

Ξέπλυμα χρήματος νοείται η κάθε είδους ανάμιξη σε ενέργειες ή σειρά ενεργειών που επιδιώκουν να συγκαλύψουν τη μορφή ή την προέλευση εσόδων που προέρχονται από εγκληματικές δραστηριότητες . Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακλουθεί τα παρακάτω τρία βασικά στάδια :

1. Τοποθέτηση : Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο γενικότερο οικονομικό σύστημα, σε παραδοσιακό ή μη χρηματοοικονομικό οργανισμό, όπως τράπεζα με κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις.
2. Στρωματοποίηση: Ο δράστης επιχειρεί σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι να μεταμφιέσει τις αληθινές πήγες κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεγκτικά όργανα του φορέα στον όποιο επενδύθηκαν τελικά.
3. Ενσωμάτωση : Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας όπως για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ, έτσι ώστε τα εν λόγω κεφάλαια να επιστραφούν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια.

Η επανάσταση στην πληροφορική τεχνολογία έπαιξε καθοριστικό ρόλο στην απόκρυψη αλλά και στη διακίνηση των οικονομικών προϊόντων εγκληματικών ενεργειών. Έτσι λοιπόν, βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεσαι με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή προσφέρει, με σύγχρονους τρόπους και μεθόδους πάντα όμως με τον ίδιο επιδιωκόμενο σκοπό. Το βασικό πλεονέκτημα του ξεπλύματος χρήματος μέσω ιντερνέτ είναι ότι δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων μέρων με άμεσο επακόλουθο, οι δράστες να νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους να νομιμοποιούν έσοδα παρανόμων δραστηριοτήτων. Όπως στην μεγάλη πλειοψηφία των εγκληματών του διαδικτύου, έτσι και το ξέπλυμα χρήματος είναι εξαιρετικά δύσκολο να ανιχνευτεί, καθώς δεν υπάρχουν ακόμα οι κατάλληλοι μηχανισμοί εντοπισμού και ελέγχου.

- **Νιγηριανή απάτη**

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητεί τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα

βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επομένη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάτε λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχειά της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν

3. Μέθοδοι αντιμετώπισης

Σε αυτό το κεφάλαιο αναφέρονται οι βασικότερες έννοιες που αφορούν την ασφάλεια, την πρόληψη καθώς και κάποιες από τις πλέον διαδομένες τακτικές προς αποφυγή της θυματοποίησης του πολίτη με την χρήση ηλεκτρονικού υπολογιστή. Με τις παρακάτω ¨μεθόδους¨ επιτυγχάνεται η αποτροπή μιας επίθεσης είτε πριν την εκδήλωση της είτε μετά.

3.1 Βασικές Έννοιες της Ασφάλειας

1. Εμπιστευτικότητα. Η εμπιστευτικότητα αναφέρεται στην προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών. Για την επίτευξη της εμπιστευτικότητας απαιτείται περιορισμός της πρόσβασης σε συστήματα και δεδομένα μόνο στους νόμιμους χρήστες.
2. Ακεραιότητα. Η διατήρηση της ακεραιότητας συνδέεται με την προστασία των δεδομένων από τυχόν τροποποίηση (προσθήκη, διαγραφή). Η αλλοίωση της ακεραιότητας μπορεί να προκύψει εξαιτίας κάποιου λάθους στο σύστημα ή ακόμα να είναι αποτέλεσμα δόλιας ενέργειας
3. Διαθεσιμότητα. Η διαθεσιμότητα σχετίζεται με τη δυνατότητα άμεσης προσπέλασης των συστημάτων και των δεδομένων, όταν ή όποτε απαιτείται. Στις επιθέσεις άρνησης εξυπηρέτησης υπάρχει παραβίαση της διαθεσιμότητας, όταν δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στους πόρους του συστήματος.

3.2 Βασικά προληπτικά εργαλεία και πώς αυτά λειτουργούν

Χρήση Λογισμικού Ασφαλείας - Λογισμικό Antivirus

Η διασπορά ιών είναι μια από τις πιο διαδεδομένες μορφές επίθεσης στο διαδίκτυο. Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους. Ένα τέτοιο πρόγραμμα που πρέπει να είναι εγκατεστημένο σε κάθε ηλεκτρονικό υπολογιστή επιτελεί τρείς βασικές λειτουργίες. Αυτές είναι: 1. Ανίχνευση των ιών : Η λειτουργία αυτή πραγματοποιείται κατόπιν ενέργειας του χρήστη (έλεγχος του σκληρού δίσκου μέσω του antivirus λογισμικού) ή μπορεί να γίνει και αυτόματα (έλεγχος από το antivirus λογισμικό που είναι φορτωμένο στη μνήμη RAM του ηλεκτρονικού υπολογιστή). 2. Προσδιορισμός ταυτότητας ιών: Στην περίπτωση που το σύστημα έχει προσβληθεί από κάποιον ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητα του. 3. Καθαρισμός των ιών : Αφού έχει προηγηθεί ο εντοπισμός του ιού, ακολουθεί η αφαίρεσή του. Το λογισμικό antivirus επιδιορθώνει το μολυσμένο από τον ιό αρχείο ή ακόμα μπορεί και να το διαγράψει.

Πιστοποίηση του χρήστη

Η πιο συνηθισμένη τεχνική πιστοποίησης της ταυτότητας ενός χρήστη είναι η δημιουργία και η χρήση συνθηματικών λέξεων ή συμβόλων. Έτσι το όνομα χρήστη (user id) και ο κωδικός πρόσβασης (password) είναι απαραίτητα στοιχεία προκειμένου να επιτραπεί η είσοδος του εξουσιοδοτημένου χρήστη στο σύστημα. Η τεχνική αυτή , είναι από τις πιο παλιές , όχι μόνο λόγο της απλότητας της αλλά και της μεγάλης ασφάλειας που προσφέρει . Σήμερα οι κωδικοί πρόσβασης αποτελούν αναπόσπαστο κομμάτι οποιουδήποτε πληροφοριακού συστήματος .Η επιλογή του κωδικού πρόσβασης είναι πολύ σημαντική . Πρώτη επιλογή των χρηστών είναι κωδικοί που μπορούν εύκολα να θυμούνται (Ονόματα , ημερομηνίες γέννησης , κλπ) με αποτέλεσμα κάποιος κακόβουλος να μπορεί να τους μαντέψει . Μεγαλύτερη ασφάλεια επιτυγχάνεται όταν η επιλογή κωδικού δεν είναι ελεύθερη στους χρήστες αλλά πραγματοποιείται από τους διαχειριστές του συστήματος .

Firewalls

Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπιση τους. Η σωστή πρακτική είναι το firewall να ρυθμίζεται έτσι ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις firewall ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες. Τα Firewalls δρουν ως φράκτες ανάμεσα στο ιντερνέτ και στο εσωτερικό δίκτυο ή έναν υπολογιστή και σταματάει διάφορους κινδύνους και επιθέσεις, συμπεριλαμβανομένων και ορισμένων ιών (virus). Τα Firewalls μπορεί να είναι λογισμικό που τρέχει σε έναν υπολογιστή (πχ. το windows firewall), λογισμικό που προστατεύει το δίκτυο (πχ. Microsoft ISA Server) ή συσκευή hardware συνδεδεμένη στο δίκτυο. Τα firewalls φιλτράρουν την πληροφορία που εισέρχεται στο δίκτυο ή εξέρχεται από αυτό, με βάση κανόνες τους οποίους έχουμε θέσει. Με τον τρόπο αυτό προστατεύεται το δίκτυο από εισβολείς (hackers, ορισμένους ιούς κλπ). Επιπλέον, απαγορεύεται η αποστολή πληροφορίας από τους υπολογιστές του δικτύου, όπως π.χ. ποιοί τύποι αρχείων επιτρέπεται να αποστέλλονται. Στα μειονεκτήματα των Firewalls καταλογίζονται το υψηλό οικονομικό κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και τέλος το γεγονός ότι η

προστασία που παρέχουν είναι εντελώς σχετική. Είναι γνωστό για παράδειγμα πως τα modems αποτελούν ένα σημείο εισόδου στο δίκτυο το οποίο υπερφαλαγγίζει κάθε firewall. Ένας σημαντικός τρόπος για προστασία από πολλά είδη επιθέσεων είναι η σχεδίαση της τοπολογίας του δικτύου ώστε να είναι δύσκολο να γίνει εισβολή. Ένα firewall είναι ένα επιπλέον επίπεδο προστασίας τοποθετημένο γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Ένα firewall που προστατεύει ένα δίκτυο θα περιλαμβάνει συνήθως ένα δρομολογητή (router) που μπορεί να προγραμματιστεί ώστε να μην επιτρέπει επιλεκτικά την πρόσβαση σε ένα δίκτυο, για παράδειγμα θα απορρίπτει πακέτα που δεν στέλνονται σε συγκεκριμένες επιτρεπόμενες θύρες. Όταν ένα πακέτο φτάνει στον δρομολογητή του firewall, αυτός το επεξεργάζεται και αποφασίσει αν θα το αφήσει να περάσει στο δίκτυο που προστατεύει ή όχι. Μια ακόμα ισχυρότερη χρήση ενός firewall είναι σε ένα σενάριο δυο επιπέδων προστασίας, όπου χρησιμοποιείται ένας δρομολογητής που παρακολουθεί την επικοινωνία με το ιντερνέτ και ένας ακόμη που παρακολουθεί την επικοινωνία στο εσωτερικό δίκτυο.

3.3 Κρυπτογραφία και Ασφάλεια

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών *κρυπτογράφησης* και *αποκρυπτογράφησης* με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ο ένας από τους δύο κλάδους της κρυπτολογίας (ο άλλος είναι η κρυπτανάλυση), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Κρυπτογράφηση καλείται η διαδικασία της επεξεργασίας και κωδικοποίησης της ψηφιακής πληροφορίας κατά τέτοιο τρόπο ώστε αυτή να παραμένει αναγνώσιμη στην κατανοητή μορφή της μόνο από τους εξουσιοδοτημένους παραλήπτες που διαθέτουν το κατάλληλο «κλειδί» - κώδικα, δηλαδή η πληροφορία καθίσταται εμπιστευτική. Αρχικά η τεχνολογία της κρυπτογράφησης δημιουργήθηκε με σκοπό την προστασία του απορρήτου του μηνύματος. Στην πορεία, η εξέλιξη της κρυπτογράφησης προσφέρει στον αποστολέα του μηνύματος μμεγαλύτερη ασφάλεια σχετικά με το ακέραιο αλλά και το απόρρητο του μηνύματος κατά την αποστολή του. Ένα κρυπτογραφικό σύστημα αποτελεί ένα σύνολο λειτουργιών οι οποίες είναι παραμετροποιημένες από κλειδιά και χρησιμοποιούνται για τη διατήρηση εχεμύθειας στην επικοινωνία. Με τις ενσωματωμένες λειτουργίες της ένκρυψης και της απόκρυψης, το σύστημα παρέχει ασφάλεια και προστασία στην ιδιωτικότητα, αποκλείοντας έτσι την χωρίς εξουσιοδότηση πρόσβαση σε υλικό που ορίστηκε να παραμείνει απόρρητο. Το κρυπτογραφικό περιεχόμενο δεν μπορεί να γίνει προσβάσιμο από οποιονδήποτε που θα προσπαθήσει να το προσπελάσει χωρίς να γνωρίζει τι περιέχει. Συνεπώς, αποκλείεται η έκθεση σε βλαπτικό υλικό για όποιον θα μπορούσε να προσβληθεί ακόμα και αν αυτό συνέβαινε τυχαία. Ένα σύγχρονο σύστημα κρυπτογράφησης αποτελείται από τέσσερα (4) βασικά σημεία. Αυτά είναι: 1. Το αρχικό μήνυμα. 2. Το κρυπτογραφικό σύστημα αποτελούμενο από έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο αποκρυπτογράφησης. 3. Το κρυπτογραφημένο μήνυμα. Πρόκειται για το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη. 4. Το κλειδί,

το οποίο είναι μια συμβολοσειρά. Η συμβολοσειρά αυτή χρησιμοποιείται στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης από τους αλγόριθμους Οι βασικότεροι στόχοι που επιτυγχάνονται με την κρυπτογράφηση είναι:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

3.4 Προστασία κατά την περιήγηση στο Διαδίκτυο

Συμβουλές για τους Γονείς

- Προτιμήστε να τοποθετήσετε τον Η/Υ σας σε χώρους, όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.
- Κάντε την πλοήγηση στο Διαδίκτυο μία οικογενειακή δραστηριότητα. Χρησιμοποιείστε τον Η/Υ μαζί με τα παιδιά σας.
- Ενημερώστε τα παιδιά σας για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chatrooms.
- Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.
- Διδάξτε τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ακόμα και ωράρια σχολείου ονόματα φίλων κ.λπ.) και να μην χρησιμοποιούν την κάρτα σας.
- Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου.
- Διδάξτε τα επίσης, να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν, μπορεί να είναι επικίνδυνοι.
- Χρησιμοποιείστε τα λεγόμενα «φίλτρα» που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητές σελίδες (βία, πορνογραφία).
- Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.α., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.
- Ενημερωθείτε σχετικά με τις αρμόδιες αρχές, που θα πρέπει να επικοινωνήσετε σε περίπτωση που συναντήσετε βλαβερό ή παράνομο περιεχόμενο στο Internet.

Συμβουλές Για νέους

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

Συμβουλές για ασφαλείς οικονομικές συναλλαγές

- Αποφεύγετε να πραγματοποιείτε οικονομικές συναλλαγές μέσω Διαδικτύου από Internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές . Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας.
- Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείτε για τις διαδικτυακές συναλλαγές:
  - Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.
  - Αποφεύγετε να χρησιμοποιείτε ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα
  - Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπής τους θα διευκολύνετε πολύ τους δράστες.
  - Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια κάρτες σας.
  - Μην δίνετε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι

τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.

- Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet banking.
- Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.
- Κάνετε αγορές μόνο από γνωστές εταιρείες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το Διαδίκτυο, χρησιμοποιείτε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.
- Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας.
  - Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιήστε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοση του.
  - Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχτείτε κατά τις περιηγήσεις σας στο διαδίκτυο.
  - Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

- Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mails):
  - Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό σας.
  - Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μην στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μίας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail). Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.
- Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων
- Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και

ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά.

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

Προστασία από το Spamming

- Να μην απαντάτε ποτέ σ' ένα spam e-mail και να μην κάνετε πουθενά κλικ, γιατί απλούστατα η απάντησή σας ή και η άρνησή σας θα επιβεβαιώσει την εγκυρότητα του δικού σας e-mail και έτσι το e-mail σας θα γίνει μια πολύτιμη πληροφορία για πολλούς spammers.
- Να έχετε μια πρόχειρη και μη συχνά χρησιμοποιούμενη ηλεκτρονική διεύθυνση, εκτός φυσικά από την κανονική, και να την δίνετε σε πρώτη ζήτηση έτσι ώστε να πηγαίνουν εκεί όλα τα ανεπιθύμητα e-mails.
- Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails. Να ελέγχετε πάντα αν αυτά τα προγράμματα-φίλτρα κάνουν σωστά το μπλοκάρισμα των spam e-mails.
- Να μην κάνετε ποτέ προώθηση (forward) των spam e-mails σε φίλους ή και τρίτους, γιατί κι αυτοί θα προστεθούν στην λίστα αποδοχής.
- Να μην παρασύρεστε ποτέ από δελεαστικούς τίτλους, όπως a very special message for you, earn money easily, urgent and confidential κ.α.
- Να μην δημοσιεύεται την διεύθυνση του ηλεκτρονικού ταχυδρομείου (e-mail). Η ύπαρξη της ηλεκτρονικής διεύθυνσης σε μια ιστοσελίδα, είναι σχεδόν σίγουρο ότι σύντομα θα φέρει πολλά μηνύματα spam στο γραμματοκιβώτιο σας.
- Να μην δίνετε εύκολα την διεύθυνση του ηλεκτρονικού ταχυδρομείου (e-mail). Πρέπει να είστε προσεκτικοί όταν επισκεπτόσαστε διάφορους δικτυακούς τόπους και ζητείται η συμπλήρωση προσωπικών στοιχείων και στοιχείων επικοινωνίας, όπως είναι το e-mail. Θα πρέπει να διαβάσετε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας για την οποία δεσμεύεται ο δημιουργός της ιστοσελίδας.
- Να μην απαντάμε ποτέ στα spam e-mails ακόμα και στην υποτιθέμενη ένδειξη διαγραφής, γιατί έτσι διαπιστώνεται η εγκυρότητα της ηλεκτρονικής μας διεύθυνσης και επομένως θα αποτελούμε πολύτιμο στόχο για τους spammers.
- Να χρησιμοποιείται ειδικά προγράμματα-φίλτρα.

Συμβουλές για ασφαλή χρήση κοινωνικών δικτύων

- Αποφύγετε να γράφεται πολύ προσωπικές πληροφορίες όπως διευθύνσεις κατοικίας, τηλέφωνα, επωνυμία της εταιρίας που εργάζεστε κτλ. Υπάρχουν πολλοί κακόβουλοι που μπορούν να χρησιμοποιήσουν τέτοιες πληροφορίες για να σας βλάψουν.
- Αν δεν μπορείτε να αποφύγετε να δημοσιεύσετε κάποια επικίνδυνη πληροφορία, φροντίστε να περιορίστε το σύνολο των ανθρώπων που μπορούν να την δουν. Οι

ιστοσελίδες κοινωνικών δικτύων σας παρέχουν την δυνατότητα διαβάθμισης κάθε πληροφορίας που εισάγεται στο προφίλ σας, έτσι ώστε να ορίζεται ποιοι μπορούν να έχουν πρόσβαση σε αυτές. Για παράδειγμα το Facebook παρέχει τρεις βασικές διαβαθμίσεις για κάθε πληροφορία στο προφίλ και στο timeline σας: Δημόσιο, Φίλοι φίλων, Φίλοι και Μόνο εγώ.

- Προσοχή στα spam μηνύματα και email. Είναι πιθανό να λάβετε emails ή μηνύματα μέσα στο κοινωνικό δίκτυο που χρησιμοποιείται με αποστολέα ένα όνομα κάποιου γνωστού σας, αναφέροντας μέσα σε αυτό πολλά στοιχεία της προσωπικής σας ζωής (γεγονός που σας κάνει να μην χαρακτηρίσετε το μήνυμα αυτό να είναι spam) και προτρέποντας σας να του αποκαλύψετε ευαίσθητα και επικίνδυνα προσωπικά δεδομένα, όπως διευθύνσεις, τηλέφωνα ή ακόμη και στοιχεία πιστωτικών καρτών.4
- Σιγουρευτείτε 100% πριν δημοσιεύσετε μια πληροφορία, ένα post ή μια φωτογραφία στο προφίλ σας. Μπορείτε βέβαια να την σβήσετε μετά από λίγο, αλλά ο χρόνος που αυτή παραμένει online μπορεί να χρησιμοποιηθεί από οποιονδήποτε.
- Προσπαθήστε να μάθετε περισσότερα για την χρήση του κοινωνικού δικτύου που χρησιμοποιείτε και ιδιαίτερα για τις ρυθμίσεις απορρήτου ώστε να είστε σε θέση να εκμεταλλευτείτε όλες τις δυνατότητες του και να τις χρησιμοποιήσετε για την ασφάλεια σας.

Συμπεράσματα

Η πληροφορία δε γνωρίζει σύνορα αλλά ούτε και το έγκλημα πια. Ο χρήστης του διαδικτύου είναι περισσότερο ευάλωτος από οποιονδήποτε άλλον δεδομένου ότι οι κίνδυνοι που ελλοχεύουν και από την πιο απλή χρήση του διαδικτύου είναι αναρίθμητοι και πολλαπλασιάζονται καθημερινά με γοργό ρυθμό. Οι δράστες εκμεταλλευόμενοι την ανωνυμία που προσφέρει το διαδίκτυο μπορούν να τελέσουν ακόμα και εγκλήματα που με τον παραδοσιακό τρόπο δε θα τολμούσαν καν να σκεφτούν. Είναι γενικά παραδεκτό πως η ηλεκτρονική εγκληματικότητα διογκώνεται καθημερινά και αποτελεί την ουσία της ασφαλείας των πληροφοριακών συστημάτων της σύγχρονης ψηφιακής κοινωνίας. Η ολοένα και αυξανόμενη χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου καθώς και οι γενικότερες αλλαγές που επέφεραν οι καινοτόμες τεχνολογίες, έχουν δώσει νέες διαστάσεις στη συμβατική εγκληματικότητα καθιστώντας την απειλητική και επικίνδυνη ακόμα και στους μέσους και ενημερωμένους χρήστες ηλεκτρονικού υπολογιστή. Αυτή η ραγδαία εξελισσόμενη πραγματικότητα όπως επίσης και η υπερεθνική διάσταση που παίρνουν κάποια από τα ηλεκτρονικά εγκλήματα είναι οι βασικότεροι παράγοντες που δυσχεραίνουν το έργο του νομοθέτη σχετικά με τη δίωξη και την ποινική αντιμετώπιση των διαφόρων περιστατικών. Οι σύγχρονες εγκληματικές απειλές χαρακτηρίζονται από τη χρησιμοποίηση της τεχνολογίας εξελιγμένων συστημάτων και υψηλής τεχνογνωσίας. Η αντιμετώπιση τους είναι ζήτημα καίριας σημασίας για κάθε οργανισμό που θα πρέπει να μεριμνά συνεχώς για την πρόληψη εκδήλωσης επιθέσεων, ανίχνευση τους αλλά και άμεση αντίδραση προς αποκατάσταση της προκληθείσας ζημιάς όταν αυτή συμβεί. Η όλη πολιτική ασφαλείας επιβάλλει συνδυασμό τεχνολογικών μέτρων, συνεχούς επιμόρφωσης και εκπαίδευσης του προσωπικού όπως και των απλών οικιακών χρηστών σε θέματα ασφάλειας. Τέλος, όσο αφορά το έργο των αρμόδιων διωκτικών αρχών, χρειάζεται εκσυγχρονισμός των υφιστάμενων υπηρεσιών δίωξης ηλεκτρονικού εγκλήματος καθώς και εκπαίδευση του προσωπικού των υπηρεσιών στη μεθοδολογία διερεύνησης εγκλημάτων στα οποία χρησιμοποιείται με οποιαδήποτε τρόπο η ψηφιακή τεχνολογία.

Βιβλιογραφία – Πηγές διαδικτύου

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

Ζάννη Αν. «*Το διαδικτυακό έγκλημα*», Αθήνα :Αντ. Ν. Σάκκουλας ,2005

Κριθαράς Θ. «*Ποινικό Δίκαιο και Διαδίκτυο*», Αθήνα: Νομική Βιβλιοθήκη ,2009

Furnell St. «*Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας*», (μετάφραση: Φ. Μηλιώνη), Αθήνα: Εκδόσεις Παπαζής ,2006

Τσουραμάνης Χρ. «*Ψηφιακή Εγκληματικότητα - Η (αν)ασφαλής όψη του διαδικτύου*» ,Αθήνα, Εκδ.Β.Ν. Κατσαρού 2005

Κ. Βλαχόπουλος «*Ηλεκτρονικό Έγκλημα*» , Αθήνα: Νομική Βιβλιοθήκη ,2007

http://www.saferinternet.gr

http://www.e-crime.gr

http://www.astynomia.gr

http://www.en.wikipedia.org

http://www.pharming-fishing.gr

http://el.wikibooks.org

http://electroniccrime.wordpress.com

https://sites.google.com/site/elektronikoenklema2012

https://iguru.gr

http://www.youth-health.gr