ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ - ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ»

ΑΛΒΕΡΤΗΣ ΧΡΗΣΤΟΣ

ΑΦΟΡΔΑΚΟΣ ΕΥΑΓΓΕΛΟΣ

ΡΑΠΤΗΣ ΣΤΥΛΙΑΝΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΑΡΙΣΤΕΙΔΗΣ ΜΠΑΚΑΛΗΣ

ΠΑΤΡΑ, 2016

ΠΡΟΛΟΓΟΣ

Η χρήση του διαδικτύου είναι μια από τις κυριότερες ασχολίες του σύγχρονου ανθρώπου. Εκπαίδευση, ψυχαγωγία και ενημέρωση περνάνε από τη χρήση του διαδικτύου. Για αυτό το λόγο η ασφάλεια του διαδικτύου είναι από τα κυριότερα μελήματα των παρόχων των διαδικτυακών εφαρμογών και των χρηστών.

Με την ολοκλήρωση της πτυχιακής μας εργασίας θα θέλαμε αρχικά να εκφράσουμε τις ευχαριστίες μας στον εποπτεύοντα καθηγητή μας κύριο Αριστείδης Μπακάλης για την υπομονή, την καθοδήγηση αλλά και τις χρήσιμες συμβουλές της σε όλη τη διάρκεια εκπόνησης της πτυχιακής μας εργασίας.

Επίσης, θα θέλαμε να ευχαριστήσουμε τους γονείς μας, για την ψυχολογική υποστήριξη που μας παρείχαν καθ΄ όλη τη διάρκεια των σπουδών μας.

ΠΕΡΙΛΗΨΗ

Στο πρώτο κεφάλαιο της παρούσας εργασίας παρουσιάζεται η έννοια του διαδικτύου, η χρήση του στη Ελλάδα καθώς και η διαδικασία μεταφοράς των μηνυμάτων και των προσωπικών δεδομένων.

Στο δεύτερο κεφάλαιο εισάγεται η έννοια της ασφάλειας του διαδικτύου, οι υπηρεσίες παροχής και σύνδεσης καθώς και ο χαρακτηρισμός του δικτύου υπολογιστών.

Στο τρίτο κεφάλαιο παρουσιάζονται τα στοιχεία της ανεπιθύμητης αλληλογραφίας, η εμφάνιση της και τα είδη της.

Στο τέταρτο κεφάλαιο προσδιορίζεται η έννοια του spam τα βασικά γνωρίσματα του, τα είδη του και οι παραλλαγές του.

Στο πέμπτο κεφάλαιο παρουσιάζονται οι απειλές της ασφάλειας του δικτύου και του ηλεκτρονικού ταχυδρομείου. Παρουσιάζονται οι τρόποι ασφάλειας και τα μέσα προστασίας της αλληλογραφίας καθώς και ο προσδιορισμός των ιών.

Τέλος παρουσιάζονται τα συμπεράσματα και η εκτενής βιβλιογραφία που χρησιμοποιήθηκε για την παρούσα εργασία.

SUMMARY

The first chapter of this paper the concept of the Internet occurs, its use in Greece as well as the process of transferring messages and personal data.

The second chapter introduces the concept of internet security, the supply and connection services and the classification of computer network.

The third chapter presents the elements of spam, the occurrence and types of.

The fourth chapter identifies the meaning of spam the main features of the species and its variants.

The fifth chapter presents the threat of network security and of the ilektronikoy tachydromeioy. Show how security and mail protection means and the determination of viruses.

Finally presents the conclusions and the extensive bibliography used for this work.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1
ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΑΛΛΗΛΟΓΡΑΦΙΑ

1.1..... Τ Ι ΕΙΝΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο αποτελεί μια σύνδεση υπολογιστών οι οποίοι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους μέσω ενός κοινού πρωτόκολλου γνωστό με την ονομασία TCP/IP (Transmission Control Protocol/Internet Protocol). Η μεταφορά αρχείων γίνεται μέσω του διαδικτύου εύκολα και με απλή διαδικασία. Οι κυριότερες ασχολίες των χρηστών του διαδικτύου είναι η αλληλογραφία, η μεταφορά εικόνων και η συζήτηση μεταξύ τους (Γκρίτζαλης, 2003).

Τα αρχεία στο διαδίκτυο μεταφέρονται μεταξύ δύο υπολογιστών με τη χρήση πρωτοκόλλου μεταφοράς (transfer protocol). Τα πρωτόκολλα που χρησιμοποιούνται κατά κύριο λόγο στη μεταφορά είναι :

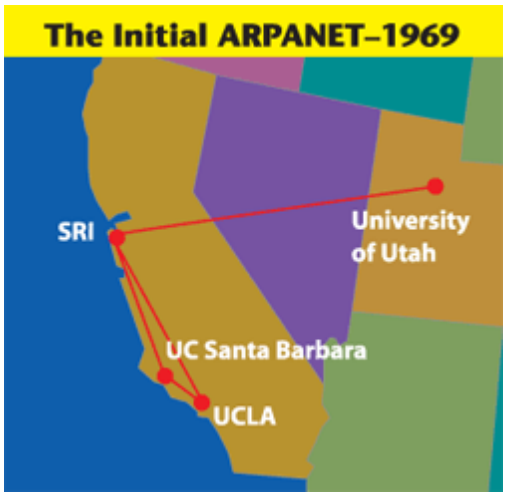
- **Hypertext Transfer Protocol (HTTP)**/ World Wide Web (WWW)
- **Network News Transfer Protocol (NNTP)**/ ομάδες συζητήσεων
- **Simple Mail Transfer Protocol (SMTP)**/ ηλεκτρονικό ταχυδρομείο
- **File Transfer Protocol (FTP)**: / μεταφορά αρχείων

1.2..... Ι ΣΤΟΡΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Κατά τη διάρκεια του ψυχρού πολέμου στην Αμερική πραγματοποιήθηκε η πρώτη προσπάθεια δημιουργίας του διαδικτύου. Ο J.K.R. Licklider υποστήριξε τη δημιουργία ενός δικτύου υπολογιστών οι οποίοι θα μετέφεραν πληροφορίες μεταξύ τους. Η λογική της δημιουργίας του διαδικτύου ήταν η προστασία από την Ρωσία σε περίπτωση επίθεσης. Ο Paul Baran κατάφερε να φέρει τη λύση σε ένα πρόβλημα

μεγάλης σημασίας που είχε προκύψει. Το δίκτυο έπρεπε να είναι αποκεντρωμένο ώστε σε περίπτωση επίθεσης να ήταν ασφαλής η επικοινωνία με τους άλλους υπολογιστές. Έτσι προέκυψε το κατανεμημένο δίκτυο το οποίο χρησιμοποίησε την νέα ψηφιακή τεχνολογία. Ο Leonard Kleinrock εισήγαγε την ανταλλαγή ψηφιακών δεδομένων με σκοπό την διατήρηση των πληροφοριών.

Το νέο δίκτυο υπολογιστών που δημιουργήθηκε ονομάστηκε ARPANET. Το 1696 λειτούργησε για πρώτη φορά το συγκεκριμένο δίκτυο το οποίο είχε τέσσερις κόμβους που συνδέονταν μεταξύ τους με 4 μικρουπολογιστές ο οποίοι βρίσκονταν στα πανεπιστήμια της Σάντα Μπάρμπαρα, του Λος Άντζελες, της Γιούτα και του Στάνφορντ. Έως το 1972 23 ακαδημαϊκά ιδρύματα της Αμερικής επικοινωνούσαν μεταξύ τους μέσω του συστήματος ARPANET. Στη συνέχεια εισήχθη η διαχείριση μέσω ηλεκτρονικού ταχυδρομείου.



Έως το 1979 είχαν χρησιμοποιήσει το δίκτυο αυτό και άλλες χώρες όπως η Νορβηγία και η Αγγλία. Το τέλος του συστήματος ARPANET έφτασε το 1989 λόγω μη επαρκούς χρηματοδότησης. Το National Science Foundation Net ήταν το νέο σύστημα που εισήχθη σε πολλές χώρες, ακαδημαϊκά ιδρύματα και κρατικά ιδρύματα.

Έως το 1990 το National Science Foundation Net λαμβάνει τη θέση του στις προτιμήσεις πολλών χωρών και την ίδια δεκαετία εισάγεται η έννοια του ιντερνέτ και το σύστημα Gopher όπου επιτρέπει την περιήγηση αρχείων μέσω ιντερνέτ. Τα δίκτυα κάνουν εφικτή την επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου (e-mail), της ηλεκτρονικής διάσκεψης (conferencing) και της ηλεκτρονικής συνομιλίας (IRC), των

ομάδων συζήτησης (newsgroups, forums), της μεταφοράς αρχείων (FTP-File Transfer Protocol) κτλ.

Τέλος έως το 1995 γίνεται η εισαγωγή του παγκοσμίου Ιστού με την ταυτόχρονη διαχείριση αρχείων με εικόνα, ήχο και κείμενο.

1.3..... ΣΧΕΤΙΚΗ ΟΡΟΛΟΓΙΑ

Παγκόσμιος Ιστός (World Wide Web - WWW)

Ο παγκόσμιος ιστός αποτελεί ένα τμήμα του διαδικτύου. Είναι το πιο αναπτυσσόμενο κομμάτι του. Χρησιμοποιεί ένα από τα πρωτόκολλα του Διαδικτύου, το Hypertext Transfer Protocol (HTTP). Αποτελεί το μέσο με το οποίο πραγματοποιείτε η ανάκτηση των πληροφοριών που προσφέρονται από το Διαδίκτυο.

Ιστοσελίδα (web page)

Όλες οι πληροφορίες που παρέχονται μέσω του Παγκόσμιου Ιστού είναι μορφοποιημένες με τη γλώσσα HTML (Hypertext Markup Language) σε μορφή ιστοσελίδων (web pages). Υπάρχουν εκατομμύρια διαθέσιμες ιστοσελίδες μέσω Ιντερνέτ. Οι ιστοσελίδες μπορεί να περιέχουν εκτός από κείμενο, εικόνες, video, ήχο, κινούμενες εικόνες κτλ.

Διακομιστής Ιστού (web server)

Ο διακομιστής ιστού είναι το μέσω στο οποίο βρίσκονται οι ιστοσελίδες. Στην ουσία ο διακομιστής είναι υπολογιστές οι οποίοι κατέχουν ένα ειδικό λογισμικό και είναι συνδεδεμένοι στο διαδίκτυο. Αποτέλεσμα της σύνδεσης αυτής είναι να επιτρέπετε η

πλοήγηση στις ιστοσελίδες σε όλους τους ενδιαφερόμενους. Η διάθεση των ιστοσελίδων γίνεται μετά από την αναζήτηση του χρήστη και ο διακομιστής στέλνει την πληροφορία.

Πρόγραμμα Περιήγησης (web browser)

Ο web browser (πρόγραμμα περιήγησης) αποτελεί ένα πρόγραμμα μέσω του οποίου πραγματοποιείτε η αναζήτηση από τους χρήστες. Ο διακομιστής εμφανίζει την ιστοσελίδα που αναζητά ο χρήστης. Παραδείγματα προγραμμάτων περιήγησης είναο το Internet Explorer, το Mozilla και το Google Chrome.

Διευθύνσεις Ιστού (Web Addresses)

Η μοναδικότητα της κάθε ιστοσελίδας προσδιορίζεται από τη διεύθυνση της γνωστή ως Uniform Resource Locator (URL). Η διεύθυνση της κάθε ιστοσελίδας βοηθά στον εντοπισμό της μέσα από τον διακομιστή ιστού. Η διεύθυνση του ιστού αποτελείτε από:

- το πρωτόκολλο μεταφοράς,
- το όνομα περιοχής (domain name) του διακομιστή Ιστού
- τη διαδρομή στο αρχείο της ιστοσελίδας
- το όνομα του αρχείου της ιστοσελίδας (Γκρίτζαλης, 2003)

αποτελείται από τα εξής μέρη:

- **http://** - χρησιμοποιείται το πρωτόκολλο μεταφοράς HTTP
- **www** - το όνομα του Web Server. Μπορεί να είναι οποιοδήποτε όνομα, αλλά το www είναι το όνομα που χρησιμοποιείται περίπου από το 90% των servers σήμερα.
- **www.sch.gr** - το όνομα περιοχής του διακομιστή Ιστού. Το τελευταίο μέρος δηλώνει το περιεχόμενο της σελίδας (πχ .com: εμπορικό, .edu: εκπαιδευτικό,

.gov: κυβερνητικό, .org: μη κερδοσκοπικό) ή την χώρα (πχ .au: Αυστραλία, .gr: Ελλάδα).

- **/postings/** - το όνομα του φακέλου που περιέχει το αρχείο της ιστοσελίδας.
- **publications.php** - το όνομα του αρχείου της ιστοσελίδας.

Υπερσύνδεσμος (hyperlink ή link)

Ο υπερσύνδεσμος είναι το μέσω που διευκολύνει την περιήγηση στον Παγκόσμιο Ιστό. Στην ουσία ο υπερσύνδεσμος αναγνωρίζει την πληροφορία και τη μετακίνηση εντός της ιστοσελίδας (Κοζύρης, 2006).

1.4..... Χ ΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ

Το Παγκόσμιο Οικονομικό Φόρουμ αναφέρει στην έκθεση του ότι η Ελλάδα το 2010-2011 καταλαμβάνει την 64η θέση μεταξύ 138 χωρών στην αξιοποίηση των τεχνολογιών πληροφορικής και δικτύου. Η έκθεση επίσης αναφέρει ότι η σύνδεση των τεχνολογιών πληροφορικής σε μια χώρα συμβάλει στην ανάπτυξη της οικονομίας, στον ανταγωνισμό καθώς και στην ποιότητα των παρεχόμενων υπηρεσιών. Στις πιο τεχνολογικά ανεπτυγμένες χώρες συγκαταλέγονται η Φιλανδία, η Δανία και οι χώρες της Αμερικής (Biesterfeld, 1998).

Η Ελλάδα είναι από της χώρες που άργησε να ενσωματώσει τις νέες πρακτικές της ψηφιακής επικοινωνίας. Η ανάπτυξη βέβαια στην ενσωμάτωση τους είναι ραγδαία. Αξίζει να σημειωθεί πως η Ελλάδα είναι μια χώρα που έχει χαμηλά ποσοστά διείσδυσης νέων στις τεχνολογίες πληροφορίας και επικοινωνιών με 1 στους 5 Έλληνες να χρησιμοποιούν τις νέες τεχνολογίες. Ακόμα, σύμφωνα με το Παρατηρητήριο για την Κοινωνία της Πληροφορίας, 20% των ελλήνων χρησιμοποιούν τις υπηρεσίες του Διαδικτύου τουλάχιστον μια φορά την εβδομάδα.

Στην περίπτωση των μεγάλων πόλεων παρουσιάζεται μια πιο γρήγορη ανάπτυξη τόσο στους χρήστες όσο και στα παροχές του διαδικτύου. Είναι προφανές ότι οι μικρότερες

ηλικίες 16-24 χρησιμοποιούν περισσότερο το διαδίκτυο σε ποσοστό που αγγίζει το 45% ενώ οι ηλικίες 25-35 χρησιμοποιούν το διαδίκτυο σε ποσοστό 30%.

Οι τιμές στην Ελλάδα σε σχέση με τις υπόλοιπες χώρε στης Ευρώπης που αφορούν τις παροχές του διαδικτύου χαρακτηρίζονται ως υψηλές. Το γρήγορο ιντερνέτ φαίνεται να βρίσκετε ακόμα σε χαμηλό επίπεδο. Οι χρήστες του διαδικτύου στην Ελλάδα συχνά αναζητούν πληροφορίες που αφορούν κυρίως τα είδη ρουχισμού και για οικονομικές αγορές οι οποίες πραγματοποιούνται μέσω διαδικτύου.

Οι ελληνικές επιχειρήσεις προσπαθούν να εφαρμόσουν διαδικτυακή παρουσία και να δίνουν ιδιαίτερη σημασία στη δυνατότητα ηλεκτρονικών πληρωμών. Οι ηλεκτρονικές επιχειρήσεις δίνουν ιδιαίτερη έμφαση στις παραγγελίες μέσω διαδικτύου ενώ οι μικρομεσαίες επιχειρήσεις προσπαθούν και αυτές να έχουν μεγαλύτερο μερίδιο αγοράς διαδικτυακά σε σχέση με την παραδοσιακή αγορά παρόλο που το ποσοστό τους κυμαίνεται στο 35%. Σημαντικός τομέας στην ηλεκτρονική πραγματικότητα της Ελλάδος παρουσιάζει η ψηφιοποίηση των υπηρεσιών του δημοσίου τομέα. Η ηλεκτρονική διακυβέρνηση αποτελεί την ψηφιακή συναλλαγή μεταξύ πολιτών-επιχειρήσεων και κράτους. Η Έλληνες καταναλωτές δε δηλώνουν μεγάλη ικανοποίηση για τη νέα διαδικτυακή παροχή υπηρεσιών του δημοσίου τομέα καθώς σε μεγάλο βαθμό θεωρούν ότι δεν είναι εύχρηστες. Παράδειγμα μη ικανοποίησης αποτελούν οι διαδικτυακές υπηρεσίες του ιδρύματος κοινωνικών ασφαλίσεων (Lee,2009).

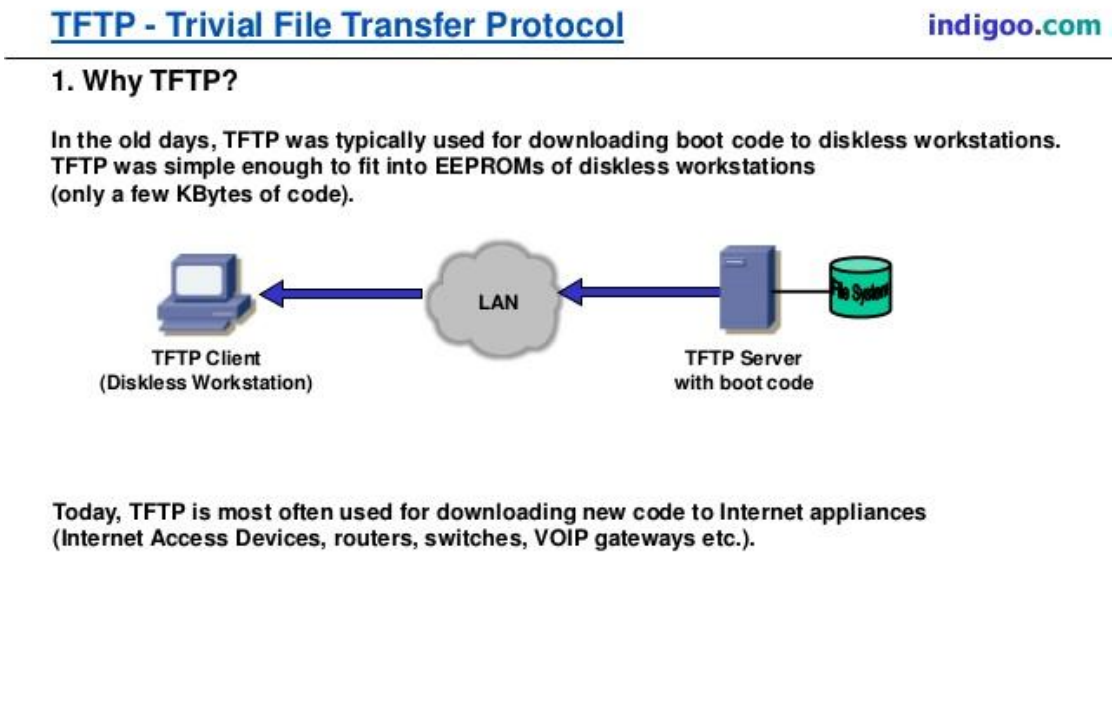
1.5 ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Η ηλεκτρική αλληλογραφία αποτελεί την πιο σημαντική και λαοφιλή διαδικτυακή υπηρεσία. Στην ηλεκτρονική αλληλογραφία ο χρήστης έχει τη δυνατότητα να στέλνει και να λαμβάνει μηνύματα σε μία ηλεκτρονική διεύθυνση με τη διαδικασία να παρομοιάζεται με την παραδοσιακή αποστολή και λήψη του ταχυδρομείου. Ο προσδιορισμός του κάθε μηνύματος σχετίζεται με την ηλεκτρονική διεύθυνση του αποστολέα, με τα περιεχόμενα του μηνύματος που μπορεί να είναι εικόνα ή κείμενο και την ηλεκτρονική διεύθυνση του παραλήπτη. Η ανάκτηση των

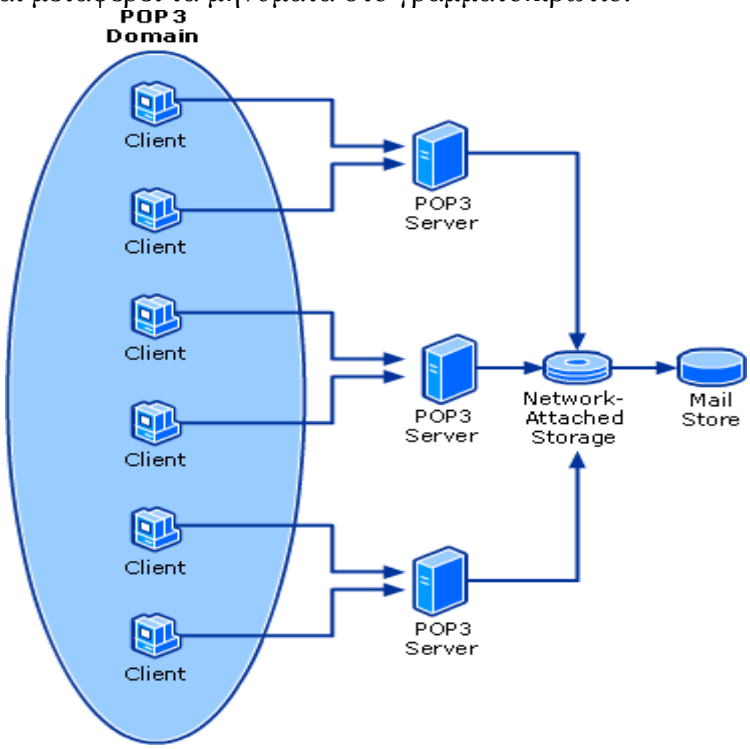
μηνυμάτων γίνονται από τα ηλεκτρονικά γραμματοκιβώτια (mailboxes) τα οποία καταχωρούν και φυλήσουν τα μηνύματα (Akyildiz,1995).

1.6..... Η ΜΕΤΑΦΟΡΑ ΤΩΝ ΜΗΝΥΜΑΤΩΝ

Για να πραγματοποιηθεί η αποστολή του μηνύματος χρησιμοποιείτε το πρωτοκόλλα μεταφοράς πληροφορίας του Διαδικτύου, του Total Transfer Protocol (SMTP) το οποίο δίνει τη δυνατότητα να μεταφερθεί το μήνυμα από ένα Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου (Mail Server) του Διαδικτύου σε ένα άλλο. Σε κάθε μήνυμα υπάρχει η επικεφαλίδα η οποία χρησιμεύετε για να αναγνωριστεί η ηλεκτρική διεύθυνση του παραλήπτη, η ηλεκτρική διεύθυνση και το όνομα του αποστολέα, και λεπτομέρειες για τούς κόμβους από τους οποίους θα εισαχθεί το μήνυμα μέχρι να καταλήξει στον παραλήπτη (Δουκίδης, 2001).



Το πρωτόκολλο Post Office Protocol (POP) είναι υπεύθυνο για την ανάκτηση των μηνυμάτων ενώ η Τρίτη του έκδοση (POP3) είναι η επικρατούσα στη διαχείριση της αλληλογραφίας μέσω των προγραμμάτων e-mail Clients τα οποία δημιουργούν ένα γραμματοκιβώτιο το οποίο σε κάθε σύνδεση του Ηλεκτρονικού Ταχυδρομείου ανακτά και μεταφέρει τα μηνύματα στο γραμματοκιβώτιο.



1.7 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ – ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Η αξιοπιστία των πληροφοριών στο Διαδίκτυο έχει οδηγήσει πολλούς χρήστες στην παραπληροφόρηση καθώς αρκετές από αυτές μπορεί να είναι ψευδείς ή λανθασμένες. Για αυτό λοιπόν, ο χρήστης θα πρέπει να ενημερώνεται συνεχώς και να «σερφάρει» με ασφάλεια στο κόσμο του Διαδικτύου. Επίσης, οφείλει να φιλτράρει οποιαδήποτε πληροφορία εμφανίζεται ως ύποπτη ώστε αν προκύψει κάποιο πρόβλημα να διαφυλάξει τα προσωπικά του δεδομένα και τα αρχεία στον υπολογιστή.

Η ελεύθερη μεταφορά προσωπικών δεδομένων είναι χαρακτηριστικό φαινόμενο του Διαδικτύου. Αρκετοί χρήστες δημοσιοποιούν προσωπικά τους στοιχεία χωρίς να σκέπτονται τις αρνητικές συνέπειες που θα έχει σε αυτούς. Οι παγίδες που μπορούν να εμφανιστούν είναι ποικίλοι όπως π.χ. διαδικτυακή παρενόχληση (cyber bulling), υποκλοπή προσωπικών στοιχείων, εισαγωγή ιών απ την εφαρμογή κάποιου προγράμματος στον υπολογιστή κ.α.

Για αυτό ο χρήστης είναι απαραίτητο να ακολουθεί κάποιους κανόνες προστασίας για την περιήγηση του στο Διαδίκτυο:

- Είναι σημαντικό, ο χρήστης να γνωρίζει ότι η δημοσιοποίηση ή αποστολή των στοιχείων του μέσω ηλεκτρονικού ταχυδρομείου μπορεί να παραβιαστεί από οποιοδήποτε. Για αυτό το λόγο, θα πρέπει να αποφεύγεται η αποστολή υλικού είτε αυτό είναι φωτογραφικό ή άλλου είδους.
- Η χρήση μακροσκελών κωδικών με αυξημένη πολυπλοκότητα είναι δύσκολο να βρεθούν. Υπάρχουν μηχανές αναζήτησης ακόμα και προγράμματα που μπορούν εύκολα να εντοπίζουν κωδικούς για αυτό ο χρήστης θα πρέπει να είναι ιδιαίτερα προσεκτικός. Οι κωδικοί αυτοί θα πρέπει να έχουν τουλάχιστον 9 χαρακτήρες που θα εμπεριέχονται μέσα σύμβολα, αριθμοί, γράμματα.

- Οι κωδικοί αυτοί απαγορεύονται να σταλθούν μέσω ηλεκτρονικού ταχυδρομείου.
- Αλλαγή των κωδικών ανά τακτά χρονικά διαστήματα.
- Όταν ο χρήστης κάνει εγγραφή σε κάποια ιστοσελίδα οφείλει να σιγουρέψει την εγκυρότητα της πριν προχωρήσει στην αποστολή των προσωπικών του δεδομένων που απαιτείται για την εγγραφή. Συνίσταται όταν δεν αποφαίνεται η αξιοπιστία της ιστοσελίδας ο χρήστης καλό θα ήταν να εγγράφεται με διαφορετικό κωδικό για την προφύλαξη τόσο των στοιχείων όσο και των αρχείων του υπολογιστή του.
- Όταν γίνεται χρήση κάμερας (web camera) χρειάζεται να είναι προσεκτικός καθώς συνδυάζεται η οπτική επαφή με την ομιλία.
- Κρίνεται απαραίτητο η απενεργοποίηση ή η κάλυψη της κάμερας αν δεν χρησιμοποιείται απ το χρήστη προς αποφυγή κίνδυνων.

1.8 ΠΡΟΣΤΑΣΙΑ ΣΗΜΑΝΤΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Πέραν όμως των παραπάνω κανόνων κυριαρχούν και άλλοι πιο σημαντικοί που αφορούν την προστασία των δεδομένων στον υπολογιστή κα είναι οι εξής:

- Είναι σημαντικό ο χρήστης να κρατά αντίγραφα των αρχείων (backup) του σε περίπτωση που γίνει μια πιθανή υποκλοπή των δεδομένων του ή η εισβολή κάποιους ιού στον ηλεκτρονικό υπολογιστή του.

- Αν ο σκληρός δίσκος υποστεί ζημιά ή κακόβουλος ιός καταστρέψει αρχεία στον υπολογιστή ο χρήστης θα πρέπει να απευθυνθεί σε τεχνικό ώστε να αντιμετωπιστεί το πρόβλημα. Ακόμα κι αν διαγράφουν ή καταστραφούν αρχεία υπάρχουν προγράμματα που μπορούν να τα επαναφέρουν.

- Είναι δυνατόν πολλά αρχεία πού έχουν σταλθεί από αγνώστους αποστολείς να περιέχουν ιούς οπότε εφιστάται η προσοχή κατά το άνοιγμα αυτών των μηνυμάτων.

- Τέλος, υπάρχουν εταιρίες που ασχολούνται με την διαφύλαξη προσωπικών δεδομένων ή αρχείων των χρηστών και μπορούν να προστατεύσουν τον χρήστη σε τέτοιου είδους περιπτώσεις.

1.9 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Οι ηλεκτρονικές συναλλαγές διέπονται κι αυτές από κάποιους κανόνες προστασίας που αφορούν τους χρήστες όπως:

- Οι ηλεκτρονικές συναλλαγές πρέπει να πραγματοποιούνται μόνο σε έγκυρα sites (e-bay, Amazon κ.α.) που ο χρήστης γνωρίζει
- Ο χρήστης αν δεν μπορεί να επαληθεύσει την αξιοπιστία της ιστοσελίδας μπορεί να πληκτρολογήσει και να βρει τυχόν κριτικές για αυτήν από άλλους χρήστες.
- .Όταν πραγματοποιούνται συναλλαγές μέσω πιστωτικής κάρτας οι χρηστές θα πρέπει να είναι προσεκτικοί ώστε να μην γίνει κάποια παραβίαση κατά την συναλλαγή. Για αυτό όλοι χρηστές οφείλουν να ελέγχουν συχνά τους τραπεζικούς τους λογαριασμούς.

1.9.1 ΑΣΦΑΛΕΙΑ ΚΑΤΑ ΤΗΝ ΆΜΕΣΗ ΣΥΝΟΜΙΛΙΑ

Αναμφισβήτητα ο ρόλος των κοινωνικών δικτύων (social media) έχει επηρεάσει κατά πολύ την ζωή των ανθρώπων και ειδικότερα των νέων. Τα κοινωνικά δίκτυα πέραν ότι είναι ιστότοποι ευχάριστης ενασχόλησης εγκυμονούν και πολλούς κινδύνους για τους χρηστές. Έπειτα, ο χρήστης είναι απαραίτητο να γνωρίζει τις βασικές λειτουργίες τέτοιων δικτύων και να μην αποκαλύπτει προσωπικά του στοιχεία, παρά μόνο όταν εξασφαλίσει την εγκυρότητα των δικτύων αυτών.

Το Διαδίκτυο μας προσφέρει πολλούς τρόπους άμεσης συνομιλίας ένας από αυτούς είναι το «chat».Πρόκειται για ένα πλήθος χρηστών που συναντώνται σε ένα διαδικτυακό ιστότοπο ο οποίος ονομάζεται «δωμάτιο επικοινωνίας» (chat room) και επικοινωνούν μεταξύ τους μέσω μηνυμάτων ή κάνοντας χρήση της κάμερας για ζωντανή συνομιλία (live chat). Το chat δίνει την δυνατότητα στους ανθρώπους και ειδικότερα στους νέους να επικοινωνούν γρήγορα και άμεσα με άλλους ανθρώπους ανά την υφήλιο.

Για να πραγματοποιηθεί η συνομιλία μεταξύ των χρηστών δεν είναι αναγκαία η εγκατάσταση κάποιου προγράμματος στον υπολογιστή ή ειδικού λογισμικού(π.χ. το IRC ή διαφορές μορφές τύπων messengers). Η πρόσβαση σε αρκετά δωμάτια επικοινωνίας (chat rooms) είναι ανεξάρτητη οποιοσδήποτε μπορεί έχοντας απλά ένα ψευδώνυμο να εισέλθει ή να εξέλθει στις συζητήσεις.

Επίσης, αρκετοί χρηστές προτιμούν την ιδιωτική συνομιλία (private chat) αποσυνδέονται δηλαδή από τους υπόλοιπους για να επικοινωνούν με μια συγκεκριμένη ομάδα ή άτομα που θέλουν.

1.9.2 ΟΙ ΕΠΙΚΙΝΔΥΝΕΣ ΠΑΓΙΔΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΓΙΑ ΤΟΥΣ ΑΝΗΛΙΚΟΥΣ

Συγχρόνως, κάνοντας χρήση ψευδωνύμων οι χρηστές διατηρούν την ανωνυμία τους. Με αποτέλεσμα, να παρακινούν το παιδί-χρήστη και να δημιουργούν την ψευδαίσθηση της ασφάλειας όταν αυτό βρίσκεται στο χώρο του σπιτιού του ή σε κάποιο Internet cafe. Έτσι, αυτός ο τρόπος επικοινωνίας μετατρέπεται σε μια από τις επικίνδυνες και σοβαρές παγίδες του Διαδικτύου.

Αξίζει να σημειωθεί, ότι κατά τη διάρκεια τέτοιου είδους συνομιλιών έχουν καταγράφει καταγγελίες των ίδιων των παιδιών ότι παρενοχλήθηκαν λεκτικά ακόμα και σεξουαλικά από διαφόρους επιτηδείους ώστε να υπάρξει επιθυμητή συνάντηση μεταξύ τους.

Παράλληλα, έχουν παρατηρηθεί σε πολλές χώρες του εξωτερικού δεκάδες κρούσματα εξαφάνισης παιδιών, όπου παρασύρθηκαν από παιδόφιλους ή έπεσαν

θύματα παιδικής πορνογραφίας τους οποίους και συνάντησαν στα λεγόμενα «chat rooms».

Είναι αναγκαίο, τόσο οι γονείς όσο και οι εκπαιδευτικοί να είναι σε επαγρύπνηση και ενημερωμένοι για τις παγίδες που κρύβει αυτή η παγκόσμια μηχανή αναζήτησης ειδικότερα τα «chat rooms» ώστε να μπορέσουν να προστατέψουν τις ζωές των ανηλίκων παιδιών.

Για αυτό, και η περιήγηση σε τέτοιου είδους ιστότοπους είναι ιδιαίτερα επικίνδυνη για τους ανήλικους χρήστες. Από την άλλη μεριά αν οι γονείς δεν καταφέρουν να αποτρέψουν ή να ελέγξουν τα παιδιά τους, χρειάζεται να τους εξηγήσουν την επικινδυνότητα υπάρχει στο Διαδίκτυο και να μην αποκαλύπτουν προσωπικά δεδομένα τους που στόχο έχει την παραπλάνηση τους από διάφορους επιτήδειους.

Οι χρήστες όταν επικοινωνούν μέσω των «chat rooms» οφείλουν να μην αποκαλύπτουν προσωπικά δεδομένα τους όπως π.χ. αριθμό τηλεφώνου, διεύθυνση του ηλεκτρονικού τους ταχυδρομείου, όνομα κ.α. και να αρνούνται να στείλουν οποιοδήποτε φωτογραφικό υλικό σε αγνώστους, ούτε να πραγματοποιούν συναντήσεις μαζί τους. Θεωρείται επιβεβλημένο, να γνωρίζουν ότι λόγω της ανωνυμίας τους ότι δεν είναι προστατευμένοι.

Συχνό φαινόμενο, αποτελούν πολλοί επιτήδειοι οι όποιοι εντοπίζοντας την IP address των χρηστών αποκτούν πρόσβαση στα αρχεία τους και εισάγουν έτσι ιούς με κακόβουλο λογισμικό. Οι ανήλικοι χρήστες επιβάλλεται να συζητούν με τους γονείς τους για τους νέους φίλους που κάνουν σε αυτά τα δωμάτια επικοινωνίας και να φροντίζουν να επικαλούνται για τυχόν παρενόχληση τους από αγνώστους στα «chat rooms».Τέλος, οι γονείς είναι ανάγκη να βρίσκονται σε επαγρύπνηση και να ενεργοποιούν τους νέους να δημιουργούν δεσμούς επικοινωνίας με φίλους τους που βρίσκονται μακριά και γνωρίζουν ήδη παρά με αγνώστους σε διάφορους ιστότοπους .

(https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-)

1.10ΔΙΑΜΟΙΡΑΣΜΟΣ ΑΡΧΕΙΩΝ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ(FILE SHARING)

Αρχικά, μέσω του file sharing οι χρηστές έχουν την δυνατότητα να διαμοιράζονται οποιαδήποτε αρχεία μεταξύ τους με την βοήθεια του Διαδικτύου. Η διαδικασία αυτή πραγματοποιείται μέσα από διάφορα προγράμματα όπως π.χ. Dropbox.(?) Κάποια φυσικά είναι επί πληρωμή κάποια άλλα όχι. Έπειτα, όσοι χρήστες χρησιμοποιούν το ίδιο πρόγραμμα και συνδέονται μέσω Διαδικτύου ένα τμήμα του σκληρού δίσκου του υπολογιστή τους γίνεται κοινόχρηστο.

Κάθε χρήστης αναζητά αρχεία απ τους υπολογιστές άλλων χρηστών και δημιουργεί αντίγραφα στο δικό του υπολογιστή. Για αυτό το λόγο τα προγράμματα που συμμετέχουν σε αυτή τη σύνδεση επικοινωνίας μεταξύ των υπολογιστών λέγονται ομότιμης σύνδεσης προγράμματα (peer to peer programs). Δημιουργούνται έτσι αυξημένες διαδικτυακά πληθυσμιακές κοινότητες όπου αντιγράφεται και αποθηκεύεται κάθε είδους υλικό χωρίς καθόλου κόστος για τον χρήστη. Ταυτόχρονα, από την χρήση προγραμμάτων file sharing εγκυμονούν και πολλοί κίνδυνοι όπως :

- Η «υγεία» του υπολογιστή μας είναι απαραίτητη για την σωστή λειτουργία του. Οι ιοί και προγράμματα spyware μπορούν να καταστρέψουν αρχεία στον υπολογιστή και να στείλουν τις πληροφορίες σε τρίτους ακόμα κι αν δεν είναι συνδεδεμένος ο χρήστης στο Διαδίκτυο.
- Πρόσβαση των ανηλίκων σε πορνογραφικό υλικό. Άθελα τους κατά την περιήγηση τους στο Διαδίκτυο γίνονται δέκτες τέτοιου είδους μηνυμάτων. Βέβαια, πολλά προγράμματα έλεγχου πλοήγησης όπως είναι κι αυτό του Σχολικού Δικτύου δεν προσφέρουν την απαραίτητη προστασία ώστε να αποφεύγονται τέτοιου είδους καταστάσεις.
- Η απόκτηση (download) και η διάθεση (upload) αρχείων χωρίς την άδεια του κατόχου μπορεί να δημιουργήσει νομικά προβλήματα. Για αυτό το λόγο υπάρχουν νόμοι που προστατεύουν τον κάτοχο για την ελεύθερη διάθεση των αρχείων του στο Παγκόσμιο Ιστό.

· Προσωπικά δεδομένα που έχει ο χρήστης στον υπολογιστή μπορούν να γίνουν κοινόχρηστα σε άλλους χρηστές που χρησιμοποιούν το πρόγραμμα αυτό.

1.11 ΔΙΚΤΥΟ ΥΠΟΛΟΓΙΣΤΩΝ

Αρχικά, τα δίκτυα υπολογιστών είναι ένα σύνολο από αυτόνομους ή μη, διασυνδεδεμένους υπολογιστές. Αυτόνομοι λέγονται οι υπολογιστές όταν κάποιος άλλος υπολογιστής δεν μπορεί να ελέγξει τη λειτουργία του και διασυνδεμένοι όταν κάνουν ανταλλαγή πληροφοριών μεταξύ τους.

Οι υπολογιστές χωρίζονται σε διακομιστές (servers) και πελάτες (clients). Ο διακομιστής είναι αυτός που διευκολύνει τους επιμέρους υπολογιστές του δικτύου (clients), προωθώντας τους λογισμικό και στοιχεία κείμενων κ.α. που είναι αποθηκευμένα στην βάση δεδομένων του υπολογιστή (server). Ένας διακομιστής οφείλει να είναι συνδεδεμένος με τους «πελάτες» του και να έχει το κατάλληλο λογισμικό.

ΚΕΦΑΛΑΙΟ 2
ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 ΕΙΣΑΓΩΓΗ

Αδιαμφισβήτητα, όλο και περισσότεροι άνθρωποι αποκτούν το δικαίωμα της εύκολης πρόσβασης στο διαδίκτυο κάνοντας το απαραίτητο εργαλείο στην καθημερινότητα τους και στην κοινωνία γενικότερα. Η διάχυση της πληροφορίας μέσω του διαδίκτυο έχει επηρεάσει τις ζωές των ανθρώπων λόγω του καταιγισμού πληθώρας πληροφοριών που συναντούν καθημερινά. Έτσι, ολόκληρη η κοινωνία συμμετέχει κι αυτή στις αλλαγές που έχει επιφέρει το Διαδίκτυο, καθώς με ένα «κλικ» έχει μπροστά στην οθόνη της όποια πληροφορία θέλει.

Αυτό έχει σαν αποτέλεσμα να επηρεάζονται οι ανθρώπινες σχέσεις, η ψυχολογία των ανθρώπων, οικονομικό και πολιτικό σκηνικό, η εκπαίδευση, ο κλάδος των επιχειρήσεων και του εμπορίου μέχρι και αλλαγές στο τρόπο εργασίας των ατόμων. Η ταχύτατη διάθεση της πληροφορίας ενώνει εμπειρίες και κουλτούρες ανθρώπων από όλο τον κόσμο καθιστώντας το Διαδίκτυο ικανό μέσο επικοινωνίας και της γνώσης. Τα δίκτυα δίνουν την δυνατότητα να εισαχθούν οι χρήστες σε ένα ευρύ περιβάλλον παγκοσμιοποίησης και διαλόγου , μέσα από το όποιο θα γεφυρώνονται σχέσεις χωρίς όρια και περιορισμούς. Αξίζει να σημειωθεί ότι, οι χρήστες το περισσότερο τους χρόνο στο Διαδίκτυο τον αφιερώνουν σε ιστοσελίδες ή φόρουμ για συζητήσεις σε διάφορα θέματα καθώς και σε ομαδικές συνομιλίες.

Έπειτα, αυτή η ελεύθερη πρόσβαση παρακινεί τους χρήστες στην αναζήτηση ολοένα και περισσοτέρων πληροφοριών με διαφόρους συνομιλητές που μπορεί να τους προτείνουν από τυχερά παιχνίδια μέχρι γευσιγνωσία κρασιών και πρόσβαση σε βιβλιοθήκες Ιδρυμάτων.

(https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-)

Με αυτόν τον τρόπο τα προσωπικά δεδομένα δεν με μένουν ανεπηρέαστα διαταράσσεται έτσι η ιδιωτική ζωή των χρηστών και έχει ανεπανόρθωτες συνέπειες.

Σε μια προσπάθεια κινητοποίησης κυβερνητικών και μη οργανισμών για την ασφαλή πλοήγηση στο Διαδίκτυο και συγκεκριμένα για την προστασία των

ανηλίκων παιδιών, το Ευρωπαϊκό Κοινοβούλιο (Απόφαση αριθ. 276/1999/ΕΚ το Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Ιανουαρίου 1999) προχωρεί στην υλοποίηση μιας ευρωπαϊκής εκστρατείας και ενός προγράμματος δράσης πληροφόρησης και συνειδητοποίησης, με χρηματοδότηση από τον προϋπολογισμό της Ευρωπαϊκής Ένωσης, για να πληροφορηθούν οι γονείς και όλοι όσοι ασχολούνται με παιδιά (δάσκαλοι, κοινωνικοί λειτουργοί κ.λπ.) για τον καλύτερο τρόπο (περιλαμβανομένων των τεχνικών ζητημάτων) προστασίας των ανηλίκων από την έκθεση σε περιεχόμενο που θα μπορούσε να είναι βλαβερό για την ανάπτυξή τους, έτσι ώστε να εξασφαλιστεί η ευημερία τους. Σε μια προσπάθεια προστασίας της προσωπικής ζωής, της μάθησης, του παιχνιδιού, των ηλεκτρονικών μας δεδομένων και στα πλαίσια μιας ασφαλούς πλοήγησης στο Διαδίκτυο συνοψίζουμε κάποια βασικά σημεία τα οποία θα πρέπει να λαμβάνουν υπόψη τους τόσο οι αρχάριοι όσο και οι προχωρημένοι χρήστες του.

2.2 ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟΝ ΠΑΓΚΟΣΜΙΟ ΙΣΤΟ

Ο Παγκόσμιος Ιστός (World Wide Web) είναι ένα από τα σημαντικότερα εργαλεία του Internet, καθώς δίνει την δυνατότητα στους χρήστες τους να έχουν ελεύθερη πρόσβαση σε ένα παγκόσμιο δίκτυο διάχυσης της πληροφορίας. Αναφέρεται σε πληθώρα αρχείων που είναι αποθηκευμένα σε εκατομμύρια υπολογιστές ανά την υφήλιο και τα οποία ανανεώνονται συνεχώς από τους χρήστες που τα εισάγουν στον χώρο τους τις ιστοσελίδες τους.

Το λεγόμενο «σερφάρισμα» στις ιστοσελίδες αυτές γίνεται μέσω ειδικευμένων προγραμμάτων περιήγησης τους «browsers» όπως π.χ. Internet Explorer, Google Chrome κ.α. απαιτείται όμως από τους χρήστες να έχουν επίγνωση του κίνδυνου που πολλές φορές θα αντιμετωπίσουν με την πλοήγηση τους στο Διαδίκτυο καθώς προέχει η ασφάλεια του υπολογιστή και των προσωπικών στοιχείων τους.

Τα μέτρα τα οποία είναι απαραίτητα για την σωστή και ασφαλή περιήγηση στο Παγκόσμιο Ιστό εξαρτώνται από: α) τις προσφερόμενες υπηρεσίες του πάροχου σύνδεσης (Internet Provider) β) από ενέργειές που ακολουθεί ο ίδιος ο χρήστης π.χ. η εγκατάσταση ειδικευμένων προγραμμάτων Antivarious με σκοπό την προστασία του

υπολογιστή από κακόβουλα λογισμικά κα ιούς δ) η άμεση εγκατάσταση των τελευταίων ενημερώσεων του λειτουργικού συστήματος του υπολογιστή οι οποίες περιλαμβάνουν ενημερώσεις ασφαλείας, λογισμικού ε) έλεγχος των εκτελέσιμων αρχείων (.exe) για την εγκυρότητα τους .

(https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-)

2.3 ΥΠΗΡΕΣΙΕΣ ΠΑΡΟΧΟΥ ΣΥΝΔΕΣΗΣ

Μια ασφαλής πλοήγηση στο Διαδίκτυο εξαρτάται σημαντικά από τις υπηρεσίες του παρόχου σύνδεσης στο Διαδίκτυο(Internet Provider).Έτσι, λοιπόν ένας σωστός παροχέας μπορεί να προσφέρει:

- Φιλτράρισμα των ιστοσελίδων(websites) που επισκέπτεται ο χρήστης.
- Φιλτράρισμα των μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mails) του χρήστη.

Χαρακτηριστικό παράδειγμα φιλτραρίσματος αποτελεί το Πανελλήνιο Σχολικό Δίκτυο του οποίου η εποπτεία πραγματοποιείται με δύο τρόπους:

- Ανιχνεύει τις ιστοσελίδες που έχει επισκεφτεί ο χρήστης και αναζητά λέξεις με ακατάλληλο περιεχόμενο π.χ. τυχερά παιχνίδια
- Διατηρεί βάση δεδομένων που του επιτρέπει να ψάχνει αν η ιστοσελίδα είναι ορθή ή όχι.

Για να απαγορεύσει την πρόσβαση σε μια συγκεκριμένη ιστοσελίδα εμφανίζει προειδοποιητικό μήνυμα σε καθεμία για τις παραπάνω περιπτώσεις. Όταν πρόκειται για εισερχόμενη ηλεκτρονική αλληλογραφία ανιχνεύει για τυχόν ύπαρξη κακόβουλου λογισμικού ή ιών στα επισυναπτόμενα αρχεία, ενώ μέσω ειδικών φίλτρων προστατεύει τον παραλήπτη από spam e-mails(ανεπιθύμητη αλληλογραφία).

Είναι φανερό ότι, κάποιες ιστοσελίδες που εισάγουν ακατάλληλο περιεχόμενο δεν πολλές φόρες δεν περιέχουν τις λέξεις που «σαρώνουν» τα προγράμματα φιλτραρίσματος ή δεν έχουν καταχωρηθεί στις βάσεις δεδομένων τους. Παράλληλα, αρκετές σελίδες απαγορεύονται από το πρόγραμμα φιλτραρίσματος παρόλο που δεν επηρεάστηκαν από κακόβουλο υλικό. Τέλος ο χρήστης θα πρέπει να ενημερώνει τον διαχειριστή του προγράμματος (Cashemaster) σε τέτοιες περιπτώσεις ώστε αυτός να επιληφθεί της παρούσας κατάστασης.

2.4 ΕΝΕΡΓΕΙΕΣ ΤΟΥ ΊΔΙΟΥ ΤΟΥ ΧΡΗΣΤΗ

Είναι φανερό ότι, αν ο χρήστης δεν λάβει τα απαραίτητα μέτρα προστασίας και δεν είναι προσεκτικός στην περιήγηση του στο Παγκόσμιο Ιστό δεν μπορεί από μονός του ο παροχος σύνδεσης να αντιμετωπίσει το πρόβλημα του θα δημιουργηθεί. Ο σημαντικότερος κανόνας η εξονυχιστική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στον υπολογιστή. Ο χρήστης θα πρέπει να εξετάζει τα μηνύματα προτού κάνει «κλικ» πάνω τους ώστε να δει το περιεχόμενο τους , ενώ όταν εισάγεται αβίαστα ένα παράθυρο να το «κλείνει» εφόσον δεν το καταλαβαίνει (Pop up Windows).

Τα Pop up Windows είναι παράθυρα που ενεργοποιούνται χωρίς να το προκαλέσει ο χρήστης και το θέμα τους διαφέρει κάθε φορά και το ποίο μπορεί να είναι:

- Διαφημίσεις
- Προειδοποιητικά μηνύματα που παρακινούν τον χρήστη να προβεί σε βήματα (ώστε να αποδεχτεί προσφορές) με ανυπολόγιστες συνέπειες.
- Προτάσεις για παιχνίδια στην πλειονότητα τους τυχερά
- Δωρεές
- Παραπομπές σε σελίδες ερωτικού περιεχομένου και πληθώρα σχετικού είδους προτάσεων.

Επιπλέον για να μπορέσουν οι χρήστες να κλείσουν αυτά τα παράθυρα πέραν του **X** που βρίσκεται δεξιά πάνω στην οθόνη του υπολογιστή υπάρχουν κι άλλες εναλλακτικές οι οποίες είναι :

- Κάνοντας δεξί «κλικ» στην γραμμή κατάστασης και επιλογή «κλείσιμο» στο αντίστοιχο εικονίδιο.
- Πληκτρολογώντας ταυτόχρονα alt+ F4(επιλογή που κλείνει το ενεργό παράθυρο)

Για να σταματήσει ο χρήστης την εμφάνιση τέτοιων παραθύρων πρέπει να εγκαταστήσει ειδικά προγράμματα (Pop blockers/ Killers) και τα οποία τα παρέχονται στο Διαδίκτυο. Επίσης, η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την είσοδο του χρήστη σε κάποιες ιστοσελίδες. Για παράδειγμα, υπάρχουν εταιρίες που μέσω των Pop up Windows προσφέρουν προγράμματα εφαρμογών ώστε να εμφανίζουν πλήθος ιστοσελίδων(Flash Player από την Macromedia, Mwpluggin από την LCSI για το Microworlds κ.λπ.).Τέλος, ο χρήστης έχει την δυνατότητα να απενεργοποιήσει τον blocker.

Μια άλλη ενέργεια που ακολουθεί ο χρήστης είναι η διαδικασία τοπικής αποθήκευσης (Download).Μέσω αυτής αποθηκεύει τοπικά στον υπολογιστή προγράμματα που διατίθενται στο Διαδίκτυο, οφείλει όμως ιδιαίτερη προσοχή καθώς επρόκειτο να περιέχουν κακόβουλους ιούς οι όποιοι να μπορεί να καταστρέψουν αρχεία του υπολογιστή.

Για αυτό το λόγο ο χρήστης χρειάζεται να εξασφαλίζει την εγκυρότητα της ιστοσελίδας την οποία προτείνει το πρόγραμμα. Συνήθως, οι ιστοσελίδες πιστοποιούν την εγκυρότητα τους μέσω μηνύματος κατά τη διάρκεια της λήψης.

Είναι σημαντικό να αναφέρουμε την ρύθμιση ασφαλείας φυλλομετρητών. Οι τελευταίες εκδόσεις φυλλομετρητων (π.χ. Google Chrome) εισάγουν σε όλα τα επίπεδα ρυθμίσεις για την προστασία κατά την περιήγηση του χρήστη. Εάν ο χρήστης δεν έχει τις απαραίτητες γνώσεις για αυτές τις ρυθμίσεις καλύτερα να απευθυνθεί σε έναν τεχνικό.

Επιπρόσθετα, η εγκατάσταση προγραμμάτων θεωρείται απαραίτητη για την ασφάλεια του υπολογιστή. Οι χρήστες έχουν την δυνατότητα να εγκαταστήσουν προγράμματα φιλτραρίσματος (filtering software) ή τειχών προστασίας (firewalls)

στον υπολογιστή ώστε να αποτρέψουν τους εξωτερικούς παράγοντες (κακοήθεις ιοί, spyware), κάνοντας τις απαραίτητες ρυθμίσεις. Οι καινούργιες εκδόσεις των Windows προσφέρουν ενσωματωμένο πρόγραμμα Firewall.

Επιπλέον, η προστασία του ηλεκτρονικού υπολογιστή θεωρείται αυτονόητη. Οι κίνδυνοι που παραμονεύουν κατά την περιήγηση του χρήστη σε ιστοσελίδες, chat rooms, blogs, social media είναι εξαιρετικά επικίνδυνοι, καθώς πολλές φορές εμπεριέχουν ιούς ή διαφημίσεις ακαταλλήλου περιεχομένου. Έτσι, υπάρχει περίπτωση να καταστραφούν αρχεία στον ηλεκτρονικό υπολογιστή.

2.5 ΧΑΡΑΚΤΙΡΙΣΜΟΣ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Το δίκτυο ηλεκτρονικών υπολογιστών διακρίνεται μέσω συγκεκριμένων χαρακτηρισμών σε κάποιες κατηγορίες.

- Ανάλογα με τον τρόπο σύνδεσης τους χωρίζονται σε **ασύρματο** και **ενσύρματο** δίκτυο**.**
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χωρίζονται σε **ιδιωτικό** (private) και **δημόσιο** (public) δίκτυο.
- Αναλόγως με την γεωγραφική κάλυψη του δικτύου υπολογιστών διαχωρίζονται σε: α)**Τοπικά δίκτυα ή LAN(Local Area Networks)** τα οποία εξυπηρετούν καθημερινούς σκοπούς της κοινωνίας β) **Δίκτυα ευρύτερης περιοχής ή WAN (Wide Area Network)** παρέχουν την δυνατότητα επικοινωνίας σε μακρινές αποστάσεις γ) το **Μητροπολιτικό δίκτυο ή MAN(Metropolitan Area Network**) είναι μια διαφορετική εκδοχή του τοπικού δικτύου και εξυπηρετεί κυρίως τις επιχειρήσεις δ) **Δίκτυα Προστιθέμενης Αξίας (Value Added Networks-VAN)** αφορούν δημόσια δίκτυα και προσφέρουν μεταφορά και πρόσβαση δεδομένων σε βάσεις δεδομένων εμπορίου και λογισμικού.

ΚΕΦΑΛΑΙΟ 3

ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

3.1 ΟΡΙΣΜΟΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Η αλληλογραφία η οποία στέλνεται σε διάφορους παραλήπτες χωρίς οι ίδιοι να το επιθυμούν και χωρίς να έχουν έρθει σε επαφή με τον αποστολέα ονομάζεται «ανεπιθήμητη αλληλογραφία». Ο σκοπός της εμφάνισης των συγκεκριμένων μηνυμάτων είναι η διαφήμιση ή η προώθηση προιόντων καθώς επίσης και η ενημέρωση των παραληπτών.

Στα χαρακτηριστικά του συγκεκριμένου είδους αλληλογραφίας περιλαμβάνονται:

- η αποστολή μηνυμάτων στους παραλήπτες χωρίς να έχουν προκαλέσει ή να έχουν επικοινωνήσει με τον αποστολέα. Αυτό σημαίνει ότι είναι απρόκλητη.
- Η αποστολή μηνυμάτων στους παραλήπτες με σκοπό την προώθηση και τη διαφήμιση προιόντων ή υπηρεσιών. Αυτό την καθιστά εμπορική.
- Τέλος, άλλο ένα χαρακτηριστικό του συγκεκριμένου είδους αλληλογραφίας είναι το γεγονός ότι αποστέλλεται σε πολλά άτομα. Αυτό την καθιστά μαζική.

Οι λόγοι για τους οποίους κρίνεται απαραίτητο να αντιμετωπίζεται και να διαγράφεται η ανεπιθύμητη αλληλογραφία είναι οι εξής:

- Αρχικά η ανεπιθύμητη αλληλογραφία εγκυμονεί κινδύνους καθώς μπορεί σε αυτά τα μηνύματα είτε να παρουσιάζονται προϊόντα ή υπηρεσίες που δεν ανταποκρίνονται σε αυτό που εμφανίζεται (δηλαδή υπάρχει αμφιβολία για την ποιότητα τους) είτε να παρουιάζονται μηνύματα σεξουαλικού περιεχομένου είτε μηνύματα τα οποία έχουν ως σκοπό την οικονομική εξαπάτηση των παραληπτών.
- Στη συνέχεια τα συγκεκριμένα μηνύματα δύναται να δημιουργήσουν προβλήματα στους εξυπηρετητές της ηλεκτρονικής αλληλογραφίας ενώ παράλληλα δημιουργούν προβλήματα και στην πρόσβαση στα συστήματα των παραληπτών.
- Τέλος, η ανεπιθύμητη αλληλογραφία εγκυμονεί κινδύνους ως προς την ασφάλεια του διαδικτυακού περιβάλλοντος. Η ανεπιθύμητη αλληλογραφία που αποστέλλεται σε αρκετές περιπτώσεις είναι αρχεία τα οποία εμπεριέχουν ιούς.

3.2 Η ΕΜΦΑΝΙΣΗ ΤΗΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Κάνοντας μια ιστορική αναδρομή στην εμφάνιση της ανεπιθύμητης αλληλογραφίας αξίζει να αναφερθεί ότι παρουσιάστηκε για πρώτη φορά στα τέλη της δεκαετίας 1970. Μια κατασκευαστική εταιρεία ηλεκτρονικών υπολογιστών από την Αμερική με την ονομασία DEC δημιούργησε ένα νέο προϊόν. Με πρωτοβουλία ενός χειριστή που ονομαζόταν Einar Stefferud στάλθηκαν προσκλήσεις για μία δεξίωση μέσω του διαδικτύου σε καταναλωτές για την προώθηση αυτού του προϊόντος χρησιμοποιώντας ηλεκτρονικές διευθύνσεις από το δίκτυο ARPANET. Αυτό είχε σαν φυσικό επακόλουθο η συγκεκριμένη κατασκευαστική εταιρεία να τιμωρηθεί διότι παραβίασε κανόνες που σχετίζονται με την πολιτική της.

3.3 ΕΙΔΗ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Στη συνέχεια, σε αυτή την ενότητα θα προσδιοριστούν ορισμένες έννοιες οι οποίες σχετίζονται με τα είδη της ανεπιθύμητης αλληλογραφίας. Ειδικότερα:

- **Spamming:** η συγκεκριμένη έννοια αναφέρεται στην δραστηριότητα που πραγματοποιείται και αποστέλλονται μαζικά μηνύματα σε πολλούς παραλήπτες.
- **Spam:** αυτός ο όρος αναφέρεται στα μηνύματα που λαμβάνει ο παραλήπτης τα οποία δεν τα επιθυμεί και στην ουσία πρόκειται για το αποτέλεσμα της δραστηριότητας του Spamming.
- **Spoofing:** Πρόκειται για έναν όρο ο οποίος αποτελεί μια ενέργεια κατά την οποία πραγματοποιείται παράνομη πρόσβαση σε έναν υπολογιστή και με τη χρήση στοιχείων από νόμιμους χρήστες αποστέλλονται μηνύματα τα οποία εγκυμονούν κινδύνους είτε ασφαλείας είτε οικονομικής απάτης.
- **Host:** ο συγκεκριμένος όρος χρησιμοποιείται για να προσδιορίσει έναν υπολογιστή δικτύου ο οποίος συμβάλλει στην παροχή συγκεκριμένων υπηρεσιών όπως είναι η δυνατότητα πρόσβασης στο δίκτυο.
- **Postmaster:** η συγκεκριμένη έννοια χρησιμοποιείται για να προσδιορίσει τους υπεύθυνους που διαχειρίζονται τις σελίδες ηλεκτρονικών ταχυδρομείων (Δουκίδης, 2001).

3.4 Η ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ

Σε καθημερινή βάση οι παραλήπτες δέχονται πολλαπλά μηνύματα τα οποία αποτελούν ανεπιθύμητη αλληλογραφία ενώ πολλές φορές παρατηρείται η λήψη πολλαπλών ίδιων μηνυμάτων στους παραλήπτες. Το περιεχόμενο των συγκεκριμένων μηνυμάτων αποτελείται κατά κύριο λόγο από προϊόντα ή υπηρεσίες αμφιβόλου ποιότητας.

3.5 ΟΙ ΛΟΓΟΙ ΠΟΥ ΚΑΘΙΣΤΟΥΝ ΤΗΝ ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ ΜΕΓΑΛΟ ΠΡΟΒΛΗΜΑ

Στη συνέχεια θα παρουσιαστούν οι λόγοι για τους οποίους οι ανεπιθύμητη αλληλογραφία αποτελεί ένα μεγάλο πρόβλημα:

- Αρχικά ένα από τα προβλήματα είναι το κόστος. Τα μηνύματα ανεπιθύμητης αλληλογραφίας που στέλνονται στους παραλήπτες είναι πάρα πολλά. Το κόστος αποστολήα αυτών των μηνυμάτων είναι πάρα πολύ μικρό για αυτούς που τα στέλνουν ενώ για τους παραλήπτες είναι πολύ μεγαλύτερο.
- Επίσης, άλλος ένας λόγος που καθιστά την ανεπιθύμητη αλληλογραφία πρόβλημα είναι η εξαπάτηση που προκαλεί στους παραλήπτες. Στην ουσία πρόκειται για μια απάτη καθώς οι αποστολείς των μηνυμάτων (junk emailers) χρησιμοποιώντας διάφορες τεχνικές προκειμένου να ανοίξει η ανεπιθύμητη αλληλογραφία που αποστέλλεται.
- Ένας άλλος λόγος αποτελεί το γεγονός ότι είναι ενοχλητικό να αποστέλλονται τέτοιου είδους μηνύματα τα οποία δεν έχουν ελεγχθεί, μπορεί να εμπεριέχουν ιούς, δεν είναι νόμιμα κλπ.
- Τέλος, η ανεπιθύμητη αλληλογραφία αποτελεί ένα μεγάλο πρόβλημα καθώς θεωρείται απάτη λόγω του περιεχομένου των μηνυμάτων τα οποία προωθούν ή προϊόντα αμφιβόλου ποιότητας ή για οικονομική εξαπάτηση.

3.6 ΛΟΓΟΙ ΑΠΟΣΤΟΛΗΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Οι λόγοι για τους οποίους αποστέλλονται τέτοιου είδους μηνύματα είναι κατά κύριο λόγο για την προώθηση προϊόντων ή υπηρεσιών. Το περιεχόμενο των συγκεκριμένων μηνυμάτων δύναται να είναι:

- σεξουαλικού περιεχομένου (τηλεφωνικές γραμμες ή δικτυακές)
- προσκλήσεις τζόγου μέσω του διαδικτύου

3.7 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΚΑΤΑ ΤΗΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

ΝΟΜΟΣ 2251/1994-Προστασία των καταναλωτών

Άρθρο 4 – Σύμβαση από απόσταση

«Παρ 6. Η χρησιμοποίηση των τεχνικών επικοινωνίας πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή. Απαγορεύεται χωρίς την συναίνεση του καταναλωτή η χρησιμοποίηση τεχνικών επικοινωνίας για την πρόταση σύναψης σύμβασης όπως τηλεφώνου αυτόματης κλήσης, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου επικοινωνίας.»

Άρθρο 9 – Διαφήμιση. Έννοια παραπλανητικής και αθέμιτης διαφήμισης.

«Παρ 10. Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήση ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνο αν συναινεί ρητά ο καταναλωτής.

Παρ 11. Ανεξάρτητα από τον περιορισμό της προηγούμενης παραγράφου, η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας (άμεση διαφήμιση) επιτρέπεται μόνο αν ο προμηθευτής ή άλλος για λογαριασμό του προμηθευτή κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του καταναλωτή που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως κατάλογο ή άλλα δημοσιευμένα στοιχεία, ή από άλλο φυσικό ή νομικό πρόσωπο, εφόσον ο καταναλωτής εγκρίνει ρητά την μεταβίβαση των προσωπικών του

στοιχείων για το σκοπό της άμεσης διαφήμισης. Ο διαφημιστής είναι υποχρεωμένος να αναφέρει στον καταναλωτή τον τρόπο με τον οποίο περιήλθαν σε γνώση του τα προσωπικά στοιχεία του καταναλωτή.

Παρ 12. Στις περιπτώσεις των παραγράφων 10 και 11, ο προμηθευτής οφείλει να διακόψει κάθε μορφή άμεσης διαφήμισης και να διαγράψει τα προσωπικά στοιχεία του καταναλωτή, εφόσον το ζητήσει ο καταναλωτής.»

ΝΟΜΟΣ 2472/1997-Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Άρθρο 19 – Αρμοδιότητες, λειτουργία και αποφάσεις της Αρχής

«Παρ 4. Η Αρχή τηρεί τα ακόλουθα μητρώα:

α) Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.

β) Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.

γ) Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.

δ) Μητρώο προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή
υπηρεσιών εξ αποστάσεως.

ε) Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.

στ) Μητρώο Απόρρητων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απόρρητων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.»

ΝΟΜΟΣ 2774/1999-Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Άρθρο 9 – Μη ζητηθείσες κλήσεις

«1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση, ιδίως με χρήση αυτόματων συσκευών κλήσεως ή συσκευών τηλεομοιοτυπίας ή η

πραγματοποίηση μη ζητηθείσων κλήσεων γενικώς με οποιοδήποτε τηλεπικοινωνιακό μέσο με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών ή για κάθε είδους διαφημιστικούς σκοπούς επιτρέπεται μόνο στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους.

2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθείσων κλήσεων για τους παραπάνω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις. Ο φορέας παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιώω, υποχρεούται να καταχωρεί τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερόμενου.

3. Οι ανωτέρω ρυθμίσεις δεν ισχύουν για τους συνδρομητές που είναι νομικό πρόσωπα, εκτός εάν ο νόμιμος εκπρόσωπός τους δηλώσει ότι δεν επιθυμεί τη λήψη μη ζητηθείσων κλήσεων που γίνονται για τους παραπάνω σκοπούς.

4. Οι δηλώσεις των προηγούμενων παραγράφων γίνονται χωρίς επιβάρυνση και απευθύνονται στο φορέα παροχής δημοσίου τηλεπικοινωνιακού δικτύου ή και διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.» (Προεδρικο διαταγμα 131/2003)

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 131/2003-Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (Οδηγία για το ηλεκτρονικό εμπόριο)

Άρθρο 6 – Μη ζητηθείσα εμπορική επικοινωνία

«1. Εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με ηλεκτρονικό ταχυδρομείο και εφόσον δεν απαγορεύεται, πρέπει να αναγνωρίζεται σαφώς και επακριβώς ευθύς ως περιέλθει σ'αυτόν.

2. Με την επιφύλαξη των διατάξεων της ΚΥΑ Ζ1-496/2000 (Β΄ 1545) για την προστασία των καταναλωτών για τις εξ αποστάσεως συμβάσεις, του Ν. 2472/97 (Α 50) για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και των διατάξεων του Ν. 2774/99 (Α 287) για την προστασία της ιδιωτικής ζωής στον επικοινωνιακό τομέα οι φορείς παροχής υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου οφείλουν να τηρούν και να συμβουλεύονται τακτικά μητρώα «επιλογών», όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες.» (Προεδρικο διαταγμα 131/2003)

ΝΟΜΟΣ 3471/2006-Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Άρθρο 11- Μη ζητηθείσα επικοινωνία

«1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (fax) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθείσων επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθείσων επικοινωνιών για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες επικοινωνίες. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερόμενου.

3. Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.

4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που

έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας.

5. Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.» (ΝΟΜΟΣ 3471/2006)

Άρθρο 14- Αστική ευθύνη

«1. Φυσικό ή νομικό πρόσωπο που, κατά παράβαση του νόμου αυτού, προκαλεί περιουσιακή βλάβη υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση.

2. Η κατά το άρθρο 932 Α.Κ. χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται, κατ' ελάχιστο, στο ποσό των δέκα χιλιάδων ευρώ (10.000 €), εκτός αν ζητηθεί από τον ενάγοντα μικρότερο ποσό. Η χρηματική ικανοποίηση επιδικάζεται ανεξάρτητα από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

3. Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τη διαδικασία των άρθρων 664 έως 676 Κ.Πολ.Δ., ανεξάρτητα από την έκδοση ή μη απόφασης της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών για τη διαπίστωση παρανομίας ή την άσκηση ποινικής δίωξης.»

Οι Έλληνες χρήστες του διαδικτύου δεν είναι απροστάτευτοι από την εγχώρια νομοθεσία όσον αφορά την ανεπιθύμητη αλληλογραφία. Με το προεδρικό διάταγμα 131/2003 ορίζεται πως εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με το ηλεκτρονικό ταχυδρομείο πρέπει να αναγνωρίζεται μόλις αυτή περιέλθει σε αυτόν. Δηλαδή, αυτό σημαίνει πως πρέπει να αναφέρεται το θέμα του ηλεκτρονικού μηνύματος καθώς και τα στοιχεία του αποστολέα, για να μπορεί έτσι να αναγνωριστεί η ιδιότητα του αποστολέα.

Με την τήρηση της παραπάνω προϋπόθεσης αντιμετωπίζεται μόνο το μέρος που έχει σχέση με το κόστος που έχει η ανεπιθύμητη αλληλογραφία στον παραλήπτη και δεν ασχολείται καθόλου με το κόστος διαχείρισης του δικτύου, το οποίο αυξάνεται για τους παροχείς πρόσβασης στο Διαδίκτυο. Βέβαια η παραπάνω ρύθμιση έχει σαν προϋπόθεση την μη απαγόρευση της ανεπιθύμητης αλληλογραφίας. (ΝΟΜΟΣ 3471/2006)

Η προϋπόθεση αυτή αναφέρεται στην παράγραφο 2 του προεδρικού διατάγματος, σύμφωνα με την οποία οι φορείς παροχής υπηρεσιών που αναλαμβάνουν την αποστολή μη αιτηθείσας εμπορικής επικοινωνίας μέσω του ηλεκτρονικού ταχυδρομείου, πρέπει να συμβουλεύονται μητρώα «επιλογών», τα οποία αναφέρονται στους νόμους 2472/1997 και 2774/1999. Σύμφωνα, με τον νόμο 2251/1994 που αφορά τις πωλήσεις από απόσταση, απαγορεύεται η χρήση τεχνικών (όπως το ηλεκτρονικό ταχυδρομείο) για την πρόταση σύναψης σύμβασης χωρίς την συναίνεση του καταναλωτή. Επίσης, αναφορικά με την αποστολή διαφημιστικών μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου, ο ίδιος νόμος ορίζει πως αυτή επιτρέπεται μόνο αν

συναινεί ρητά ο καταναλωτής. Αυτό σημαίνει, πως η συναίνεση πρέπει να αναφέρεται στην συγκεκριμένη μορφή διαφήμισης, έστω και αν υπάρχουν προηγούμενες συναλλακτικές σχέσεις μεταξύ του διαφημιστή και του καταναλωτή. Όμως, η αποστολή διαφημιστικών μηνυμάτων επιτρέπεται αν ο προμηθευτής κάνει χρήση στοιχείων που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις με τον καταναλωτή από πηγές όπως είναι κατάλογοι ή άλλα δημοσιευμένα στοιχεία, εφόσον ο καταναλωτής εγκρίνει την μεταβίβαση των στοιχείων του για τον σκοπό της άμεσης διαφήμισης.

Το νομικό πλαίσιο που αφορά την αποστολή μη αιτηθείσας εμπορικής επικοινωνίας μέσω e-mail συμπληρώνεται με τις διατάξεις του δικαίου που αφορούν την προστασία των προσωπικών δεδομένων. Σύμφωνα, με τον νόμο 2774/1999 υιοθετείται η «εκ των προτέρων ρητή συγκατάθεση» του
καταναλωτή για την αποδοχή της εμπορικής επικοινωνίας. Επίσης, προβλέπεται και η δημιουργία ενός μητρώου, όπου μπορούν να καταχωρηθούν όσοι δεν επιθυμούν την λήψη ηλεκτρονικής αλληλογραφίας διαφημιστικής μορφής.

Η τήρηση Μητρώου «προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως» αποτελεί, σύμφωνα με τον νόμο 2472/1997, αρμοδιότητα της Αρχής Δεδομένων Προσωπικού Χαρακτήρα. Ωστόσο, η Ελλάδα είναι μία από τις χώρες που έλαβαν ειδοποίηση από την Ευρωπαϊκή Επιτροπή για την έγκαιρη ενσωμάτωση της οδηγίας 2002/58/ΕΚ έως τις 31 Οκτωβρίου 2003 με αποτέλεσμα την παραλίγο παραπομπή της στο Διεθνές Ευρωπαϊκό Κοινοβούλιο. Ο νόμος 3471/2006 αποτελεί τροποποίηση του ήδη υπάρχοντα νόμου 2472/1997, με την ενσωμάτωση της οδηγίας 2002/58/ΕΚ και αφορά την προστασία των προσωπικών δεδομένων χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών με την θέσπιση των προϋποθέσεων που πρέπει να υπάρχουν για την επεξεργασία τους.

Στον νόμο αυτό αναφέρεται πως η πραγματοποίηση μη ζητηθείσων επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών επιτρέπεται μόνο αν ο συνδρομητής (καταναλωτής) έχει εκ των προτέρων συμφωνήσει ρητώς καθώς και πως στην περίπτωση που ο συνδρομητής έχει δηλώσει αντίθετος στην αποδοχή των μη ζητηθεισών επικοινωνιών, ο φορέας έχει υποχρέωση να καταχωρίσει αυτές τις δηλώσεις σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι διαθέσιμος στον κάθε ενδιαφερόμενο.

Η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου απαγορεύεται αν δεν αναφέρεται ευδιάκριτα η ταυτότητα και η έγκυρη ηλεκτρονική διεύθυνση του αποστολέα και η παράβαση των προστατευτικών διατάξεων για τους χρήστες, παρέχει στους θιγόμενους αποζημίωση τόσο για την περιουσιακή όσο και τη μη περιουσιακή ζημία που μπορεί να φτάσει έως και 100.000 ευρώ (ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 131/2003).

ΚΕΦΑΛΑΙΟ 4
SPAM

4.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ SPAM

Τα χαρακτηριστικά του Spam εστιάζουν σε τρία βασικά σημεία. Αρχικά, το Spam περιγράφεται ως **απρόκλητο** καθώς δεν δημιουργείται κάποια σχέση ανάμεσα σε παραλήπτες και αποστολέα που να δικαιολογεί ή να προκαλεί συγκεκριμένου είδους επικοινωνία. Δεύτερον έχει χαρακτηριστεί **εμπορικό** καθότι πολλές φορές τα μηνύματα που αποστέλλονται σχετίζονται με την προβολή και τη διαφήμιση προϊόντων ή υπηρεσιών ώστε να γίνει πραγματοποιήσιμη η προσέλκυση νέων πελατών και η αύξηση των πωλήσεων(*http://www.gateweb.gr/el/support/email/avoid-spam.html*).

Τέλος, έχει χαρακτηριστεί και **μαζικό** εφόσον η αποστολή των μηνυμάτων ακολουθεί ένα μεγάλο αριθμό παραληπτών. Μολονότι, τις περισσότερες φορές οι παραλήπτες δέχονται όμοια ή εν μέρει διαφοροποιημένα μηνύματα.

Ταυτοχρόνως, πέραν των χαρακτηριστικών που αναφέρθηκαν παραπάνω κυριαρχούν και τα εξής:

- Οι παραλήπτες δεν μπορούν να διαγραφούν απ τις λίστες των αποστολέων .Σε κάθε περίπτωση μια διαγραφή σημαίνει ότι υπάρχει ορισμένη ηλεκτρονική διεύθυνση που μπορεί να επιβεβαιωθεί.
- Με τη χρήση συγκεκριμένων τεχνικών πραγματοποιείται η αποστολή των μηνυμάτων, που έχει ως αποτέλεσμα αποκρύπτεται η πραγματική ταυτότητα του αποστολέα .
- Ο παραλήπτης δεν έχει την δυνατότητα επικοινωνίας με τον αποστολέα καθώς δεν υπάρχει η έγκυρη ηλεκτρονική διεύθυνση του δεύτερου .
- Τα μηνύματα στέλνονται χωρίς διάκριση μέσω αυτοματοποιημένων μέσων στον παραλήπτη .
- Το Spam τις περισσότερες φορές εμπεριέχει κακόβουλο ή παράνομο περιεχόμενο .
- Το περιεχόμενο αυτών των μηνυμάτων μπορεί να είναι αναληθές ώστε να παραπλανήσει τον παραλήπτη .

- Για να γίνει η απόκτηση των ηλεκτρονικών διευθύνσεων των παραληπτών χρησιμοποιήθηκε ένα λογισμικό ανίχνευσης διευθύνσεων (οι αναφερόμενες «αραχνες») ή να έχουν αγοραστεί έναντι μικρού κόστους από εταιρίες που αγοράζουν CD με τέτοιου είδους περιεχόμενο (Roger, 2000).

4.2 ΙΣΤΟΡΙΑ ΤΟΥ SPAM

Αξίζει να σημειωθεί ότι η προέλευση του όρου «spam» είναι αρκετά ενδιαφέρουσα. Το Spam αποτελούσε το κύριο φαγητό του Βρετανικού στρατού κατά το Β' Παγκόσμιο πόλεμο. Ήταν δηλαδή μια κονσέρβα κρέατος και η ονομασία αυτή προήλθε από τον συνδυασμό των λέξεων «spiced» που σημαίνει πικάντικος και «ham» που σημαίνει ζαμπόν.

Μέσω ενός σατιρικού σκετς δυο Βρετανοί κωμικοί οι «Monthy Python's» παρουσίασαν ένα ζευγάρι να προσπαθεί να παραγγείλει ώστε να διαπιστώσει στο τέλος πως όλο το μενού του καταστήματος περιέχει «spam» δηλαδή κονσέρβα από συσκευασμένο κρέας που πρόσφερε η εταιρία Horned Foods.

Εντούτοις μέσω αυτού του σκετς η λέξη «Spam» ακούστηκε τουλάχιστον 94 φορές ενώ παράλληλα ακουγόταν το παίξιμο ενός τραγουδιού από μια παρέα Βίκινγκς τρώγοντας το αγαπημένο τους φαγητό δηλαδή το Spam (Roger, 2000).

Με την επέλαση του κορεσμού στην εποχή μας για το φαινόμενο του spam υιοθετήθηκε και καθιερώθηκε ως ορισμός για να δηλώνει την προσβολή και τον αρνητισμό των χρηστών λόγω των ανεπιθύμητων μηνυμάτων που έχουν δεχθεί στο ηλεκτρονικό τους ταχυδρομείο

(*http://download.beta.mcafee.com/webhelp/4/1032/GUID-E4DC6AC2-2C3B-4ABE-8BCA-D9DC6ADF4EEF.html*).

Αυτό είχε ως αποτέλεσμα την έντονη αντίδραση της εταιρίας Horned Foods καθώς η ιδία εισήγαγε την κονσέρβα spam το 1937 στην αγορά. Όσες προσπάθειες έκανε η εταιρία απέβησαν άκαρπες ώστε να σταματήσει η χρήση του όρου «spam» και αποφάσισε να κάνει συμβιβασμό στη διάκριση μεταξύ του «spam» με μικρούς

χαρακτήρες που χαρακτηρίζει την ανεπιθύμητη αλληλογραφία και του «SPAM» με κεφαλαίους χαρακτήρες που αναφέρεται στο προϊόν της συγκεκριμένης εταιρίας.

Ας σημειωθεί ακόμη ότι η έννοια του «spam» εμφανίστηκε το 1978 αλλά καθιερώθηκε πολύ αργότερα το 1994 όπου παρατηρηθήκαν οι πρώτες προσβάσεις των χρηστών στην ανεπιθύμητη αλληλογραφία με στόχο το οικονομικό κέρδος (commercial spam)

(http://www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam).

Η εταιρία DEC, που σήμερα αποτελεί κομμάτι της Hewlett-Packard, το 1978 εποχή που βρισκόταν σε λειτουργία το APRANET, για να παρουσιάσει τον νέο της μοντέλο ηλεκτρονικού υπολογιστή απέστειλε προσκλήσεις σε όλες τις ηλεκτρονικές διευθύνσεις της δυτικής ακτής των Ηνωμένων Πολιτειών της Αμερικής. Αύτη η τακτική κρίθηκε να παραβιάζει του κανόνες χρήσης του APRANET και απ ευθείας έγινε αποστολή σε όλους τους χρηστές μέσω των ηλεκτρονικών διευθύνσεων να τους επισημάνει ότι πρέπει να σέβονται το διαδίκτυο και τους χρηστές του (Roger, 2000).

4.3 ΒΑΣΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ SPAM

Μέσω συγκεκριμένων γνωρισμάτων καθίστανται εμφανή τα μηνύματα spam, τα οποία σχετίζονται με το περιεχόμενο αυτών των μηνυμάτων και την κεφαλίδα τους. Ιδιαίτερα σημαντικό θεωρείται ότι αρκετές φορές το περιεχόμενο αυτών των μηνυμάτων είναι διαφημιστικού χαρακτήρα που έχει για την προώθηση προϊόντων ή υπηρεσιών από επιχειρήσεις ενώ παρατηρείται συχνά το φαινόμενο οι χρηστές να μην δείχνουν ενδιαφέρον για το συγκεκριμένο μήνυμα και να το αγνοούν. Είναι γεγονός ότι τα περισσότερα μηνύματα αποδίδουν σε διαφόρους συνδέσμους(links) για τους παραλήπτες έτσι ώστε : α) να αναφέρουν την δυσαρέσκεια τους στην αποδοχή τέτοιων μηνυμάτων στην ηλεκτρονική τους διεύθυνση β) περιέχουν πληροφορίες σχετικές με το προϊόν ή την υπηρεσία που διαφημίζεται.

Από την άλλη μεριά, αυτό έχεις ως αποτέλεσμα στο μέλλον την αποστολή περισσότερων e-mail spam καθώς μια απάντηση απ το παραλήπτη ή επιλογή παρομοίου συνδέσμου πρακτικά σημαίνει και την ενεργή ηλεκτρονική του διεύθυνση.

Έπειτα η κεφαλίδα των e-mail spam, δηλαδή ο τομέας που δίνει τις ενημερώσεις σχετικά με το θέμα, τον αποστολέα ,τον χρήστη, κάποιες φορές φαίνεται ότι η ηλεκτρονική διεύθυνση είναι ανακριβής ή ότι χρησιμοποιείται μόνο για να αποστέλλει e-mail spam στους παραλήπτες της .

Χαρακτηριστικό παράδειγμα αποτελούν οι spammers οι όποιοι για να παρακινήσουν το χρηστή χρησιμοποιούν φράσεις που θα αναφέρονται σε κέρδη, προτάσεις γνωριμίας, δωρεάν πορνογραφικό υλικό κ.α. Επιπλέον για να πειστούν οι παραλήπτες για την απάντηση σε κάποιο e-mail που είχαν στείλει συνήθως εμφανίζεται στη γραμμή του θέματος η λέξη «Re:».Εκφράσεις που αναφέρονται συχνά ως περιεχόμενο είναι «Επείγουσα Ανακοίνωση», «Ακύρωση συνάντησης », «Έκτακτη Ειδοποίηση» κ.λπ. Συμπερασματικά, λόγω του μεγάλου όγκου παραληπτών που υπάρχει για την αποστολή τέτοιου είδους μηνυμάτων, οι spammers βασίζονται κατά κύριο λόγο στην αφέλεια ορισμένων χρηστών (Roger, 2000)..

(http://download.beta.mcafee.com/webhelp/4/1032/GUID-E4DC6AC2-2C3B-4ABE-8BCA-D9DC6ADF4EEF.html)

4.4 ΕΙΔΗ SPAM

Συγχρόνως η έννοια του spam δεν εμπεριέχει μόνο μηνύματα που αφορούν διαφημίσεις προϊόντων ή υπηρεσιών αλλά και μηνύματα κοινωνικού, πολιτικού ,θρησκευτικού και ιδεολογικού χαρακτήρα. Έπειτα, αναλύονται εκτενέστερα τα βασικότερα είδη των μηνυμάτων spam.

4.4.1 ΑΛΥΣΙΔΩΤΑ E-MAIL

Για να γίνει πιο σαφές, ένα από τα πιο χαρακτηριστικά είδη spam είναι τα **αλυσιδωτά e-mail**, γνωστά και ως **hoaxes,** με απώτερο σκοπό την παραπλάνηση του παραλήπτη. Συνεπώς τα μηνύματα αυτά μπορεί να περιέχουν μηνύματα που προειδοποιούν τους χρήστες για κάποιο κακόβουλο ιό, έκκληση βοήθειας για ένα

πρόβλημα που αντιμετωπίζει η κοινωνία είτε μπορεί να είναι μήνυμα που να αφορά προτάσεις φορολόγησης δεδομένων μέσω διαδικτύου.

Η αποστολή αυτών των μηνυμάτων έχει ως στόχο την παραπλάνηση του χρήστη συστήνοντας του κάθε φορά κάτι διαφορετικό όπως ένα χρηματικό έπαθλο ή υποσχόμενα κέρδη ώστε να μηνύματα αυτά να φτάσουν σε ένα μεγάλο όγκο ατόμων.

Ο όρος hoax χρησιμοποιείται για να περιγράψει κάτι ψεύτικο ή μια απάτη. Πιο εμπεριστατωμένος θεωρείται ο όρος Urban Legend(Αστικός Θρύλος) εφόσον ένα Hoax είναι μια φήμη δηλαδή ένας θρύλος που περιπλανιέται στο Διαδίκτυο. Πάραυτα υπάρχουν ποικίλοι τρόποι ώστε ο παραλήπτης να αντιληφθεί αν το μήνυμα που έλαβε είναι αληθές ή αποτελεί θρύλο του διαδικτύου. Οι τρόποι αναγνώρισης είναι:

- **Τεχνική Διάλεκτος**: Μέσω επιστημονικών ή τεχνικών όρων οι όποιοι μπορεί να φαίνονται επίσημοι αλλά να μην έχουν καμία απολύτως σημασία ώστε να φαίνεται η αξιοπιστία των μηνυμάτων.
- **Επίκληση μιας αξιόπιστης πηγής**: Τα hoaxes μέσω των μηνυμάτων που στέλνουν και για αυξήσουν την αξιοπιστία τους δηλώνουν ότι τα μηνύματα αυτά στέλνονται από μεγάλους οργανισμούς όπως είναι η Microsoft. Λόγω παραποίησης του e-mail οι μεγάλοι οργανισμοί αποφεύγουν τέτοιου είδους κινήσεις και οι ανακοινώσεις τους γίνονται πάντα στον Τύπο.
- **Προτροπή προώθησης του ίδιου μηνύματος σε τρίτους:** Όταν ζητείται η προώθηση ενός μηνύματος πρόκειται σίγουρα για μήνυμα hoax. Αυτό φυσικά είναι και το αναγνωριστικό των Αστικών Θρύλων.
- **Αδυναμία Ελέγχου:** Μέσω της ιστοσελίδας του ο αποστολέας που έχει δημιουργήσει και παρέχοντας πληροφορίες καθιστά το περιεχόμενο του μηνύματος αρκετά σημαντικό. Το μήνυμα θεωρείται γενικά ύποπτο όταν δεν αναφέρεται στο e-mail ή η διεύθυνση δεν είναι πραγματική .

Εκτός όμως από τις παραπάνω τεχνικές αναγνώρισης των hoaxes που αναφέρθηκαν είναι επίσης ο εκφοβισμός ,ο αναλφαβητισμός ,η ορθογραφία (κεφάλαια γράμματα σύμβολα κ.α.) και η χρήση συγκεκαλυμμένων απειλών

(*http://www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam*).

4.4.2 ΜΗΝΥΜΑΤΑ ΜΕ ΣΚΟΠΟ ΤΟ PHISHING

Επιπροσθέτως, ένα είδος ανεπιθύμητου e-mail που παρουσιάζεται όλο και πιο δυναμικά είναι το «phishing»(ηλεκτρονικό ψάρεμα).Πρόκειται δηλαδή για ένα μήνυμα που στέλνεται σε όσο τον δυνατόν περισσότερους παραλήπτες και παρουσιάζεται ότι προέρχεται από μεγάλους οργανισμούς, ηλεκτρονικά καταστήματα ακόμα και τράπεζες. Το μήνυμα αυτό ζητά από τον χρήστη να αποκαλύψει ή να επικυρώσει τα προσωπικά του στοιχεία όπως για παράδειγμα ημερομηνία γέννησης, στοιχεία λογαριασμού, αριθμούς και PIN πιστωτικών ή χρεωστικών καρτών. Το phishing θα αναλυθεί διεξοδικά στο επόμενο κεφάλαιο.

4.4.3 ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΙΤΗΣΕΙΣ

Οι διαδικτυακές αιτήσεις αποστέλλονται με σκοπό την προώθηση τους και σε άλλους αποδέκτες διατηρώντας τις ίδιες ηλεκτρονικές τους διευθύνσεις. Έπειτα, οι αιτήσεις αυτές στέλνονται στο αποστολέα αφού πρώτα έχουν συμπληρωθεί από τελευταίο αποδεκτή. Έτσι λοιπόν οι spammers με ένα και μόνο μήνυμα επιβεβαιώνουν όλες τις ηλεκτρονικές διευθύνσεις που έχουν στις όποιες μετά μπορούν να στείλουν καινούργια ανεπιθύμητα μηνύματα.

(*http://download.beta.mcafee.com/webhelp/4/1032/GUID-E4DC6AC2-2C3B-4ABE-8BCA-D9DC6ADF4EEF.html*)

4.5 ΤΕΧΝΙΚΕΣ ΠΟΥ ΟΔΗΓΟΥΝ ΣΤΟ SPAM

Αξίζει να σημειωθεί ότι για την αποφυγή νομικών συνεπειών οι αποστολείς τέτοιου είδους μηνυμάτων στέλνουν τα μηνύματα τους από ενδιάμεσα συστήματα ηλεκτρονικών υπολογιστών χωρίς βέβαια να έχουν επίγνωση οι παραλήπτες του. Για να μπορέσουν να εισέλθουν σε αυτά τα συστήματα εφαρμόζουν τις εξής τεχνικές:

- Hacking: Με βάση τις τεχνολογικές γνώσεις τους για τα λειτουργικά περιβάλλοντα, οι spammers για την αποστολή e-mail spam και χρησιμοποιώντας όλους του διαθέσιμους πόρους εισβάλουν βαθύτερα στο υπολογιστικό σύστημα σαν να ήταν οι νόμιμοι χρήστες.
- IP Spoofing: είναι μια μέθοδος μες από την οποία εμφανίζονται TCP/IP πακέτα τα οποία χρησιμοποιούνται από άλλη IP διεύθυνση αποστολέα και την πραγματική. Εντούτοις οι routers δίνουν ιδιαίτερη προσοχή μόνο την IP διεύθυνση «προορισμού» και όχι την IP διεύθυνση «προέλευσης». Αφού αποκωδικοποιηθεί η διεύθυνση «προέλευσης» και γίνει η παρουσίασης της στο τελικό προορισμό της ώστε αν ζητηθεί η απάντηση να είναι γνωστή η διεύθυνση του spammer
- Packet sniffing: αυτή η μέθοδος εστιάζει στην παρακολούθηση των πακέτων πληροφορίας που βρίσκονται σε ένα δίκτυο. Στα μη κωδικοποιημένα πακέτα εγγυται ο κίνδυνος αποκάλυψης προσωπικών δεδομένων ή πληροφοριών των χρηστών όπως για παράδειγμα passwords, e-mails. Για να αντιμετωπιστεί αυτό το θέμα βρέθηκε σαν λύση η κωδικοποίηση των πληροφοριών
- Phishing: αναφέρεται σε μια τεχνική κατά την οποία εγκαινιάζεται ένας παράνομος δικτυακός τόπος που λειτουργεί όμως σαν νόμιμος. Όταν λοιπόν οι χρηστές επισκεφτούν αυτόν τον παράνομο ιστότοπο δίνουν τα προσωπικά τους δεδομένα όπως στοιχεία χρεωστικών καρτών κ.α. κάνοντας συναλλαγές θεωρώντας τον ως πραγματικό.
- Harassment (Παρενόχληση): σχετίζεται με την αποστολή υβριστικών, επιθετικών ηλεκτρονικών μηνυμάτων σε άτομα ή σε ομάδες χρηστών.
- Spam filtering: είναι ένα λογισμικό φιλτραρίσματος μηνυμάτων spam που χρησιμοποιείται για την λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails).

Συνεπώς, οι αποστολείς τέτοιου είδους μηνυμάτων εισάγουν κι άλλες μεθόδους τόσο για την συλλογή ηλεκτρονικών διευθύνσεων όσο και για την αποστολή κακόβουλου περιεχομένου. Έτσι για την συλλογή των ηλεκτρονικών διευθύνσεων χρησιμοποιούνται οι εξής μέθοδοι:

- **Από μηνύματα που στέλνεται σε news group (Usenet)**

Μέσω ειδικών προγραμμάτων , οι spammers ανιχνεύουν σε ποικίλους ισότοπους όσο το δυνατόν περισσότερες ηλεκτρονικές διευθύνσεις. Υπάρχουν προγράμματα που ψάχνουν τις ηλεκτρονικές διευθύνσεις στην κεφαλίδα του e-mail και εμφανίζονται με τις φράσεις '**From:**' ή '**Reply to**' ωστόσο υπάρχουν άλλα προγράμματα που ανιχνεύουν τη χρήση υπογράφων ή όταν εμπεριέχεται το «@» στο κύριο μέρος των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.

- **Από λίστες με ηλεκτρονικές διευθύνσεις**

Επειδή, οι spammers γνωρίζουν την εγκυρότητα των διευθύνσεων εφόσον η συλλογή αυτών πραγματοποιείται μέσα από λίστες διευθύνσεων πολλών συνδρομητών. Η πιο συνηθέστερη τεχνική που εφαρμόζουν οι spammers είναι να ζητήσουν από κάποιο εξυπηρετητή να τους παραδώσει την λίστα με τις διευθύνσεις τους (η τεχνική αύτη υιοθετείται συχνά από ορισμένους εξυπηρετητές για την διευκόλυνση των νόμιμών χρηστών) ώστε να σταλθούν μηνύματα spam στα συγκεκριμένα e-mails. *

(http://download.beta.mcafee.com/webhelp/4/1032/GUID-E4DC6AC2-2C3B-4ABE-8BCA-D9DC6ADF4EEF.html)

4.6 ΠΑΡΑΛΛΑΓΕΣ ΤΟΥ SPAM

Αρχικά το spim είναι μια παραλλαγή του spam. Χαρακτηρίζεται ως **«αυτόκλητο διαφημιστικό μήνυμα»** καθώς εμφανίζεται μέσω ενός συστήματος παραγωγής στιγμιαίων μηνυμάτων. Η προέλευση της ονομασίας αυτή πρόεκυψε απ τα αρχικά γράμματα των **S**pam **I**nstant **M**essage. Η τάση των διαφημιστών για την προσέγγιση όλο και μεγαλύτερου αριθμού καταναλωτών μέσω οποιοδήποτε μέσων τους οδήγησε στην υιοθέτηση του spim. Μέσω των προγραμμάτων «bots» γίνεται η παράγωγη των

spim. Όταν οι χρήστες «σερφάρουν» στο Διαδίκτυο, γίνεται μεταφορά από τους διακομιστές (servers) που έχουν τις ιστοσελίδες , τμήματα του λογισμικού που παράγει τα spim στους υπολογιστές τους σε σκόπιμη μορφή όπως γραφικά ήχο κτλ. Σε συγκεκριμένο παράθυρο οθόνης. Το περιεχόμενο των μηνυμάτων αυτών είναι παρεμφερή με εκείνο της ιστοσελίδας που τα εισήγαγε ,καθώς η διαφημιστές θεωρούν ότι η πλοήγηση σε μια τέτοια σελίδα φανερώνει το ενδιαφέρον για τα ίδια θέματα που δημιουργούνται σε αυτή.

Το **link spamming** είναι μια παραλλαγή του spam που εμφανίζεται σε web sites που λειτουργούν ως Forum και καταγράφουν on-line συζητήσεις των χρηστών και αυτή η μορφή δεν χαρακτηρίζεται για την αποστολή ομαδικών μηνυμάτων. Επίσης το spam έχει αντιγραφεί και εφαρμόζεται από όλες τις εταιρίες **κινητής τηλεφωνίας**. Για πολλούς παραλήπτες η διαπίστωση αυτή επέρχεται με την αποστολή μηνύματος (SMS,MMS) ή ηλεκτρονικά , το όποιο φυσικά θα διαφημίζει ένα προϊόν ή υπηρεσία. Μηνύματα τέτοιας μορφής αποστέλλονται από χώρες που η τιμή χρέωση τους είναι χαμηλότερη π.χ. χώρες της Ευρώπης. Από την άλλη μεριά, πολλοί επιτήδειοι με τη χρήση των μηνυμάτων MMS στέλνουν φωτογραφικό υλικό ή ακόμα και βίντεο ώστε να διαφημιστούν όσο τον δυνατόν περισσότερο. Τα MMS μηνύματα παραπέμπουν πολλές φορές μέσω διασυνδέσεων και σε ιστοσελίδες ώστε να δει καλύτερα ο πελάτης το προϊόν που διαφημίζεται.

Ταυτόχρονα, κυριαρχεί και μια άλλη μορφή γνωστή και ως **scam.** Αναφέρεται, δηλαδή γραπτά μηνύματα ή εξερχόμενες κλήσεις στο κινητό του παραλήπτη με απώτερο σκοπό την υψηλή τιμολόγηση. Συνεπώς, είναι προσπάθειες δημιουργίας παράνομου κέρδους που προκλήθηκαν μέσω των κλήσεων ή των μηνυμάτων απ τον αποστολέα με σκοπό την παραπλάνηση του παραλήπτη και οι οποίες μπορεί να μην αφορούν κάποια διαφημιστική καμπάνια. Στη συνέχεια, ο χρήστης δέχεται κλήσεις στο κινητό του χωρίς να προλάβει να απαντήσει. Έτσι όταν ο χρήστης καλέσει τον συγκεκριμένο αριθμό γίνεται αυτόματη χρέωση χωρίς βέβαια ο ίδιος να το γνωρίζει καθώς όσο περισσότερα λεπτά είναι κλήση τόσο πιο αυξημένη είναι η χρέωση.
Αξίζει να σημειωθεί ότι, στην περίπτωση που ο χρήστης λάβει ένα μήνυμα στο κινητό του και το περιεχόμενο αφορά μια πρόσκληση ώστε να δώσει τον αριθμό που βρίσκεται σε αυτό. Ορισμένες φορές ο παραλήπτης δέχεται υψηλές χρεώσεις όταν προτίθενται να απαντήσει μέσω των μηνυμάτων αυτών. Τέλος, ο παραλήπτης

καλείται να απαντήσει αν θέλει ή όχι να δέχεται παρόμοια μηνύματα τα όποια έχουν ως στόχο την υψηλή χρέωση.

ΚΕΦΑΛΑΙΟ 5
ΑΠΕΙΛΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

5.1 SPOOFING

Οι κατηγορίες στις οποίες διακρίνεται το spoofing είναι οι εξής:

- IP spoofing
- ARP spoofing
- DNS spoofing
- SMTP spoofing

Η έννοια του spoofing αποτελεί μια διαδικασία η οποία σχετίζεται με τη διεύθυνση IP. Αυτό σημαίνει ότι ο αποστολέας στέλνει ένα μήνυμα σε έναν παραλήπτη χρησιμοποιώντας μια διεύθυνση IP ενός άλλου αξιόπιστου χρήστη. Με αυτό τον τρόπο δεν φαίνεται ο πραγματικός αποστολέας αλλά ένας έγκυρος χρήστης. Αυτό έχει σαν αποτέλεσμα την εξαπάτηση των χρηστών και έτσι να πραγματοποιούνται «επιθέσεις» στα συστήματα των χρηστών. Μία από τις πιο συχνές επιθέσεις είναι αυτή της «άρνησης υπηρεσιών» ή «DoS – Denial of Service» οι οποίες έχουν σαν στόχο να προκαλέσουν δυσλειτουργία στους ηλεκτρονικούς υπολογιστές των χρηστών μέσω της μαζικής αποστολής πολλών πακέτων (Δουκίδης, 2001).

Στη συνέχεια θα αναλυθούν οι κατηγορίες στις οποίες διακρίνεται το SPOOFING (https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-)

5.1.1. IP SPOOFING

Ο όρος IP SPOOFING αφορά τη διαδικασία κατά την οποία ο αποστολέας δημιουργεί πακέτα IP τα οποία δεν έχουν αληθινή διεύθυνση με αποτέλεσμα ο παραλήπτης να νομίζει ότι το μήνυμα έχει προέλθει από έναν αξιόπιστο υπολογιστή. Για να πραγματοποιηθεί αυτό χρειάζεται η εξής διαδικασία:

Αρχικά θα πρέπει να αναφερθεί ότι όταν δυο υπολογιστές συνδέονται μεταξύ τους και χρησιμοποιούν το πρωτόκολλο TCP/IP γίνεται το εξής: για την αποστολή ενός πακέτου TCP από τον έναν υπολογιστή στον άλλο χρησσιμοποιούνται οι αριθμοί ακολουθίας οι οποίοι αποτελούν ακέραιους αριθμούς που στην ουσία επιβεβαιώνουν και πιστοποιούν τη λήψη πακέτων.

Ο αποστολέας που θέλει να πραγματοποιήσει τη διαδικασία του IP SPOOFING θα πρέπει να είναι σε θέση να γνωρίζει τους ακέραιους αριθμούς που των άλλων δύο υπολογιστών δηλαδή τους αριθμούς ακολουθιών.

Επίσης, για να πραγματοποιηθεί η διαδικασία του IP spoofing θα πρέπει:

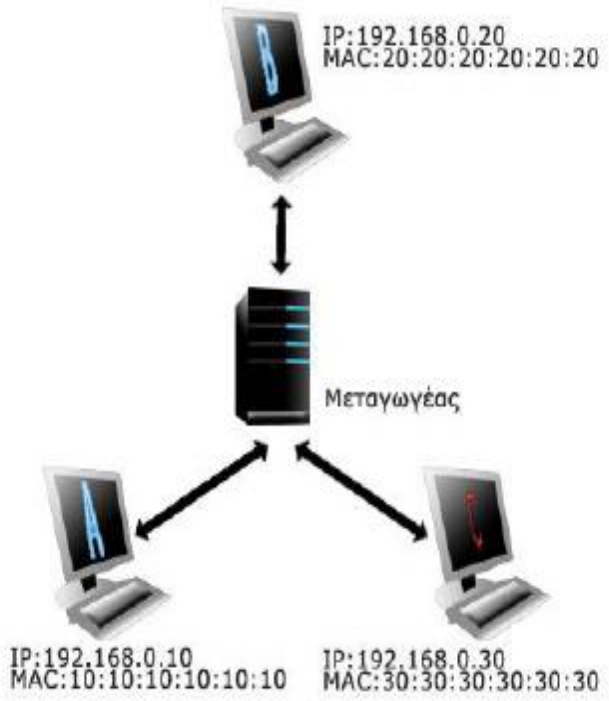
- Ο υπολογιστής στον οποίο θα εισβάλλει ο αποστολέας και θα χρησιμοποιήσει τη διεύθυνση του θα πρέπει να είναι εκτός λειτουργίας. Για να επιτευχθεί αυτό θα πρέπει να πραγματοποιήσει ο εισβολέας επιθέσεις άρνησης υπηρεσιών (DoS – Denial of Service).
- Ο εισβολέας μέσω του υπολογιστή του θα πρέπει να χρησιμοποιήσει την διεύθυνση του πραγματικού υπολογιστή και να συνδεθεί με τον διακομιστή.
- Τέλος, θα πρέπει ο αποστολέας που έχει εισβάλλει σε άλλο υπολογιστή να ανακαλύψει τον αριθμό ακολουθίας του διακομιστή.

(https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-)

5.1.2. ARP SPOOFING (ADDRESS RESOLUTION PROTOCOL)

Για τη σύνδεση των πραγματικών διευθύνσεων των υπολογιστών με τις IP διευθύνσεις χρησιμοποιείται το ARP το οποίο αποτελεί μέρος του πρωτοκόλλου

TCP-IP. Για να επιτευχθεί το ARP spoofing θα πρέπει να υπάρξει αλλαγή στην ARP cache στην οποία συλλέγονται και αποθηκεύονται όλα τα στοιχεία εκείνα που χρειάζονται για να αλλάξουν οι φυσικές διευθύνσεις σε IP διευθύνσεις. Η αλλαγή αυτή θα πρέπει να πραγματοποιηθεί ώστε να υπάρχει ισοδυναμία ανάμεσα στη πραγματική διεύθυνση του υπολογιστή που εισβάλλει και στην IP διεύθυνση του υπολογιστή που ο διακομιστής εμπιστεύεται στην πραγματικότητα. Βασική προϋπόθεση για την επίτευξη μιας τέτοιας επίθεσης όμως είναι ο εισβολέας (Cracker) να είναι συνδεδεμένος στο ίδιο δίκτυο με αυτόν που θέλει να εισβάλλει και να εξαπατήσει.



Στη συνέχεια θα ακολουθήσει ένα παράδειγμα στο οποίο πραγματοποιείται εξαπάτηση σε δύο χρήστες όπως φαίνεται και στην παραπάνω εικόνα. Πιο συγκεκριμένα:

Ο εισβολέας (Cracker C) θέλει να εισβάλλει και να εξαπατήσει τους χρήστες Α και Β. Για να γίνει αυτό θα πρέπει ο εισβολέας να στείλει πακέτα ARP στον χρήστη Α με διεύθυνση πρωτοκόλλου 192.168.0.20 και διεύθυνση MAC 30:30:30:30:30:30. Ομοίως ο εισβολέας ακολουθεί την ίδια διαδικασία για να εξαπατήσει τον χρήστη Β.

Με αυτό τον τρόπο θα χρησιμοποιείται η διεύθυνση MAC του εισβολέα όταν οι χρήστες Α και Β θα ξεκινήσουν να αποστέλλουν μεταξύ τους αρχεία. Ωστόσο για να μην καταλάβουν οι χρήστες ότι παρακολουθούνται θα πρέπει ο εισβολέας να προωθεί τα αρχεία που δεν απευθύνονται σε αυτόν στους πραγματικούς παραλήπτες.

5.2 PHISHING

Το «phishing» αποτελεί μια ενέργεια κατά την οποία οι χρήστες εξαπατούνται με σκοπό την απόκτηση των προσωπικών τους δεδομένων. Η λέξη phishing προέρχεται από την αγγλική λέξη Fishing η οποία σημαίνει ψάρεμα. Σύμφωνα με αυτό θα μπορούσε να αναφερθεί ότι η ενέργεια phishing στα ελληνικά είναι το «ψάρεμα μέσω διαδικτύου».

Το phishing πραγματοποιείται με τον εξής τρόπο: Αρχικά αποστέλλεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε ένα χρήστη το οποίο φαίνεται ότι προέρχεται από κάποια μεγάλη διάσημη εταιρεία ή οργανισμό όπως είναι μια τράπεζα χωρίς όμως να είναι. Σκοπός της συγκεκριμένης ενέργειας είναι να παροτρύνει τους χρήστες να εισάγουν τα προσωπικά τους δεδομένα (αριθμός κάρτας, κωδικός κλπ) ώστε οι εισβολείς να τα υποκλέψουν και να πραγματοποιήσουν συναλλαγές με τα στοιχεία των νόμιμων χρηστών.

Οι τρόποι με τους οποίους μπορεί να πραγματοποιηθεί αυτού του είδους η εξαπάτηση των χρηστών είναι:

- Μέσω μηνύματος ηλεκτρονικού ταχυδρομείου από μια υποτιθέμενη τράπεζα στο οποίο μήνυμα θα πρέπει να εισαχθούν τα προσωπικά δεδομένα των χρηστών.
- Μέσω μηνύματος ηλεκτρονικού ταχυδρομείου από την τράπεζα που χρησιμοποιεί ο χρήστης και στο οποίο θα ζητείται από τον χρήστη να εισάγει τα προσωπικά του στοιχεία λόγω ενός υποτιθέμενου προβλήματος που παρουσιάστηκε στο λογαριασμό του χρήστη.
- Μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου στο οποίο θα αναφέρεται ότι ο χρήστης έχει κερδίσει κάποιο δώρο και θα πρέπει να εισαχθούν τα προσωπικά του δεδομένα για να το παραλάβει.
- Άλλος ένας τρόπος είναι μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στο οποίο θα φαίνεται ότι είναι η διάσημη εταιρεία eBay χωρίς να είναι και στο

οποίο μήνυμα θα αναφέρεται ότι για τη συμμετοχή του χρήστη σε μια προσφορά θα πρέπει να εισαχθούν τα προσωπικά του δεδομένα.

Ανάμεσα στους προαναφερθέντες τρόπους, στους πιο αποτελεσματικούς για την εξαπάτηση των χρηστών συγκαταλέγεται ο τρίτος τρόπος που αφορά το δώρο από μια εταιρεία και ο χρήστης για να μην το χάσει εισάγει γρήγορα τα προσωπικά του δεδομένα. Όσον αφορά τον πρώτο τρόπο με την τράπεζα και το πρόβλημα που παρουσιάζεται ο χρήστης τις περισσότερες φορές θα επικοινωνήσει με την τράπεζα για περισσότερες πληροφορίες οπότε θα αποφύγει την εξαπάτηση. Ωστόσο, οι εισβολείς συνήθως χρησιμοποιούν διάφορες τακτικές για να εξαπατήσουν το χρήστη και να εισάγει τα προσωπικά του στοιχεία.

Τα τελευταία χρόνια πραγματοποιούνται διάφορες έρευνες η οποίες σχετίζονται με το phishing. Σύμφωνα με την εταιρεία Anti-Phishing Working Group (APWG) και τα στατιστικά στοιχεία που έφερε στη δημοσιότητα μέσα από έρευνα που έχει πραγματοποιήσει για το fishing παρατηρείται μια αύξηση των επιθέσεων ιδιαίτερα τη χρονολογία 2009 ενώ τον επόμενο χρόνο φαίνεται ότι υπάρχει μια μείωση. Το ποσοστό των ιστοσελίδων που δέχτηκαν επίθεση φαίνεται ότι παρουσιάζει μια μικρή μείωση το 2011 ενώ το ποσοστό των εταιρειών που εξαπατήθηκαν αυξάνεται κάθε χρόνο.

Στη συνέχεια, αξίζει να αναφερθεί μια έρευνα που πραγματοποιήθηκε σε παγκόσμιο επίπεδο και είναι γνωστή με την ονομασία Global Corporate IT Security Risks το 2013 με πρωτοβουλία των εταιρειών B2B International και Kaspersky Lab. Στη συγκεκριμένη έρευνα συμμετείχαν και στελέχη του IT από την Ελλάδα από τους οποίους ένα ποσοστό του 69% δήλωσε ότι οι εταιρείες τους είχαν δεχτεί επίθεση εξαπάτησης. Ο μέσος όρος σε παγκόσμιο επίπεδο παρουσιάζει αύξηση το 2013 με το ποσοστό αυτό να ανέρχεται στο 66% σε σχέση με το 2012 όπου το ποσοστό αυτό ανερχόταν στο 58%. http://www.antiphishing.org/

Στη συνέχεια, σε παγκόσμιο επίπεδο το ποσοστό των εταιρειών που εξαπατήθηκαν και διέρρευσαν προσωπικά δεδομένα ανέρχεται στο 22% ενώ παράλληλα στην Ελλάδα το ποσοστό αυτό ανέρχεται στο 21%. Σύμφωνα με την ίδια έρευνα, παρατηρείται ότι οι εταιρείες που δέχονται τις περισσότερες επιθέσεις τέτοιου είδους είναι μικρού ή μεσαίου μεγέθους με το ποσοστό αυτό να ανέρχεται στο 23% ενώ οι μεγαλύτερου μεγέθους επιχειρήσεις δέχονται λιγότερες επιθέσεις με το ποσοστό αυτό να ανέρχεται στο 17%. Τέλος, η ίδια έρευνα αναφέρει ότι το ποσοστό των προσωπικών στοιχείων που διέρρευσαν από επιχειρήσεις μεγάλου

μεγέθους κατόπιν επιθέσεων phishing ανέρχεται στο 6% ενώ το ποσοστό για τις επιχειρήσεις μικρού ή μεσαίου μεγέθους ανέρχεται στο 5%.
http://www.antiphishing.org/

Οι εισβολείς χρησιμοποιούν διάφορες τακτικές προκειμένου να εξαπατήσουν τους χρήστες. Μια από τις τακτικές αυτές είναι να αντιγράφουν πιστά τα web sites τα οποία θέλουν να εξαπατήσουν. Χαρακτηριστικό παράδειγμα σε αυτό είναι η εισβολή που πραγματοποίησαν οι crackers στην εταιρεία eBay δημιουργώντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο οποίο αναφερόντουσαν χριστουγεννιάτικες προσφορές τις οποίες δεν έπρεπε να χάσουν οι χρήστες και θα έπρεπε να εισάγουν τα προσωπικά τους δεδομένα. Αξίζει να αναφερθεί η εμπειρία ενός από τους χρήστες ο οποίος έλαβε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από την εταιρεία eBay το οποίο είχε θέμα «Christmas is Coming on ebay.co.uk». Το ηλεκτρονικό μήνυμα αναφερόταν σε διάφορες προσφορές και παρέπεμπε στο site ebaychristmas.net. Μόλις ο χρήστης μπήκε στο site έπρεπε να εισάγει τα προσωπικά του στοιχεία κάτι το οποίο φάνηκε ιδιαίτερα ύποπτο. Ο χρήστης απέστειλε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στην εταιρεία γι αυτό και η οποία απάντησε ότι δεν ισχύει κάτι τέτοιο. Κατόπιν ο χρήστης θεωρώντας ότι κάτι τέτοιο είναι απάτη έστειλε εκ νέου email όπου ήλθε απάντηση από την εταιρεία ότι όντως πρόκειται για απάτη. Το γεγονός ότι η συγκεκριμένη εταιρεία παρουσιάζει αδυναμία και δεν μπορεί να αντιληφθεί τέτοιου είδους επιθέσεις (phising) δείχνει πόσο έχουν εξελιχθεί οι εισβολείς και χρησιμοποιούν τακτικές εξαπατώντας τις εταιρείες και κατ επέκταση τους ίδιους τους χρήστες. (http://richi.co.uk/blog/2005/12/ebays-anti-phishing-desk-sucks.html)

Οι εισβολείς εξελίσσοντας τις πρακτικές εξαπάτησης των χρηστών και των εταιρειών αντιγράφουν τον κώδικα της σελίδας της εταιρείας και έτσι δημιουργούν ένα πιστό αντίγραφο.

Στην Ελλάδα, οι επιθέσεις αυτού του είδους υπάρχουν αλλά όχι σε τόσο μεγάλο βαθμό λόγω της δυσκολίας που παρουσιάζει η ελληνική γλώσσα. Ωστόσο όμως, έχουν συμβεί τέτοιου είδους επιθέσεις.

Ένα από τα παραδείγματα επιθέσεων phishing είναι το μήνυμα του ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι στάλθηκε από την City bank στους πελάτες της και όπως φαίνεται στην παρακάτω εικόνα εμπεριείχε το εξής μήνυμα:

Κλεισιματος των λογαριασμων και περιοριζοντας την προσβαση στο λογαριασμο Ο λογαριασμος σας εχει **Limited**. Εμεις που αναθεωρηθηκε προσφατα στοιχεια της πιστωτικης σας καρτας, και φαινεται οτι χρησιμοποιειτε την ιδια πιστωτικη καρτα για 2 λογαριασμους. Οπως μπορειτε να διαβασετε και μας **User Agreement** (τμημα 2.13) δημιουργια πολλαπλων λογαριασμων ειναι αυστηρα απαγορευμενη. Ειστε τωρα καλειται να παρασχει πληροφοριες σχετικα με το λογαριασμο σας. **CitiBank** θα διερευνησει το θεμα γρηγορα και αν η ερευνα ειναι υπερ σας, θα αποκαταστησει το λογαριασμο σας.

Καντε κλικ εδω για να επαναφερετε το λογαριασμο σας

Όπως μπορεί να παρατηρηθεί το συγκεκριμένο μήνυμα δεν είναι σωστά συνταγμένο πράγμα που σημαίνει ότι οι εισβολείς πιθανόν το μετέφρασαν στον αυτόματο μεταφραστή. Επίσης, αυτό το μήνυμα στάλθηκε και σε χρήστες οι οποίοι δεν ήταν πελάτες της συγκεκριμένης τράπεζας με σκοπό να εξαπατήσουν περισσότερους χρήστες.

Στην επόμενη εικόνα παρατηρείται άλλο ένα phising mail που έλαβε ένας χρήστης και το οποίο επίσης δεν είναι σωστά συνταγμένο και εμπεριέχει και ορθογραφικά λάθη.

Αγαπητε πελατη

Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.

Δωροεπιταγη code: 11245325932

για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου παραπανω.

Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.

Copyright © winbank 2008

Τέλος, άλλο ένα παράδειγμα επίθεσης phishing είναι ένα ηλεκτρονικό μήνυμα που στάλθηκε από την υποτιθέμενη Alpha bank και εμπεριείχε το εξής:

"Αγαπιτέ πελάτη της Ιντερνέτ-Τράπεζας!

Επειδή η κατάσταση με Online - Τράπεζες στη χώρα μας είναι σήμερα πολύ δύσκολη, η κυβέπνιση της Ελλάδας παρακάλησέ μας να κάνουμε τον έλεγχο για όλους τους Online - λογαριασμούς της δηκής ! μας τράπεζας να μάθουμε αν υπάρχουν "λογαριασμοί μιας μέρας", τους οποίους χρησημοποιούν οι εγκληματίες για να αποπλύνονται τα κλεμμένα λεφτά. Δια ταυτα σας παρακαλούμε πολύ &sigm! a;οβαρά να συμ& pi;ληρώσετε το ερωτηματολόγιο της επιβεβαιώσεις λόγαριασμού στη επίσημη μας Ιντερμετ-σελήδα.

Οι λογαριασμοί, που δε θα επιβεβαιοθούν ως της 27.11.05, θα παγώνονται για ακαθόριστο καιρό πριν γίνει φανερό πως ακριβώς έχουν δημιουργηθεί και εκμεταλευθεί. Ο έλεγχος αυτος είν&alph! a;ι επίκαιρος οχι μόνο για ιδιωτικούς μας πελάτες, αλλα για όλους σας.

ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Σας ζητούμε συγνώμη για τις ενοχλήσεις που προκύπται απο τη διαταγή της παρούσες εκδήλωσης και ελπίζουμε για την κατανόηση και την βοήθειά σας.

Με σεβασμό,

Υπηρεσία ασφάλειος

Τράπεζα Alpha Bank"

Όπως φαίνεται στην παραπάνω εικόνα στο σημείο που αναγράφεται «Να συμπληρώσω το ερωτηματολόγιο» κάνοντας κλικ οδηγείται ο χρήστης σε ένα λινκ στο οποίο συμπληρώνονται τα προσωπικά του δεδομένα. Χαρακτηριστικό του συγκεκριμένου μηνύματος όπως και στο προηγούμενο είναι η κακή σύνταξη και τα ορθογραφικά

λάθη(http://www.ibm.com/support/knowledgecenter/el/SSKTWP_8.5.3/com.ibm.notes85.client.doc/mail_junk_t.html).

5.2.1 ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΌ ΤΟ PHISHING

Οι τρόποι για να προστατευτούν οι χρήστες από τις επιθέσεις phishing είναι να ενημερώνονται συχνά σχετικά με τη μορφή των μηνυμάτων που λαμβάνουν στο ηλεκτρονικό τους ταχυδρομείο ή στα web sites που επισκέπτονται. Παράλληλα θα πρέπει να ελέγχουν το κάθε μήνυμα που λαμβάνουν και να μην ανατρέχουν απευθείας σε link χωρίς να διαβάζουν πρώτα όλο το μήνυμα για να παρατηρήσουν οτιδήποτε ύποπτο. Επίσης δεν θα πρέπει να εισάγουν τα προσωπικά τους δεδομένα σε web sites χωρίς να έχουν επιβεβαιώσει ότι έχουν προέλθει από τον πραγματικό αποστολέα και όχι από κάποιον εισβολέα. Αυτό μπορεί να επιβεβαιωθεί είτε στέλνοντας μήνυμα στην εταιρεία η οποία μπορεί να το έχει στείλει είτε επικοινωνώντας μαζί της.

Σε γενικές γραμμές δεν αποτελεί εύκολη υπόθεση η προστασία από τέτοιου είδους επιθέσεις καθώς οι εισβολείς δεν θέλουν να δημιουργήσουν πρόβλημα στο σύστημα του υπολογιστή πράγμα που σημαίνει ότι με ένα antivirus ο χρήστης προστατεύεται αλλά θέλουν να εισβάλλουν στα προσωπικά στοιχεία του χρήστη και να τους εξαπατήσουν. Μέσα από αυτό φαίνεται ότι ο ανθρώπινος παράγοντας αποτελεί τον πιο αδύναμο κρίκο στα συστήματα ασφαλείας

(*https://purnendukumar.wordpress.com/2011/12/12/fourth-generation-wireless-technology/***).**

Στη συνέχεια θα αναφερθούν περαιτέρω τρόποι προστασίας από τις επιθέσεις phishing. Ειδικότερα:

- Οι χρήστες θα πρέπει να είναι σίγουροι ότι τα προγράμματα ασφαλείας και λειτουργίας των συστημάτων τους διαθέτουν τις τελευταίες ενημερώσεις.
- Επίσης, στο ηλεκτρονικό ταχυδρομείο τους οι χρήστες θα πρέπει να έχουν προβεί στις ρυθμίσεις και να έχουν ρυθμίσει τα φίλτρα ώστε να φιλτράρονται τα μηνύματα εξαπάτησης πριν εμφανιστούν στο χρήστη.

- Η ενημέρωση αποτελεί τον βασικότερο παράγοντα προστασίας των συγκεκριμένων επιθέσεων καθώς οι εισβολείς επινοούν συνεχώς τρόπους ώστε να εξαπατήσουν τους χρήστες.
- Ο έλεγχος προέλευσης των μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί επίσης πολύ βασικό παράγοντα προστασίας τέτοιων επιθέσεων.
- Οι χρήστες θα πρέπει να είναι πάντα υποψιασμένοι για τα μηνύματα που λαμβάνουν.
- Οι χρήστες κάθε φορά που ανατρέχουν σε κάποια διεύθυνση μέσω ενός web site που έχουν επισκεφτεί θα πρέπει να ελέγχουν αν είναι ασφαλής. Αυτό μπορεί να πραγματοποιηθεί ελέγχοντας το https όπου το s είναι η λέξη secure και ελέγχοντας πάνω δεξιά στη διεύθυνση το «λουκέτο» το οποίο σημαίνει ότι η συγκεκριμένη διεύθυνση διαθέτει πιστοποιητικό.

5.3 DNS SPOOFING

Το DNS Spoofing αποτελεί άλλη μια κατηγορία Spoofing η οποία δεν χαρακτηρίζεται υψίστης σημαντικότητας καθώς δεν είναι δύσκολο να εντοπιστεί. Στο συγκεκριμένο είδος επίθεσης ο εισβολέας προσπαθεί να αλλάξει τα δεδομένα κάποιου DNS Server με σκοπό να αντιστοιχεί το συμβολικό όνομα κάποιου υπολογιστή που εμπιστεύονται οι χρήστες, στην IP διεύθυνση ενός υπολογιστή που χρησιμοποιείται από τον εισβολέα. Αυτό θα έχει σαν αποτέλεσμα όταν θα πιστεύουν οι χρήστες ότι συνδέονται σε έναν υπολογιστή αξιόπιστο θα συνδέονται στον υπολογιστή του εισβολέα (Comer, 2007).

5.3.1 SPOOFING ΜΕΣΩ SMTP

Το Simple Mail Transfer Protocol (SMTP) αποτελεί ένα πρωτόκολλο το οποίο χρησιμοποιείται για να μεταδίδει μηνύματα μέσω του Διαδικτύου. Στην ουσία το συγκεκριμένο πρωτόκολλο δεν παρέχει κάποια ασφάλεια πράγμα που σημαίνει ότι μπορούν εύκολα να μεταβληθούν στοιχεία όπως για παράδειγμα στο πεδίο From: του ηλεκτρονικού μηνύματος.

Στη συνέχεια θα αναλυθεί μια περίπτωση επίθεσης μέσω του πρωτοκόλλου SMTP.

Αρχικά ο εισβολέας δημιουργεί μια σύνδεση στην πόρτα επικοινωνίας του SMTP (tcp-25) server του χρήστη και εισάγει τις εξής εντολές όπως παρουσιάζεται στον παρακάτω πίνακα:

```
[Cracker]   telnet victims.mailserver.org
[Server]    220 victims.mailserver.org
[Cracker]   hello asxeto.org
[Server]    250  victims.mailserver.org  Hello  asxeto.gr  [Crackers  IP
sender], pleased to meet you
[Cracker]   rcpt to:victim@mailserver.org
[Server]    250 victim@mailserver.org …Recipient ok
[Cracker]   data
[Server]    354 Enter mail, end with "." On a line by itself
[Cracker]   From: your.boss@mailserver.org
```

```
[Cracker]   To: victim@mailserver.org
```

```
[Cracker]   Subject: Παρακαλώ στείλε μου το password
[Cracker]   <μια κενή γραμμή>
[Cracker]   Γεια σου εργαζόμενέ μου. Έξχασα το password για το banking
application και δεν έχω πρόσβαση στο εταιρικό δίκτυο. Παρακαλώ στείλε μου
το password στο hotmail account μου που είναι boss123@hotmail.com
[Cracker]   ευχαριστώ
[Cracker]   <CR><LF>.<CR><LF>
[Server]    250 Message accepted for delivery
(η τελευταία ακολουθία είναι ένα Enter, μία τελεία και μετά πάλι ένα
Enter.)
```

Όπως παρατηρείται από τον κώδικα τα στοιχεία που παρουσιάζονται στον mail client είναι αυτά που έχουν εισαχθεί μετά το DATA. Ο εισβολέας άλλαξε το πεδίο From με σκοπό να ώστε να φαίνεται τα αφεντικό του χρήστη δίνοντας προσοχή στο να εισάγει το mailserver.org

(http://www.ibm.com/support/knowledgecenter/el/SSKTWP_8.5.3/com.ibm.notes85.client.doc/mail_junk_t.html)

Στη συνέχεια θα παρουσιαστούν οι πληροφορίες που εισάγονται στο Header ενός e-mail κατά την αποστολή του και ποια είναι η ερμηνεία τους.

Ανάλυση του Internet Header:

Microsoft Mail Internet Headers Version 2.0

Αυτός ο Header μπαίνει από το Outlook του αποστολέα

Received: from mail.litwareinc.com ([10.54.108.101]) by mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);

Wed, 15 Dec 2004 13:39:22 -0800

Αυτός ο Header ενημερώνει πως κάποιος υπολογιστής με όνομα mail.litwareinc.com πήρε μήνυμα από τον υπολογιστή με όνομα mail.proseware.com στις 13:39:22 την 15η Δεκεμβρίου 2004 (Λογικά αυτοί οι δύο υπολογιστές είναι mail servers).

Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com with Microsoft SMTPSVC(6.0.3790.0);

Wed, 15 Dec 2004 13:38:49 -0800

Αυτός ο header ενημερώνει πως με τη σειρά του, ο mail.litware.com πήρε το μήνυμα από κάποιον υπολογιστή με όνομα mail στις 13:38:49 την 15η Δεκεμβρίου 2004. Από τη στιγμή που στη συνέχεια δεν έχουμε κάποιο άλλο Header που να ξεκινάει με “Received:”, θεωρούμε πως ο υπολογιστής με όνομα mail και διεύθυνση IP 10.54.108.23 είναι ο υπολογιστής από τον οποίο ξεκίνησε το μήνυμα (αν και αυτό δεν ισχύει πάντα μιας και υπάρχουν τρόποι απόκρυψης του υπολογιστή που αρχικοποιεί το μήνυμα).

From: "Kelly Weadock" kelly@litware.com

Ο συγκεκριμένος header ενημερώνει πως το μήνυμα φαίνεται να έχει έρθει από κάποιο χρήστη με διεύθυνση e-mail kelly@litware.com

To: <anton@proseware.com>

Εδώ παρατηρείται το όνομα του παραλήπτη του μηνύματος.

Subject: Review of staff assignments

Αυτός ο header περιέχει το subject του μηνύματος.

Date: Wed, 15 Dec 2004 13:38:31 -0800

Ο συγκεκριμένος header περιέχει την ημερομηνία που ο αποστολέας έστειλε το μήνυμα. Η ημερομηνία αυτή έγινε generate στον υπολογιστή του αποστολέα, έτσι αν ο αποστολέας είχε λανθασμένη ημερομηνία στον υπολογιστή του αυτό θα φανεί στο συγκεκριμένο header.

MIME-Version: 1.0

Αυτός ο header μπαίνει από το Outlook και περιγράφει την έκδοση του πρωτοκόλλου MIME που χρησιμοποίησε ο αποστολέας.

Content-Type: multipart/mixed;

Ο σκοπός του συγκεκριμένου header είναι να δώσει οδηγίες στον e-mail client του παραλήπτη για να μπορέσει να κάνει format το μήνυμα σωστά.

X-Mailer: Microsoft Office Outlook, Build 11.0.5510 Αυτός ο header αναφέρει την ακριβή έκδοση του Outlook που χρησιμοποιήθηκε για να σταλεί αυτό το μήνυμα.

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

Περισσότερες πληροφορίες για τον e-mail client που χρησιμοποίησε ο αποστολέας.

Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==

Αυτός ο header χρησιμοποιείται για να γίνει λογική σύνδεση μηνυμάτων που ανήκουν στο ίδιο thread. Αυτό μπορεί να χρησιμοποιηθεί για παράδειγμα από το Outlook, όταν κάνουμε group τα μηνύματα βάση conversation (από το κεντρικό μενού του Outlook επιλέγουμε View – Arrange by – Conversation).

Return-Path: kelly@litware.com

Ο συγκεκριμένος header μας ενημερώνει για το πως μπορούμε να επικοινωνήσουμε με τον αποστολέα (π.χ. όταν επιλέγουμε να του στείλουμε ένα reply).

Message-ID: MAILbbnewS5TqCRL00000013@mail.litware.com

Κάθε μήνυμα παίρνει ένα message-ID από τον server του αποστολέα. Το μήνυμα κρατάει το ίδιο message id καθ' όλη τη διάρκεια της ζωής του. Επειδή ακριβώς το μήνυμα μπαίνει από τον originating mail server, συνήθως θα παρατηρήσουμε ότι διατηρεί και κάποιο χαρακτηριστικό γνώρισμα (πχ @mail.litware.com).

X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC) FILETIME=[2E0D4910:01C38DDC]

Αυτός είναι ένας header που μπαίνει στο μήνυμα την πρώτη φορά που θα περάσει από έναν Microsoft Exchange Server.

(*https://purnendukumar.wordpress.com/2011/12/12/fourth-generation-wireless-technology/*)

Στον παρακάτω πίνακα παρατηρείται η δομή του παραπάνω Header (από ένα κανονικό e-mail)

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com
with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Kelly Weadock" kelly@litware.com
5) To: anton@proseware.com
6) Subject: Review of staff assignments
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Return-Path: kelly@litware.com
14) Message-ID: MAILbbnewS5TqCRL00000013@mail.litware.com
15) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Στον παρακάτω πίνακα παρουσιάζεται η δομή ενός spoofed μηνύματος ηλεκτρονικού ταχυδρομείου. Όπως φαίνεται στέλνετε μήνυμα ηλεκτρονικού ταχυδρομείου στη διεύθυνση anton@proseware.com ως ceo@proseware.com.

```
1) Microsoft Mail Internet Headers Version 2.0
2)    Received:    from    mail.litwareinc.com    ([10.54.108.101])    by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3)  Received:  from  spoofer  ([10.10.105.123])  by  mail.spoofers.com  with
Microsoft                                              SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Company CEO" ceo@proseware.com
5) To: anton@proseware.com
6) Subject: Please send me my dialup password at ceo@niamodekaf.com
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnew85TqCRL00000013@mail.spoofers.com
14)    X-OriginalArrivalTime:    15    Dec    2004    21:38:50.0145    (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Στις γραμμές 2 και 3 που φαίνονται στον παραπάνω πίνακα παρατηρείται ότι υπάρχει δρομολόγηση από ξένους servers που δεν θα έπρεπε να βρίσκονται εκεί το οποίο είναι περίεργο καθώς το δίκτυο είναι εσωτερικό. Άλλη μια παρατήρηση που θα πρέπει να αναφερθεί είναι στη γραμμή 13 όπου εμπεριέχονται στοιχεία «ξένα» προς το δίκτυο του χρήστη.

Στον παρακάτω πίνακα παρατηρείται το Internet Header ενός spoofing μηνύματος ηλεκτρονικού ταχυδρομείου.

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from spoofer ([10.10.105.123]) by mail.spoofers.com with
Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Microsoft Technical Support" support@microsoft.com
5) To: anton@proseware.com
6) Subject: Change in security policy requires that you change your Hotmail
password to p@ssw0rd
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnew85TqCRL00000013@mail.spoofers.com
14) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

5.4 DIALERS

Τα Dialers αποτελούν λογισμικά τα οποία χρησιμοποιούνται για να διακόψουν τη σύνδεση μιας τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet (ISP). Στην ουσία μόλις εγκατασταθούν τα συγκεκριμένα προγράμματα στον υπολογιστή μεταβάλλουν τις ρυθμίσεις του modem από έναν πάροχο υπηρεσιών Internet σε μία

άλλη σύνδεση. Συνήθως η σύνδεση αλλάζει προς αριθμούς υψηλής χρέωσης (π.χ. 090, 901, 00xx κ.α.), οι οποίοι είναι για πρόσβαση σε συγκεκριμένες υπηρεσίες όπου είναι φυσικό ότι δεν γίνεται με τη συγκατάθεση του χρήστη.

Ο λόγος για τον οποίο δημιουργήθηκαν τα συγκεκριμένα προγράμματα είναι για την άμεση πληρωμή των εταιρειών αυτών που χρησιμοποιούσαν τα ίδια λογισμικά. Ο τρόπος με τον οποίο λειτουργούν τα συγκεκριμένα προγράμματα είναι ο εξής:

- ο χρήστης επισκέπτεται μια ιστοσελίδα η οποία διαθέτει ειδικό περιεχόμενο
- στη συνέχεια εμφανίζεται στην οθόνη του χρήστη ένα παράθυρο το οποίο ζητάει την άδεια του για να κατεβάσει το λογισμικό dialer.
- μόλις επιλεχθεί η επιλογή «yes», το πρόγραμμα του dialer εγκαθιστάτε στον υπολογιστή του χρήστη.

Όσο διαρκεί η περιήγηση του χρήστη στο ειδικό περιεχόμενο υπάρχει ένδειξη στην οθόνη ότι ο χρήστης έχει συνδεθεί στο διαδίκτυο με αυξημένη χρέωση. Μόλις ο χρήστης αποχωρήσει από την ιστοσελίδα τότε αποκαθίσταται το συγκεκριμένο πρόγραμμα από τον υπολογιστή

(*https://purnendukumar.wordpress.com/2011/12/12/fourth-generation-wireless-technology/***).**

Οι τρόποι λειτουργίας των συγκεκριμένων προγραμμάτων έχουν ως εξής:

- Οι εισβολείς μεταβάλλουν τις ρυθμίσεις του δικτύου μέσα από την τηλεφωνική σύνδεση του χρήστη και τότε ο χρήστης θα πρέπει να καλέσει ένα συγκεκριμένο αριθμό. Τοποθετούν το δικό τους αριθμό μόλις διαγράψουν τον τον αριθμό του ISP και έτσι ο χρήστης καλεί στον αριθμό που έχουν εισάγει με τις αντίστοιχες χρεώσεις.
- άλλος ένας τρόπος που χρησιμοποιούν είναι να εισέλθουν στα συστήματα του υπολογιστή του χρήστη ώστε να παρακάμψει τις ρυθμίσεις του δικτύου μέσω τηλεφωνικής γραμμής και να καλέσει ο χρήστης έναν συγκεκριμένο αριθμό που θα έχει εισάγει ο εισβολέας.

Οι ιστοσελίδες που χρησιμοποιούν οι εισβολείς για να πραγματοποιήσουν τις προαναφερθέντες ενέργειες είναι ιστοσελίδες που παρέχουν πειρατικό λογισμικό, πορνογραφικό περιεχόμενο κλπ. Μόλις ο χρήστης εισέλθει σε κάποια από αυτές τις ιστοσελίδες εγκαθίστανται αυτόματα το πρόγραμμα dialer καθώς ο εισβολέας έχει εισάγει τον κώδικα dialer στις ιστοσελίδες. Τέλος μπορεί να πραγματοποιηθεί και

μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στέλνοντας ένα συνημμένο αρχείο το οποίο μόλις ο χρήστης το κατεβάσει στον υπολογιστή του θα εγκατασταθεί το πρόγραμμα dialer.

5.4.1 ΤΟ DIALER ΣΤΟΝ ΗΛΕΚΤΡΟΝΙΚΟ ΥΠΟΛΟΓΙΣΤΗ

Η κατανόηση της εγκατάστασης του dialer στον υπολογιστή γίνεται με διάφορους τρόπους. Σύμφωνα με τη διεθνή βιβλιογραφία οι πιο συνηθισμένοι εξ αυτών είναι:

- Η αποσύνδεση του modem και η προσπάθεια ασταθούς επανασύνδεσης του.
- Η χαμηλή για τα συνήθη δεδομένα σύνδεση. Προφανώς υπάρχουν πολλοί λόγοι για την απότομη μείωση της ταχύτητας σύνδεσης αλλά η εγκατάσταση του dialer πολλές φορές παρουσιάζει αυτό το χαρακτηριστικό.
- Η μη δυνατότητα αποστολής μηνυμάτων ακόμα και όταν ο υπολογιστής βρίσκεται εντός του διαδικτύου.
- Ο λογαριασμός της συνδρομής στην εταιρία παροχής παρουσιάζεται αφύσικα υψηλός (Βενιέρης, 2003)

5.4.2 ΤΡΟΠΟΙ ΠΡΟΦΥΛΑΞΗΣ ΑΠΟ ΤΟΥΣ DIALERS

Έχουν προταθεί διάφοροι τρόποι για την προστασία του ηλεκτρονικού υπολογιστή από τους dialers. Οι τρόποι αυτοί μπορούν να ταξινομηθούν ως εξής:

- Ο υπολογιστής θα πρέπει να απενεργοποιείτε όταν δε χρησιμοποιείτε
- Τα αρχεία αγνώστου προελεύσεως δεν πρέπει ποτέ να ανοίγονται
- Ο κάθε υπολογιστής θα πρέπει να διαθέτει «αντιβιώτικά προγράμματα» λατινική ονομασία Antivirus (π.χ. Nod32, AGV).
- Θα πρέπει να γίνεται συνεχής έλεγχος του υπολογιστή για spyware.
- Θα πρέπει να εξετάζεται ανα τακτά χρονικά διαστήματα η σύνδεση του ηλεκτρονικού υπολογιστή ενώ ταυτόχρονα θα πρέπει να επιβεβαιώνονται οι αριθμοί κλήσης του modem.

· Θα πρέπει να μην ανοίγει ο χρήστης διάφορες ιστοσελίδες που εμφανίζονται κατά την περιήγηση στο διαδίκτυο.

· Η ένταση του modem θα πρέπει να είναι σε υψηλό επίπεδο ώστε να μπορεί να προσδιοριστεί η πιθανότητα ανάκλησης.

· Θα πρέπει να γίνεται συνεχής έλεγχος στην επιφάνεια εργασίας για την περίπτωση που έχει τοποθετηθεί κάποιο άγνωστο εικονίδιο.

· Να υπάρχει ενεργοποιημένη η υπηρεσία φραγής εισερχομένων κλήσεων του υπολογιστή καθώς και κλήσεων εξωτερικού και αυξημένων χρεώσεων.

5.5 E-MAIL BOMB

Σαν e-mail bomb ορίζεται το είδος επίθεσης στον υπολογιστή κατά την οποία στέλνονται μεγάλες ποσότητες μηνυμάτων προς μια διεύθυνση ηλεκτρονικού ταχυδρομείου με απώτερο σκοπό να προκαλέσει δυσλειτουργία στο σύστημα server του ηλεκτρονικού υπολογιστή μέσω της υπερφόρτωσης του διαθέσιμου χώρου στο δίσκο. Η βασική διαφορά μεταξύ του e-mail bomb και του spamming είναι ότι στην περίπτωση του e-mail bomb στέλνετε πληθώρα μηνυμάτων προς ένα παραλλήπτη ενώ στην περίπτωση spamming στέλνετε ένα μήνυμα προς μεγάλο όγκο παραλληπτών.

Η διακίνηση των e-mail bombs πραγματοποιείτε με δύο βασικούς τρόπους. Στην πρώτη περίπτωση ο cracker δημιουργεί ένα πρόγραμμα το οποίο αποστέλλει πληθώρα μηνυμάτων στην υπολογιστή του παραλήπτη. Αυτή η μέθοδος κρίνεται ως μη ιδιαίτερα αποτελεσματική λόγω του εύκολου εντοπισμού της διαδικασίας αυτής με τα μηνύματα να καταλήγουν στην ανεπιθύμητη αλληλογραφία (spam). Στη δεύτερη περίπτωση υπάρχει η μέθοδος Distributed Denial of Service (DDoS) κατά την οποία η επίθεση του cracker γίνεται από ομάδα υπολογιστών οι οποίοι αποστέλλουν το μήνυμα. Τα μηνύματα αποστέλλονται από διαφορετική διεύθυνση ID με αποτέλεσμα ο server να μην μπορεί να τα απορρίψει στην ανεπιθύμητη αλληλογραφία. Η ακριβής διαδικασία της μεθόδου Distributed Denial of Service προϋποθέτει την εγγραφή του υπολογιστή «θύματος» χωρίς τη συγκατάθεσή του. Οι διαδικτυακές υπηρεσίες που γράφετε είναι υπηρεσίες όπως τα Newsletters. Σε όσες

περισσότερες υπηρεσίες εγγραφεί μη θελημένα ο υπολογιστής τόσα περισσότερα κρούσματα ανεπιθύμητης αλληλογραφίας θα έχει.

Ο τρόπος αποφυγής της παραπάνω διαδικασίας είναι η επιβεβαίωση του χρήστη στις υπηρεσίες εγγραφής του. Παραλλαγή των e-mail bombs είναι η διαδικασία αποστολής ανεπιθύμητης αλληλογραφίας ZIP Bombs. Κατά τη διαδικασία αυτή τα ανεπιθύμητα μηνύματα λαμβάνονται σε μορφή συμπιεσμένων αρχείων όπως ZIP ή RAR. Τα μηνύματα αυτά φτάνουν κατά εκατοντάδες στον υπολογιστή ενώ εντός τους περιέχετε τουλάχιστον ένα αρχείο στην προαναφερθείσα συμπιεσμένη μορφή. Στο συμπιεσμένο έγγραφο εμπεριέχονται χαρακτήρες που κατά κύριο λόγο δέχεται μεγάλη συμπίεση όπως ο χαρακτήρας “a”. Αποτέλεσμα της διαδικασίας αυτής είναι η δυσλειτουργία του γενικού συστήματος του server όταν αυτός θα μπει στη διαδικασία αποσυμπίεσης των αρχείων (Κάτσικας, 2004).

Με την εξέλιξη της τεχνολογίας αυτού του είδους ηλεκτρονικής επίθεσης φτάνουν στο σημείο να χαρακτηριστούν μη ιδιαίτερα απειλητικές λόγω του ότι οι server πλέον έχουν εκσυγχρονιστεί με νέα φίλτρα τα οποία δύναται να αναγνωρίσουν τα e-mail bombs και να τα αποστείλουν στην ανεπιθύμητη αλληλογραφία ενώ στη περίπτωση των zip bombs δύναται να διακοπεί όλη η διαδικασία αποσυμπίεσης όταν ο server αντιληφθεί τον κίνδυνο. Ακόμα οι νέοι επεξεργαστές έχουν συνεχώς μεγαλύτερη μνήμη ώστε να μην οδηγείτε ο υπολογιστής σε δυσλειτουργία του συστήματος.

Στην περίπτωση που η ανεπιθύμητη αλληλογραφία εισέρθει στον υπολογιστή είναι πολύ δύσκολο για το χρήστη να διαγράψει τόσο μεγάλο όγκο από τα εισερχόμενα του (Comer, 2007).

5.6 HOAXES Ή URBAN LEGENDS

Η ονομασία Hoaxes προέρχεται από το Hocus Pocus (μία μαγική λέξη σαν το άμπρα κατάμπρα). Το Urban Legends σημαίνει αστικοί θρύλοι και δίνουν ακριβώς την ερμηνεία αυτών των e-mails, μιας και είναι φήμη ή θρύλος ο οποίος «περιφέρεται» στο διαδίκτυο. Το περιεχόμενο που έχουν συνήθως τα Hoaxes ή Urban Legends δεν διαφέρει πολύ από αυτό:

- *Διαμαρτυρία για την κακομεταχείριση των γυναικών στο Αφγανιστάν.*
- *Αποστολή χριστουγεννιάτικων καρτών σε ετοιμοθάνατα παιδιά.*
- *Προτάσεις φορολόγησης όσων δεδομένων διακινούνται μέσω Internet.*
- *Φυλακτά καλής τύχης ή κατάρες ακρωτηριασμού και καταστροφής.*

Τα hoaxes είναι e-mails που διακινούνται στο διαδίκτυο και δημοφιλέστερο τούς θέμα είναι οι ιοί.

Μια μεγάλη κατηγορία είναι τα email συμπαράστασης όπου εκθέτουν ένα σημαντικό και κατά κύριο λόγο ψευδές πρόβλημα υγείας ενός ατόμου και ζητούν από τους χρήστες να κινητοποιηθούν με σκοπό κινητοποιηθεί σε μεγαλύτερο όγκο χρηστών το πρόβλημα. Μια ακόμα κατηγορία είναι τα μηνύματα εκφοβισμού τα οποία απειλούν το χρήστη ότι θα γίνει κάτι κακό στην περίπτωση που δεν προχωρήσουν σε προώθηση του συγκεκριμένου μηνύματος (Δουκίδης, 2001).

Στην προσπάθεια να αναγνωριστεί η ανεπιθύμητη αλληλογραφία τύπου Hoaxes η διανθής βιβλιογραφία παραθέτει τα εξής:

1. Οι συγγραφείς των μηνυμάτων χρησιμοποιούν επίσημους όρους για να δελεάσουν τους χρήστες. Στην πρώτη γρήγορη ανάγνωση δεν διαπιστώνετε πρόβλημα στο έγγραφο. Με μια πιο προσεκτική ματιά όμως το έγγραφο δεν έχει να προσκομίσει καμία νέα ή ενδιαφέρουσα πληροφορία στο χρήστη.

Στη συνέχεια παρουσιάζεται ένα παράδειγμα κατανόησης των προαναφερθέντων.

```
"...if the program is not stopped, the computer's processor will be placed
in an nth-complexity infinite binary loop which can severely damage the
processor..."
```

αν το μελετήσουμε δεν υπάρχει κάτι που να αποκαλείται nth-complexity infinite binary loop και σε τελική ανάλυση οι επεξεργαστές είναι φτιαγμένοι για να κάνουν loops εβδομάδες χωρίς να παθαίνουν τίποτε.

2. Μια ακόμα προσπάθεια εντοπισμού κακόβουλων μηνυμάτων είναι η επίκληση του αποστολέα μια επώνυμης, ιδιαίτερα γνωστής εταιρίας όπως είναι η Microsoft, η Google και η Yahoo. Είναι όμως γνωστό ότι οι εταιρίες διεθνούς φήμης για την οποιαδήποτε ανακοίνωση χρησιμοποιούν τα μέσα του τύπου και ποτέ προσωπικά, ομαδικά μηνύματα.

3. Επόμενο, σημαντικό στοιχείο των Hoaxes είναι να ζητάει τη προώθηση του σε άλλους χρήστες. Αυτός είναι και ο στόχος του και αν ένα email ζητάει κάτι τέτοια είναι βέβαιο ότι πρόκειται για Hoax.

4. Σε πολλές περιπτώσεις χρησιμοποιείτε ο εκφοβισμός όπως για παράδειγμα «*Ψήφισε και εσύ κατά της φορολόγησης των πακέτων του Internet διαφορετικά σύντομα θα αρχίσουν να σε χρεώνουν*». Τις περισσοτερες φορές έχουν κακή σύνταξη και είναι ανορθόγραφα.

5. στην περίπτωση που το μήνυμα παρουσιάζει πραγματική σημαντικότητα θα πρέπει να αναφέρει το site το οποίο έχει δημιουργήσει το μήνυμα και τον λόγο για τον οποίο έχει δημιουργηθεί. Στην περίπτωση που υπάρχει το όνομα της ιστοσελίδας θα πρέπει ο χρήστης να εστιάσει στο όνομα και αν το θεωρεί ύποπτο να διαγράψει το μήνυμα (Scambray, 2003).

Συμπερασματικά για την ορθή προστασία του ηλεκτρονικού υπολογιστή από τα hoaxes παρατίθενται τα εξής:

Η σωστή ενημέρωση αποτελεί βασικό στοιχείο της προστασίας των χρηστών. Στην περίπτωση που ο χρήστης δέχεται ένα mail θα πρέπει να είναι σε θέση να ελεγξει την πηγή προέλευσης και σε καμία περίπτωση να μην αποδέχεται τις προτροπές του κάθε μηνύματος χωρίς σκέψη.

Τα προβλήματα που προκαλούνται από τα Hoaxes είναι δύο ειδών. Το πρώτο αφορά την κινητικότητα του διαδικτύου και το δεύτερο αφορά τη δημιουργία

μεγάλων λιστών λογαριασμών που δύναται να χρησιμοποιηθούν για μελλοντική χρήση.

Τα Chain Letters αποτελούν μια υποκατηγορία των Hoaxes τα οποία είναι φτιαγμένα για να υποσχεθούν καλή τύχη στους χρήστες για όλες τις πτυχές της ζωής τους (*http://portal.kathimerini.gr/4Dcgi/4dcgi/_w_articles_kathworld_7_13/04/2011_387432*).

Τέλος αξίζει να σημειωθεί ότι τα Hoaxes πλέον έχουν εισχωρήσει και στα κινητά τηλέφωνα. Στη συνέχεια παρατίθενται ορισμένα παραδείγματα κατανόησης για τη λειτουργία των Hoaxes ώστε να μπορεί ο χρήστης να αποφύγει την ανεπιθύμητη αλληλογραφία.

Παράδειγμα HOAX 1:

```
A MEMBER OF AOL BY THE SCREEN NAME OF ZZ331MIGHT TRY TO SEND YOU A VIRUS
WHICH COULD CRASH YOUR COMPUTER SYSTEM.
HIS TRICK: HE INNOCENTLY IM's YOU HELLO, WAITS 30 SECONDS, THEN IM's YOU
AGAIN, WAITS ANOTHER 30 SECONDS, AND THEN WRITES...
"WHAT THE FU**, WHY AREN'T YOU ANSWERING"DO NOT REPLY TO HIS IM's, NOR READ
ANY OF HIS E-MAIL BECAUSE ONCE YOU REPLY, YOUR
COMPUTER WILL FREEZE AND THATS HOW YOU KNOW YOUR HARD DRIVE IS BEING WIPED
OUT. SO PLEASE BE VERY VERY CAREFUL!!!!
PLEASE PASS THIS ON TO EVERY ONE YOU KNOW!!!
```

Παράδειγμα HOAX 2:

```
Outbreak: I'm infecting you with t-virus, my code is <random numbers>.
Forward this to <phone number> to get your own code and chance to win
prizes.
More at <website URL>
```

HOAX για το κινητό τηλέφωνο:

Ένα παράδειγμα Hoaxκινητών τηλεφώνων είναι η ακόλουθη:

"Αν σας τηλεφωνήσουν στο κινητό σας από κάποιον που θα σας πει ότι είναι τεχνικός εταιρείας, και κάνουν έλεγχο στο τηλέφωνό σας και θα πρέπει να πατήσετε #90 ή 09# ή οποιοδήποτε άλλο νούμερο, ΚΛΕΙΣΤΕ ΤΟ ΤΗΛΕΦΩΝΟ ΧΩΡΙΣ ΝΑ ΠΑΤΗΣΕΤΕ ΚΑΠΟΙΟ ΑΡΙΘΜΟ. Πρόκειται για κάποια εταιρεία-απάτη που χρησιμοποιεί κάποια συσκευή, η οποία μόλις πατήσετε τα παραπάνω νούμερα, μπορεί να μπει στην κάρτα SIM και να παίρνουν τηλέφωνα με δική σας χρέωση. Προωθήστε το μήνυμα σε όσους περισσότερους μπορείτε."

Το παραπάνω μήνυμα παρουσιάστηκε για πρώτη φορά το1999 στη Γερμανία. Την ίδια περίοδο σε μια προσπάθεια διαφύλαξης των καταναλωτών της προέβει σε μια ανακοίνωση με την οποία δήλωνε ότι το τεχνικό της τμήμα δεν μπορεί να έχει προβεί στην αποστολή αυτού του μηνύματος διότι στη χώρα της Γερμανίας δεν υφιστατε το reverse charging και το δίκτυο δεν υποστηρίζει πρόσβαση σε κάρτες SIM κατά τη διάρκεια μιας κλήσης.

Η κάρτες των χρηστών διαθέτουν ένα και μοναδικό αριθμό ασφαλείας PIN και μαζί με το κλειδί κρυπτογραφείας δεν γίνεται αποδεκτή η πρόσβαση στην κάρτα με το συνδυασμό 9009 (Comer , 2007).

Σημαντική επίσης παρουσιάζεται η τοποθέτηση της ελληνικής εταιρίας κινητής τηλεφωνίας “Vodafone” η οποία μπήκε στη διαδικασία άμεσης απάντησης για να ενημερωθεί ο πληθυσμός- πελάτες των υπηρεσιών της. Η απάντηση της υπεύθυνης της εταιρίας ήταν η εξής:

«θα θέλαμε να σας ενημερώσουμε ότι, και στο παρελθόν έχει αναφερθεί κάτι ανάλογο το οποίο όταν διερευνήθηκε διαπιστώθηκε ότι δεν ήταν πραγματικό γεγονός, δεν έχει καταγραφεί και διαπιστωθεί γιατί απλά δεν ισχύει κάτι τέτοιο. Ήταν μια κακόγουστη

φάρσα. Τεχνικά και δικτυακά δεν υπάρχει απολύτως καμία πρόσβαση στην κάρτα sim του συνδρομητή με οποιαδήποτε χρήση κωδικών ή άλλων ενεργειών εξ αποστάσεως, έτσι όπως περιγράφεται. Σε καμία περίπτωση δεν ισχύει ότι αναφέρεται. Παρακαλούμε μην διστάσετε αν έχετε κάποια άλλη ερώτηση ή απορία. Στην διάθεση σας για οποιαδήποτε διευκρίνιση.

Ευχαριστούμε που επικοινωνήσατε μαζί μας.» .

5.7 ΙΟΙ

Η έννοια των ιών απασχολεί το μεγαλύτερο μέρος των χρηστών των ηλεκτρονικών υπολογιστών. Η διαφορά του παραδοσιακού ιού με αυτόν που προσβάλει τον ηλεκτρονικό υπολογιστή είναι ότι στην περίπτωση του ηλεκτρονικού υπολογιστή χρησιμοποιείτε κώδικας δημιουργίας. Το κοινό χαρακτηριστικό τους είναι ότι μέσα από συγκεκριμένες προϋποθέσεις μπορούν να εξαπλωθούν και να πολλαπλασιαστούν.

Υπάρχουν διάφορες κατηγορίες ιών που προσβάλουν έναν ηλεκτρονικό υπολογιστή. Μια δυσάρεστη συνέπεια από την προσβολή του ηλεκτρονικού υπολογιστή είναι η διαγραφή όλων των αρχείων και τον δεδομένων από τη μνήμη του υπολογιστή. Ακόμα μπορεί να προκαλέσει δυσλειτουργία στην ενεργοποίηση και απενεργοποίηση του υπολογιστή. Σε όλες τις περιπτώσεις προκαλούν φθορά στον υπολογιστή ενώ μπορεί να προκαλέσουν και αναστολή της λειτουργίας του (Comer, 2007).

5.7.1 ΟΙ ΤΥΠΟΙ ΙΩΝ ΚΑΙ ΟΙ ΣΥΝΕΠΙΕΣ ΤΟΥΣ

Το Worms είναι ένας τύπος ιού που έχει σχεδιαστεί για να αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλο. Η βασική διαφορά με τους άλλους τύπους είναι οι ο συγκεκριμένος ιός έχει τη δυνατότητα να αντιγράφει τον εαυτό του και να εκτελείται αυτόματα. Είναι εξαιρετικά επικίνδυνος γιατί η αναπαραγωγή του γίνεται

γρήγορα και σε μεγάλο βαθμό. Μπορεί να σταλεί σε όλες τις επαφές του ηλεκτρονικού ταχυδρομείου και να προκαλέσει υπερφόρτωση του δικτύου. Παραδείγματα ιών τύπου worm είναι ο Sasses και ο Blaster. Ο ιός Blaster χρησιμοποιεί ανοικτές θύρες κλήσης απομακρυσμένης διαδικασίας (Δουκίδης, 2001).

Δούρειος Ίππος (Trojan)

Ο συγκεκριμένος ιός αναφέρεται και σαν κεκαλυμμένος ιος. Η ιδιότητα του είναι να εμφανίζεται με την ονομασία ενός αρχείου εμπιστοσύνης όπως είναι τα αρχεια των ενημερώσεων που λαμβάνει ο υπολογιστής και με την αποδοχή που θα κάνει ο χρήστης ώστε να «τρέξει» το αρχείο- πρόγραμμα θα απενεργοποιηθεί το πρόγραμμα ασφάλειας του υπολογιστή. Ο ιος μπορεί να ενσωματωθεί και στον κώδικά προγραμμάτων οποιουδήποτε τύπου και έτσι να γίνει πολύ πιο δύσκολος ο εντοπισμός του και η διαγραφή του. Σε κάθε περίπτωση θα πρέπει να γίνεται έλεγχος του συστήματος ασφαλείας του υπολογιστή και ο χρήστης να μην εμπιστεύεται μη έγκυρες πηγές ώστε να πραγματοποιήσει λήψη ενός αρχείου (Roger, 2000)

Logical Bombs

Η λογική του συγκεκριμένου ιου είναι ότι τοποθετείτε εντός ενός συστήματος και μένει ανενεργός μέχρι κάτι να προκαλέσει την ενεργοποίηση του. Συνήθως ενεργοποιείτε νε την ικανοποίηση μια κωδικοποιημένης συνθήκης. Ο παράγοντας που προκαλεί την ενεργοποίηση της είναι είτε εσωτερικός είτε εξωτερικός. Στην ουσία δεν έχει βρεθεί συγκεκριμένος τρόπος αντιμετώπισης του ιου. Στην περίπτωση ενεργοποίησης του μπορεί να προκαλέσει βλάβη στο πληροφοριακό σύστημα. Παρόμοιος τύπος ιου είναι και οι χρονικές βόμβες με τη διαφορά ότι η ενεργοποίηση τους γίνεται σε κάποια συγκεκριμένη και δεδομένη χρονική στιγμή.

Mail Bugs

Ο συγκεκριμένος ιός είναι δύσκολος στην αναγνώριση του γιατί βρίσκεται σε μορφή HTML. είναι εύκολο να παραβιάσει το απόρρητα των πληροφοριών ενός ηλεκτρονικού υπολογιστή. Τα Micros Virus Scripts, εποτελούν ιούς γνωστούς για την αποστολή τους μέσω ηλεκτρονικού ταχυδρομείου που περιέχουν εντολές αυτόματης εκτέλεσης που πραγματοποιούνται με το άνοιγμα του ηλεκτρονικού μηνύματος (Νομικό περιοδικό ‘Αρμενόπουλος 2007/993).

Άλλοι λιγότερο σημαντικοί ιοί:

Adware, Backdoors, Boot viruses, Bot-Net, EICAR test file, Exploit, Grayware, Honeypot, Keystroke logging, Polymorph viruses, Program viruses, Spyware, Zombie.

5.8 SNIFFING

Αποτελεί ίο που συγκαταλέγεται στους παθητικού ιους. Κύριος σκοπός αυτού του ιου είναι η συλλογή χρήσιμων στοιχείων από τον υπολογιστή τα οποία αρχειοθετεί και την κατάλληλη στιγμή τα χρησιμοποιεί ώστε να επιτεθεί στο λειτουργικό συστημα του υπολογιστή. Αξιοσημείωτο παράδειγμα είναι οι υποκλοπές κωδικών πρόσβασης που πραγματοποιούνατι με αυτόν τον ιο.

Υπάρχουν όμως και προγράμματα sniffers που η χρησιμοποίηση τους είναι νόμιμη. Κατά κύριο λόγο χρησιμοποιούνται από διαχειριστές ώστε να διορθώσουν προβλήματα σε κάποιο σύστημα όμως χρησιμοποιούνται και από crakers.

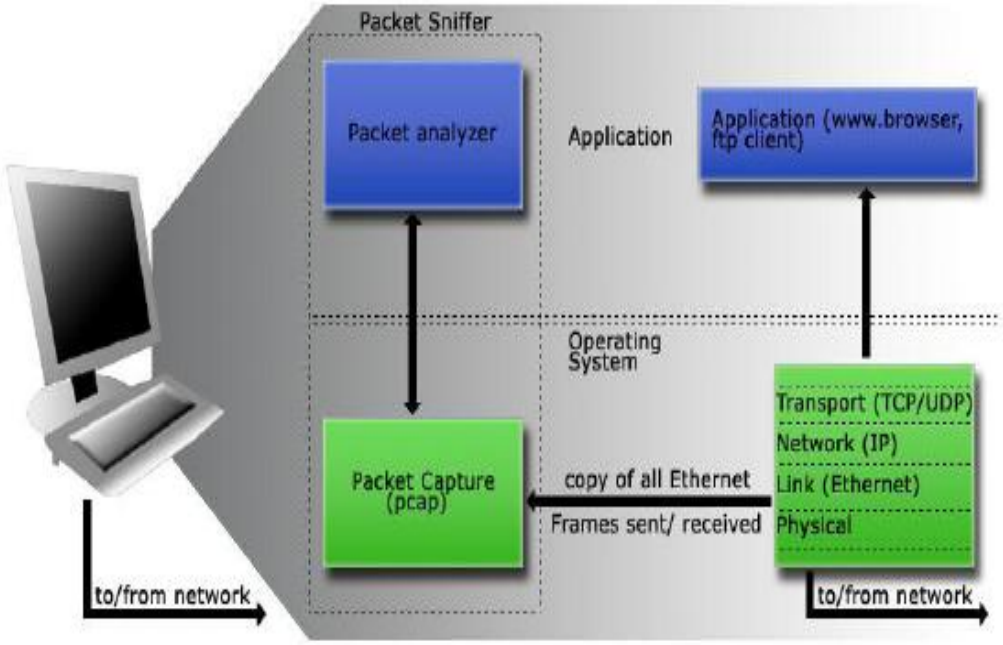
Ο ιός λειτουργεί με βάση τη σύνδεση Lan των υπολογιστών. Πολλοί υπολογιστές πλοηγούνται στο διαδίκτυο με την ίδια σύνδεση. Το sniffer αναγκάζει την κάρτα δικτύου του να αρχίσει να προσέχει και τα πακέτα που δεν προορίζονται για αυτόν, αλλά για τους υπόλοιπους υπολογιστές. Για να το πετύχει αυτό θέτει την κάρτα δικτύου σε ειδική λειτουργία, γνωστή ως promiscuous mode. Όταν η κάρτα δικτύου βρίσκεται σε αυτή τη λειτουργία (μία κατάσταση που απαιτεί δικαιώματα

ανώτερου χρήστη, root), τότε μπορεί το μηχάνημα να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Το sniffing μπορεί να αποφευχθεί με τη χρήστη αντιβιωτικών που είναι γνωστά ως anti sniffing. Ο κυριότερος κίνδυνος του ιου είναι η παθητική του μορφή. Ο κύριος τρόπος για να φανεί η επίθεση στον υπολογιστή από sniffing είναι οι μέθοδοι Ping method, Arp method, local host και latency method και η κρυπτογράφηση με SSL, PGP, SSH κ.α., έτσι ώστε και να αποκτήσει πρόσβαση στα δεδομένα μας ο cracker να μην μπορεί να τα αποκωδικοποιήσει(Νομικό περιοδικό ‘Αρμενόπουλος 2007/993).

.

Στο σχήμα που ακολουθεί φαίνεται η δομή ενός packet Sniffer



Στο δεξί μέρος του Σχήματος είναι τα πρωτόκολλα που υπάρχουν με κανονική μορφή στον υπολογιστή. Στο παραλληλόγραμμο σχήμα έχουμε τον packet Sniffer ο οποίος συνήθως είναι μία προσθήκη στο λογισμικό, που αποτελείται από δύο μέρη.

Το πρώτο μέρος είναι η βιβλιοθήκη σύλληψης πακέτων, η οποία λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης που στέλνεται ή λαμβάνεται από τον

υπολογιστή μας. Ενώ το δεύτερο είναι ο αναλυτής πακέτων, ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό αυτό, ο αναλυτής πακέτων πρέπει να «καταλαβαίνει» τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα (Roger, 2000).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στη σύγχρονη κοινωνία παρατηρείται όλο και περισσότερο η χρήση του ηλεκτρονικού εμπορίου. Αυτό σημαίνει ότι τα ζητήματα ασφαλείας και προστασίας των προσωπικών δεδομένων των χρηστών είναι ιδιαίτερης σημασίας και αποτελούν τον αδύναμο κρίκο του συστήματος. Γι αυτό το λόγο δεν είναι λίγοι οι χρήστες οι οποίοι είναι καχύποπτοι στο να πραγματοποιούν τις συναλλαγές τους μέσω στο διαδικτύου.

Ωστόσο βέβαια το νομοθετικό πλαίσιο που ισχύει σήμερα και για το ηλεκτρονικό εμπόριο αλλά και για τα μηνύματα ηλεκτρονικού ταχυδρομείου εξασφάλίζει μια μια ασφάλεια γύρω από τις ηλεκτρονικές συναλλαγές. Επίσης, θα πρέπει να αναφερθεί ότι έχουν δημιουργηθεί αρκετά προγράμματα τα οποία παρέχουν ασφάλεια και προστασία προσωπικών δεδομένων των χρηστών και όσων πραγματοποιούν ηλεκτρονικές συναλλαγές.

Το διαδίκτυο θεωρείται απαραίτητο εργαλείο για όλους και χρησιμοποιείται σε καθημερινή βάση από όλους. Αυτό σημαίνει ότι χρειάζεται ιδιαίτερη προσοχή η χρήση του λόγω των κινδύνων που εγκυμονεί. Οι εισβολείς βρίσκουν συνεχώς πρακτικές και πραγματοποιούν ενέργειες για να εξαπατήσουν τους χρήστες εισβάλλοντας στους υπολογιστές τους και αποσπώντας τα προσωπικά τους στοιχεία όπως για παράδειγμα κωδικούς τραπεζικών λογαριασμών.

Επίσης άλλος ένας τρόπος με τον οποίο προσπαθούν να εξαπατήσουν τους χρήστες είναι μέσω ηλεκτρονικής αλληλογραφίας. Το γεγονός ότι το ηλεκτρονικό ταχυδρομείο είναι μια από τις διασημότερες υπηρεσίες του διαδικτύου το καθιστά ιδιαίτερα επιρρεπή σε επιθέσεις από εισβολείς για την εξαπάτηση των χρηστών. Γι αυτό το λόγο έχουν δημιουργηθεί προγράμματα τα οποία προσπαθούν να αντιμετωπίσουν τις οποιεσδήποτε επιθέσεις.

Οι χρήστες από τη μεριά τους θα πρέπει να είναι ιδιαίτερα προσεκτικοί με τα μηνύματα που λαμβάνουν και τις ιστοσελίδες στις οποίες εισέρχονται και γι αυτό θα πρέπει να είναι συνέχεια ενήμεροι και να εκπαιδεύονται ώστε να μπορούν να αναγνωρίζουν τις ύποπτες ενέργειες. Η εκπαίδευση θεωρείται πολύ σημαντική και αποτελεί ένα πολύ βασικό παράγοντα αντιμετώπισης των επιθέσεων που πραγματοποιούνται στο ηλεκτρονικό ταχυδρομείο, στις ιστοσελίδες κλπ. καθώς

πολλά άτομα δεν έχουν τις απαραίτητες γνώσεις και πέφτουν θύματα εξαπάτησης των εισβολέων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Comer D., (2007) *Δίκτυα και Διαδίκτυα Υπολογιστών – και εφαρμογές τους στο Internet*, Εκδόσεις Κλειδάριθμος.

Scambray J, McClure S, Kurtz G, (2003) *Χάκερ Επίθεση και Άμυνα - Τέταρτη Έκδοση 2003*, Εκδόσεις Μ. Γκιούρδας Πολλάλης Γ., (2007), Ηλεκτρονικό Επιχειρήν, Σταμούλη, Αθήνα.

Βλαχοπούλου Μ., (2003), E-marketing : διαδικτυακό μάρκετινγκ\, Rossili, Αθήνα.

Γκρίτζαλης Σ, Κάτσικας Σ, (2003) Ασφάλεια Δικτύων Υπολογιστών – Τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης, Εκδόσεις Παπασωτηρίου.

Γκρίτζαλης Σ, Κάτσικας Σ, (2003) *Ασφάλεια Δικτύων Υπολογιστών – Τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης*, Εκδόσεις Παπασωτηρίου.

Δουκίδης Γ., Α. Πουλημενάκου, V. Γεωργόπουλος, Θ. Μότσιος, (2001), Το ηλεκτρονικό επιχειρείν στις μεγάλες επιχειρήσεις: Θέματα και προοπτικές, Νέων Τεχνολογιών, Αθήνα.

Κάτσικας Σ, Γκρίτζαλης Δ, Γκρίτζαλης Σ, (2004) *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών.

Κοζύρης Φ., Θεοδωρίδης Κ., (2006), *Διαφήμιση & Παρενόχληση: spam και τηλεόραση*, Εκδόσεις Αντ. Ν. Σάκκουλα

Νομικό περιοδικό 'Αρμενόπουλος 2007/993', *Μελέτη «Διαδίκτυο και Αστικό Δίκαιο»* του Παν. Κορνηλάκη

F. Akyildiz and J. S. M. Ho,1995 "Dynamic Mobile User Location Update for Wireless PCS Networks", ACM-Baltzer J. Wireless Networks, vol. 1, no. 2,

J. Biesterfeld and K. Jobmann, 1998"The Use of Prediction Areas to Improve Mobility Management Algorithms", Proc. International Conference on Telecommunications, Chalkidiki, Greece

Roger L.2000 Freeman Manual for Telecommunications Engineering second edition

Sian Chong Je_rey Lee,2009 Discrete Multitone Modulation for Short-Range Optical Communications Eindhoven: Technische Universiteit Eindhoven

Ιάκωβος Στ. Βενιέρης, 2003 "Δίκτυα Ευρείας Ζώνης", Εκδόσεις Τζιόλα,

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

http://portal.kathimerini.gr/4Dcgi/4dcgi/_w_articles_kathworld_7_13/04/2011_387432

http://cyberlovesecurity.com/2015/03/30/explain-voice-over-ip-voip-and-how-to-hack/

https://purnendukumar.wordpress.com/2011/12/12/fourth-generation-wireless-technology/

http://www.asus.com/Networking/USBN13/

http://www.slideshare.net/neeraja507/introduction-of-4g

http://www.sch.gr/2010-04-07-09-22-34/-spam

https://support.office.com/el-gr/article/%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CF%86%CE%AF%CE%BB%CF%84%CF%81%CE%BF%CF%85-%CE%B1%CE%BD%CE%B5%CF%80%CE%B9%CE%B8%CF%8D%CE%BC%CE%B7%CF%84%CE%B7%CF%82-%CE%B1%CE%BB%CE%BB%CE%B7%CE%BB%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1%CF%82-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089

http://www.ibm.com/support/knowledgecenter/el/SSKTWP_8.5.3/com.ibm.notes85.client.doc/mail_junk_t.html

https://support.apple.com/kb/PH2649?locale=el_GR&viewlocale=el_GR

https://it.auth.gr/el/mailServices/antispam

http://www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam

http://www.gateweb.gr/el/support/email/avoid-spam.html

http://download.beta.mcafee.com/webhelp/4/1032/GUID-E4DC6AC2-2C3B-4ABE-8BCA-D9DC6ADF4EEF.html