ΤΕΙ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ & ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ : ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ (SPAMMING) ΚΑΙ ΟΙ ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ.

ΣΠΟΥΔΑΣΤΕΣ:

ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΝΔΡΕΑΣ ΑΜ 912

ΣΤΑΣΙΝΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΑ ΑΜ 964

ΕΙΣΗΓΗΤΗΣ: κ. ΔΗΜΗΤΡΙΟΣ ΜΩΥΣΙΔΗΣ

ΠΑΤΡΑ 2008

Περιεχόμενα

Κεφάλαιο 3

Περίληψη

Από τον πρώτο καιρό της εμφάνισής του, το Διαδίκτυο (Internet) είναι συνυφασμένο με ένα στόχο: την διευκόλυνση της επικοινωνίας των ανθρώπων με την χρήση των υπολογιστών.

Αν και το ηλεκτρονικό μήνυμα (e-mail) θεωρείται το μέσο που έχει αλλάξει τον τρόπο επικοινωνίας των ανθρώπων αφού όχι μόνο τους απελευθέρωσε από το τηλέφωνο, αλλά τους έδωσε και την δυνατότητα να επικοινωνήσουν ανεξάρτητα από τις αποστάσεις και το κόστος, η εμφάνιση της «μη ζητηθείσας» ηλεκτρονικής αλληλογραφίας (spam) έχοντας κατακλύσει τις ηλεκτρονικές θυρίδες κάνει την επικοινωνία αυτή αρκετά δύσκολη.

Σήμερα, το μεγαλύτερο ποσοστό των χρηστών κατακλύζεται από αυτά τα μηνύματα, τα οποία στην ουσία «θάβουν» την ουσιώδη αλληλογραφία. Οι περισσότεροι χρήστες πιστεύουν πως εξαιτίας των μηνυμάτων spam η χρήση του internet έχει γίνει ανυπόφορη. Σύμφωνα με έρευνες που έχουν γίνει, τα 2/3 των μηνυμάτων που δέχονται οι χρήστες είναι spam και αυτό έχει σαν αποτέλεσμα να γίνεται δύσκολη η επικοινωνία αφού μηνύματα από γνωστούς, συναδέλφους χάνονται.

Γίνονται προσπάθειες τόσο σε επίπεδο εθνικών κυβερνήσεων όσο και από την Ευρωπαϊκό Κοινοβούλιο για να περιοριστεί το φαινόμενο της ανεπιθύμητης αλληλογραφίας σε όσους τομείς έχει εμφανιστεί. Η Ευρωπαϊκή Ένωση έχοντας ως προτεραιότητά της την προστασία των καταναλωτών έχει εκδώσει δύο οδηγίες το 1997 και 2002 που αφορούν α) την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις και β) την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Και στις δύο οδηγίες εμποδίζεται η εμπορική επικοινωνία αν δεν υπάρχει η συγκατάθεση του καταναλωτή. Στην Ελλάδα η ισχύουσα νομοθεσία έχει ενσωματώσει την οδηγία του Ευρωπαϊκού Κοινοβουλίου για την προστασία των προσωπικών δεδομένων

των καταναλωτών στις ηλεκτρονικές επικοινωνίες. Στις Ηνωμένες Πολιτείες της Αμερικής υπάρχουν ρυθμίσεις οι οποίες περιλαμβάνουν μέτρα για την πρόληψη και τον περιορισμό της ανεπιθύμητης αλληλογραφίας καθώς και κυρώσεις για τους αποστολείς της ανεπιθύμητης αλληλογραφίας. Το πρόβλημα με τις παραπάνω ρυθμίσεις είναι πως οι αποστολείς των μηνυμάτων spam (spammers) χρησιμοποιούν συχνά εξυπηρετητές (servers) από χώρες που έχουν χαλαρό νομικό προστατευτικό καθεστώς για να μην υπόκεινται σε διώξεις.

Οι spammers για να αποφύγουν τις νομικές επιπτώσεις των πράξεών τους στέλνουν τα μηνύματα spam από συστήματα ηλεκτρονικών υπολογιστών στα οποία έχουν αποκτήσει πρόσβαση χωρίς να το γνωρίζουν οι νόμιμοι διαχειριστές τους χρησιμοποιώντας διάφορες τεχνικές όπως IP spoofing, phishing κτλ. Για να κρύψουν την πραγματική τους διεύθυνση χρησιμοποιούν ηλεκτρονικές διευθύνσεις άλλων χρηστών, τις οποίες έχουν αποκτήσει με την χρήση διάφορων μεθόδων όπως είναι ειδικά προγράμματα (spiders) με την βοήθεια των οποίων ψάχνουν σε δικτυακούς τόπους για την εύρεση ηλεκτρονικών διευθύνσεων.

Όσο αφορά την αντιμετώπιση αυτού του φαινομένου μπορούν τόσο οι χρήστες όσο και οι διακομιστές ηλεκτρονικού εμπορίου να κάνουν κάποιες ενέργειες για την προστασία της ηλεκτρονικής αλληλογραφίας.

Οι λύσεις που εφαρμόζονται στους διακομιστές του ηλεκτρονικού ταχυδρομείου για την προστασία των χρηστών εμποδίζουν την είσοδο των μηνυμάτων spam στα γραμματοκιβώτια των χρηστών ή δεν αφήνουν μηνύματα που προέρχονται από spammers να εισέρχονται σε αυτούς. Οι λύσεις αυτές κυρίως ελέγχουν αν τα μηνύματα που δέχονται προέρχονται από έγκυρους servers. Ωστόσο, υπάρχουν και προγράμματα anti-spamming που μπορούν να χρησιμοποιηθούν για αυτό τον σκοπό όπως τα Barracuda spam Firewall, spam Assassin κ.α.

Οι χρήστες, από την άλλη μεριά, μπορούν να αποφύγουν τα ανεπιθύμητα email καταφεύγοντας σε απλές λύσεις όπως είναι η αποφυγή δημοσίευσης της

ηλεκτρονικής τους διεύθυνσης σε δικτυακούς τόπους. Μια καλή τακτική είναι η δημιουργία δύο ηλεκτρονικών διευθύνσεων όπου η μία διεύθυνση να χρησιμοποιείται για την επικοινωνία με γνωστούς, συγγενείς, φίλους και η δεύτερη θα χρησιμοποιείται για απόκτηση πρόσβασης σε διάφορους ιστοχώρους. Εκτός από τις ενέργειες που μπορεί να κάνει ο κάθε χρήστης για την προσωπική του ασφάλεια, υπάρχουν και αξιόλογα προϊόντα που μπορούν να βοηθήσουν στον έλεγχο των μηνυμάτων που δέχονται. Τα προϊόντα αυτά είναι είτε εμπορικά είτε shareware.

Τέλος, όλη η προσπάθεια που γίνεται για την αντιμετώπιση της ανεπιθύμητης αλληλογραφίας είναι μία προσπάθεια για να διατηρηθεί ο ηλεκτρονικός τρόπος επικοινωνίας, ένα σημαντικό εργαλείο στην καθημερινότητά μας.

Εισαγωγή

Στην εργασία αυτή γίνεται λόγος για την μεγάλη ανάπτυξη του Διαδικτύου και των υπηρεσιών που προσφέρει. Ο παγκόσμιος ιστός, η ηλεκτρονική αλληλογραφία και το ηλεκτρονικό εμπόριο είναι ίσως οι μεγαλύτερες υπηρεσίες που προσφέρει. Κάθε άτομο ή επιχείρηση μπορεί να έχει πρόσβαση στο Διαδίκτυο για παρουσίαση ιδεών και παροχή πληροφοριών.

Η ηλεκτρονική αλληλογραφία είναι από τις δημοφιλέστερες υπηρεσίες του Διαδικτύου γιατί με μικρό κόστος και σε ελάχιστο χρόνο μπορεί κανείς να επικοινωνήσει με άλλα άτομα όπου και αν βρίσκονται.

Το Διαδίκτυο διευκολύνει το ηλεκτρονικό εμπόριο γιατί λόγω του χαμηλού κόστους επικοινωνίας (email), οι επιχειρήσεις μπορούν να προωθήσουν τα προϊόντα και τις υπηρεσίες που προσφέρουν στους καταναλωτές χωρίς πολλά έξοδα. Αυτό έχει ως αποτέλεσμα την διεξαγωγή συναλλαγών μέσω του διαδικτύου .

Παρακάτω θα γίνει μια μικρή ανάλυση του διαδικτύου και των δύο σημαντικότερων υπηρεσιών που μας προσφέρει (ηλεκτρονικό εμπόριο και ηλεκτρονική αλληλογραφία).

Διαδίκτυο

Το Διαδίκτυο ή Internet όπως είναι η διεθνής ονομασία που έχει επικρατήσει, είναι ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών με στόχο την παροχή πληροφοριών και γνώσεων.

Ο στόχος του είναι να διευρύνει τους ορίζοντες της ανθρώπινης γνώσης και επικοινωνίας φέρνοντας τους ανθρώπους σε άμεση και έμμεση επαφή. Πρόκειται για ένα υπερ-δίκτυο στο οποίο χιλιάδες υπολογιστές και εκατομμύρια χρήστες, από όλες τις χώρες του κόσμου, συνδέονται καθημερινά διακινώντας τεράστιους όγκους πληροφοριών και δεδομένων.

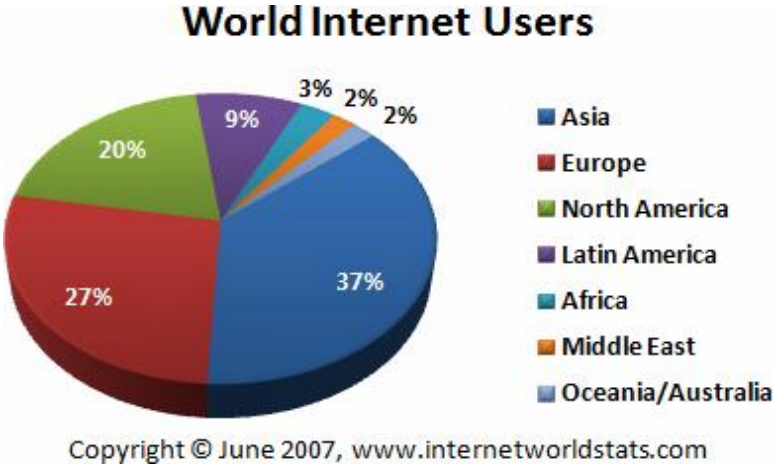
Η γένεση του Διαδικτύου τοποθετείται χρονολογικά στη δεκαετία του 1960, και πιο συγκεκριμένα στο έτος 1969. Η πρώτη του ονομασία ήταν ARPAnet (Advanced Research Projects Agency network) και δημιουργήθηκε ύστερα από εντολή του υπουργείου Άμυνας των ΗΠΑ με στόχο τη διοικητική υποστήριξη του αμερικανικού στρατού σε περίπτωση θερμοπυρηνικού πολέμου και καταστροφής των τηλεπικοινωνιακών κόμβων του. Το 1983 το δίκτυο ARPAnet μετονομάστηκε σε Internet και έγινε διαθέσιμο για δημόσια χρήση, ενώ το 1989 ο κόσμος γνώρισε ίσως την πιο σημαντική εξέλιξη μέχρι σήμερα όσον αφορά το θέμα του Διαδικτύου, την εφεύρεση του **Παγκόσμιου Ιστού** (World Wide Web) από τον Tim Berners-Lee στο CERN.

Το διαδίκτυο σήμερα

Σε χρονικό διάστημα 30 ετών - από την εποχή του δικτύου Arpanet έως την παρουσία του Παγκόσμιου Ιστού - το διαδίκτυο αναδείχτηκε σε ένα από τα πιο θαυμαστά τεχνολογικά και κοινωνικά επιτεύγματα του 20ού αιώνα. Εκατομμύρια άνθρωποι χρησιμοποιούν καθημερινά αυτό το πολύπλοκο δίκτυο διασυνδεδεμένων υπολογιστών. Αυτοί οι υπολογιστές αποτελούνται από πολλά διαφορετικά πακέτα λογισμικού και βρίσκονται σχεδόν σε όλες τις χώρες του

κόσμου. Κάθε χρόνο, πολλά χρήματα αλλάζουν χέρια πάνω από το διαδίκτυο με αντάλλαγμα κάθε λογής προϊόντα και υπηρεσίες.

Το παρακάτω διάγραμμα δείχνει τα στατιστικά χρήσης του Διαδικτύου σε παγκόσμιο επίπεδο και αφορούν τον μήνα Ιούνιο του 2007.



Ένας από τους παράγοντες που συνέβαλαν καθοριστικά στην εξάπλωση της χρήσης του Διαδικτύου, αλλά και στην εμπορευματοποίησή του, ήταν αναμφισβήτητα η ανάπτυξη του Παγκόσμιου Ιστού. Οι κυριότερες υπηρεσίες που παρέχει στους χρήστες του σήμερα είναι:

- **Ηλεκτρονικό Ταχυδρομείο** (e-mail), για την ανταλλαγή ηλεκτρονικών μηνυμάτων. Είναι κείμενα που κατά την αποστολή τους αποθηκεύονται σε υπολογιστές εξυπηρετητές (servers) έτσι ώστε ο παραλήπτης να έχει τη δυνατότητα, οποιαδήποτε στιγμή και από οποιοδήποτε σημείο έχει πρόσβαση στο διαδίκτυο, να λαμβάνει τα μηνύματά του.
- **Μεταφορά αρχείων** μέσω του πρωτοκόλλου FTP (File Transfer Protocol) από κάποιον υπολογιστή σε άλλον.
- **Σύνδεση με απομακρυσμένο υπολογιστή** έτσι ώστε να ενεργοποιεί (τρέχει) τα διάφορα προγράμματά του από απόσταση.
- **Συζήτηση** για διάφορα θέματα μέσα από λίστες συζητήσεων (USENET, newsgroups, και chat-rooms)

♦ **Ηλεκτρονική παρουσίαση** των πληροφοριών μέσα από σελίδες (Web pages) με πολυμεσικές δυνατότητες

♦ Δυνατότητες συνομιλίας με ήχο σε πραγματικό χρόνο **(voice conference)** και πολλαπλή συνομιλία με εικόνα και ήχο με συμμετοχή πολλών χρηστών **(video conference)** και

♦ **Μηχανές Αναζήτησης** (Search Engines) με τις οποίες οι χρήστες μπορούν να εντοπίσουν τις πληροφορίες που χρειάζονται με βάση λέξεις κλειδιά σε ελάχιστο χρόνο.

Τα διαγράμματα που ακολουθούν, δείχνουν την κατάσταση που επικρατεί στην Ελλάδα αναφορικά με την χρήση του Διαδικτύου από τους χρήστες.

Οι λόγοι για τους οποίους το Διαδίκτυο υιοθετήθηκε τόσο γρήγορα και τόσο μαζικά έχουν άμεση σχέση με τα τρία βασικά χαρακτηριστικά γνωρίσματα που το διέπουν. Τα γνωρίσματα αυτά είναι η ύπαρξη ελεύθερης ανταλλαγής δεδομένων και πληροφοριών μεταξύ των χρηστών του Διαδικτύου σε ολόκληρο το πλανήτη, το ιδιόμορφο ιδιοκτησιακό του καθεστώς (ανήκει σε όλους και ταυτόχρονα δεν ανήκει σε κανέναν) και οι τεράστιες οικονομικές προοπτικές που προσφέρει.

Ηλεκτρονικό ταχυδρομείο

Ένα από τα κυριότερα χαρακτηριστικά του Διαδικτύου είναι το ηλεκτρονικό ταχυδρομείο, το οποίο μείωσε στο ελάχιστο τον χρόνο που απαιτείται για την επικοινωνία και την αποστολή δεδομένων. Το ηλεκτρονικό ταχυδρομείο έκανε την εμφάνισή του από τη λειτουργία των πρώτων κιόλας υπολογιστικών συστημάτων. Ακόμα και πριν από την έναρξη του περιβόητου προγράμματος ARPANET, το ηλεκτρονικό ταχυδρομείο υπήρχε, για να καλύπτει την επικοινωνία κάποιων χειριστών που εργάζονταν στα ίδια υπολογιστικά συστήματα διαφορετικές ώρες της ημέρας. Εκείνα τα χρόνια βέβαια, η επικοινωνία έξω από το κτίριο που στέγαζε τα υπολογιστικά αυτά συστήματα ήταν αδιανόητη. Στις αρχές της δεκαετίας του '70, το ηλεκτρονικό ταχυδρομείο απασχολούσε το μεγαλύτερο μέρος του δικτύου ARPANET. Ήταν η εποχή που το ηλεκτρονικό ταχυδρομείο άρχισε να κάνει τα πρώτα του βήματα...

Σήμερα, είναι ο πιο διαδεδομένος αλλά και ευρέως χρησιμοποιούμενος τομέας του Διαδικτύου. Τα πλεονεκτήματα αυτής της υπηρεσίας είναι πολλά και υπερέχουν σημαντικά έναντι των «συμβατικών» μέσων επικοινωνίας, όπως το τηλέφωνο ή το πραγματικό ταχυδρομείο. Τα υπεραστικά τηλεφωνήματα φουσκώνουν το λογαριασμό, ενώ η αποστολή ενός γράμματος με το ταχυδρομείο απαιτεί αρκετές μέρες μέχρι να φτάσει στον παραλήπτη. Αντίθετα, το ηλεκτρονικό ταχυδρομείο δεν κοστίζει περισσότερο από ένα τοπικό τηλεφώνημα και δεν χρειάζεται παρά λίγα λεπτά για να φτάσει στον προορισμό του, όποιος και αν είναι αυτός. Αυτοί οι δύο παράγοντες (το χαμηλό κόστος δηλαδή και η μεγάλη ταχύτητα παράδοσης) σε συνδυασμό με τη δυνατότητα

ανταλλαγής όχι μόνο μηνυμάτων αλλά και αρχείων κάθε είδους καθιέρωσαν το email ως αναγκαίο εργαλείο του σύγχρονου ανθρώπου.

Πολλοί άνθρωποι χρησιμοποιούν το Διαδίκτυο αποκλειστικά για να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο, χωρίς να ενδιαφέρονται για άλλες υπηρεσίες, ενώ είναι χαρακτηριστικό το γεγονός ότι ο αριθμός των «λογαριασμών» email αυξήθηκε την τελευταία πενταετία με γεωμετρική πρόοδο. Η σημερινή σύγχρονη μορφή του ηλεκτρονικού ταχυδρομείου καλύπτει κάθε δραστηριότητα. Δεν περιορίζεται μόνο σε προσωπικό επίπεδο, αλλά επεκτείνεται και στον επαγγελματικό τομέα. Εκτός από τα μηνύματα που μπορείτε να στείλετε στους φίλους σας, έχετε τη δυνατότητα να επικοινωνήσετε με οποιαδήποτε εταιρεία, οργανισμό, πανεπιστήμιο ή απλό ιδιώτη, που διαθέτει ηλεκτρονικό ταχυδρομείο, και να ζητήσετε πληροφορίες για προϊόντα, να στείλετε αιτήσεις, να ενημερωθείτε κ.λπ.

Τα λογισμικά, που έχουν αναπτυχθεί για να εξυπηρετήσουν τη χρήση του ηλεκτρονικού ταχυδρομείου, είναι εξαιρετικά εύκολα και απαιτούν ελάχιστο χρόνο για την εκμάθηση της χρήσης τους. Αυτό έχει ως αποτέλεσμα να χρησιμοποιούνται σήμερα από ανθρώπους που δεν έχουν ιδιαίτερη εξοικείωση με τους υπολογιστές. Τα περισσότερα από τα προγράμματα αυτά παρέχουν τεχνικές διευκολύνσεις για την επεξεργασία των μηνυμάτων, όπως η ταξινόμησή τους (ως προς το χρόνο, τον/την αποστολέα, το θέμα, κ.ά.), η εκτύπωση κάθε μηνύματος με τα στοιχεία παραλήπτη, αποστολέα, ημερομηνία, κ.ά., η δημιουργία λίστας διευθύνσεων, κ.λπ.

Τη χρησιμότητα του email αναγνώρισε πρόσφατα και επισήμως το ελληνικό δημόσιο, προσφέροντας τη δυνατότητα στους πολίτες να χρησιμοποιούν την ηλεκτρονική αλληλογραφία, για να συναλλάσσονται με διάφορες υπηρεσίες του.

Ηλεκτρονικό εμπόριο

Στο πρόσφατο παρελθόν οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα ο πωλήσεις των εμπόρων γίνονταν με καθαρά συμβατικά μέσα. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά. Ένας από τους νέους και τάχιστους τρόπους εξυπηρέτησης των καταναλωτών είναι το Ηλεκτρονικό Εμπόριο το οποίο αναπτύσσεται ραγδαία στο εξωτερικό αλλά και στην Ελλάδα με πιο αργούς όμως ρυθμούς.

Με απλά λόγια θα μπορούσαμε να πούμε πως ηλεκτρονικό εμπόριο είναι η αγοραπωλησία προϊόντων και υπηρεσιών μέσω του internet. Βέβαια, ένα θέλουμε να είμαστε πιο σωστοί με τον όρο ηλεκτρονικό εμπόριο (e-commerce) εννοείται κάθε εμπορική συναλλαγή, η οποία εκτελείται αποκλειστικά σε ηλεκτρονικό επίπεδο, δηλαδή με την χρήση ηλεκτρονικών υπολογιστών που συνδέονται μέσω τηλεφωνικών γραμμών.

Το ηλεκτρονικό εμπόριο εμφανίζεται με δύο τύπους δραστηριότητας και τέσσερις μορφές. Ως προς τους τύπους μπορεί κανείς να διακρίνει ανάμεσα στο έμμεσο ηλεκτρονικό εμπόριο και το άμεσο ηλεκτρονικό εμπόριο. Από την άλλη πλευρά οι πιο συνηθισμένες μορφές ηλεκτρονικού εμπορίου είναι : α) Επιχειρήσεις προς επιχειρήσεις, β) Επιχειρήσεις προς τους καταναλωτές, γ) Επιχειρήσεις προς τη δημόσια διοίκηση, δ) Τη δημόσια διοίκηση προς τους πολίτες.

Για πολύ καιρό τώρα μεγάλες επιχειρήσεις χρησιμοποιούν το ηλεκτρονικό εμπόριο για να διεξάγουν τις μεταξύ τους τις χρηματοοικονομικές συναλλαγές τους. Η ανταλλαγή ηλεκτρονικών δεδομένων (EDI) σε ιδιωτικά δίκτυα άρχισε το στη δεκαετία του 60 με πρώτες τις τράπεζες χρησιμοποιώντας ειδικά δίκτυα για ηλεκτρονική ανταλλαγή κεφαλαίων. Αν και πρόσφατα με την αυξανόμενη ενημερότητα και δημοτικότητα του Internet, το ηλεκτρονικό

εμπόριο έρχεται να κατακτήσει του καταναλωτές καθώς και τις επιχειρήσεις όλων των μεγεθών.

Το Internet έχει ήδη αλλάξει το τρόπο που διεξάγονται οι επιχειρηματικές δραστηριότητες. Όσο η επιρροή μεγαλώνει και περισσότερες επιχειρήσεις χρησιμοποιούν το Internet, τόσο οι πιθανότητες για ανάπτυξη και διεξαγωγή ηλεκτρονικών συναλλαγών μεταξύ επιχειρήσεων θα εξαπλωθούν, και θα γίνει σαν κάτι το συνηθισμένο και σαν αναπόσπαστο κομμάτι του εμπορίου.

Η ανάγκη για Ηλεκτρονικό εμπόριο προκύπτει από την απαίτηση των επιχειρήσεων για καλύτερη χρήση της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών ώστε να βελτιωθούν οι σχέσεις αμφίδρομης επικοινωνίας με τους καταναλωτές. Η τεχνολογία και ειδικότερα το Ηλεκτρονικό Εμπόριο παρέχει ευέλικτες και ολοκληρωμένες λύσεις τοποθέτησης των επιχειρήσεων στις επιθυμητές αγορές (target markets) παρεμβαίνοντας ευεργετικά σε κάθε στάδιο της αλυσίδας αξίας τους (value chain). Το Internet ήταν αυτό που έδωσε μεγάλη ώθηση στην ανάπτυξη του ηλεκτρονικού εμπορίου.

ΚΕΦΑΛΑΙΟ 1

1.1 Ορισμός spam

Η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) αποτελεί μία από τις πιο χρήσιμες και δημοφιλείς υπηρεσίες που προσφέρει το Διαδίκτυο. Όλοι όσοι χρησιμοποιούν αυτή την υπηρεσία έρχονται κάποια στιγμή αντιμέτωποι με το λεγόμενο spam.

Με τον όρο **«spam»** χαρακτηρίζεται η αποστολή μεγάλου αριθμού μηνυμάτων με εμπορικό περιεχόμενο που έχουν σαν στόχο την διαφήμιση κάποιων προϊόντων ή υπηρεσιών, τα οποία καταλήγουν στην ηλεκτρονική θυρίδα των παραληπτών, χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα.

Μπορεί επίσης να είναι πολλές δημοσιεύσεις του ίδιου μηνύματος σε ομάδες συζήτησης ή σε διακομιστές λίστας που δεν έχουν σχέση με το θέμα του μηνύματος.

Η ανεπιθύμητη αλληλογραφία δεν περιορίζεται μόνο στα μηνύματα με εμπορικό περιεχόμενο καθώς πολλές φορές διευκολύνει απάτες, προσφέρει πορνογραφικό υλικό ή περιέχει επικίνδυνα αρχεία, επιφυλάσσοντας έτσι κινδύνους στους χρήστες.

Άλλοι όροι που χρησιμοποιούνται στο Internet για το spam είναι «Αυτόκλητα Εμπορικά Email» (Unsolicited Commercial Email -UCE) και «Αυτόκλητη Ενοχλητική Αλληλογραφία» (Unsolicited Bulk Email - UBE), μορφές email όμοιες με το spam καθώς και «junk e-mail» ή «Bulk e-mail».

Τέλος, να αναφέρουμε πως χρησιμοποιώντας τον όρο «spamming» εννοούμε την διαδικασία της αποστολής της ανεπιθύμητης αλληλογραφίας από τους λεγόμενους «spammers».

Ένα μήνυμα το οποίο συντάσσεται και αποστέλλεται σε κάποιον, τον οποίο γνωρίζει ο αποστολέας, δεν είναι spam. Το spamming απαγορεύεται από τη Δεοντολογία του Internet (Netiquette) και από τις νομοθεσίες των

περισσότερων ευρωπαϊκών κρατών, καθώς αντιτίθεται σε μεγάλο βαθμό στην προστασία των καταναλωτών και των προσωπικών τους δεδομένων και ενέχει κινδύνους όσον αφορά την ασφάλεια των δικτύων. Πολλοί δικτυακοί τόποι είτε το απαγορεύουν ρητά είτε επιλέγουν να μην δέχονται κανένα e-mail με αυτή την προέλευση.

Εικόνα 1

1.2 Ιστορία του spam

Ενδιαφέρον παρουσιάζει η προέλευση του όρου «spam». Spam ονομάζεται μια κονσέρβα κρέατος, το οποίο αποτέλεσε το κύριο φαγητό του Βρετανικού στρατού από τον Β΄ Παγκόσμιο πόλεμο και μετά. Η ονομασία αυτή προέρχεται από τον συνδυασμό των λέξεων «Spiced» και «Ham» που σημαίνουν πικάντικο ζαμπόν. Η υπερπροσφορά του spam σατιρίζεται σε ένα σκετς που έκαναν οι γνωστοί Βρετανοί κωμικοί ‘Monty Python’s’, παρουσιάζοντας ένα ζευγάρι που προσπαθεί να δώσει παραγγελία σε ένα εστιατόριο για να διαπιστώσει πως όλο το μενού του καταστήματος περιέχει spam, δηλαδή συσκευασμένο κρέας σε κονσέρβα από την εταιρία Hormed Foods.

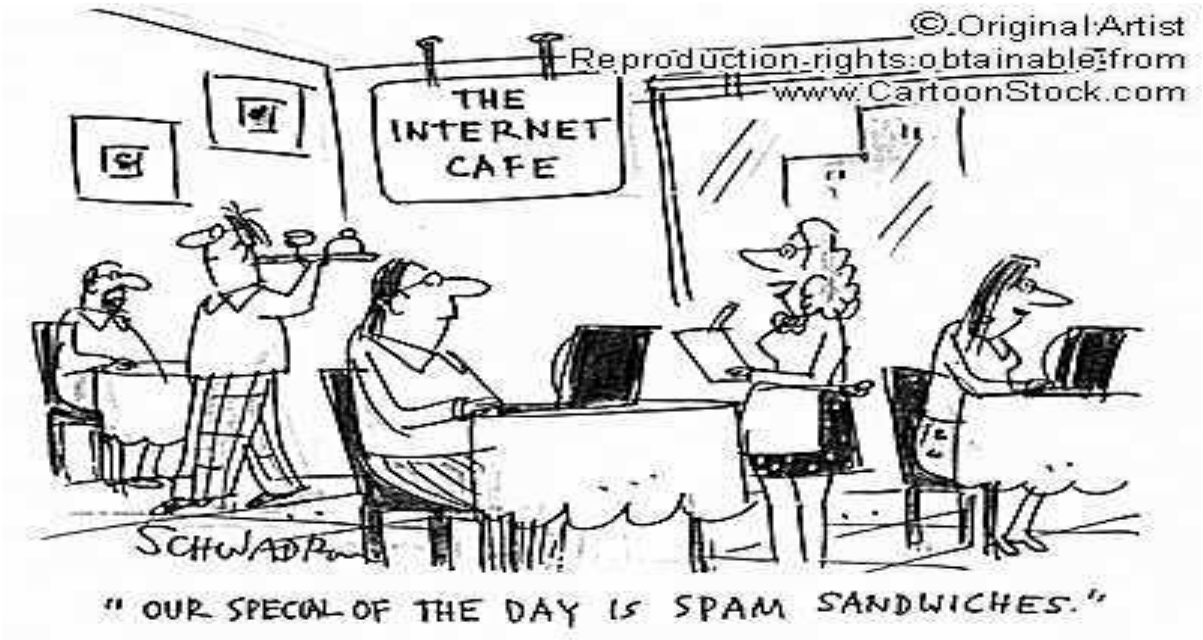
Παρόλο που το σκετς είναι μικρό σε διάρκεια, η λέξη spam ακούγεται τουλάχιστον 94 φορές παράλληλα με το παίξιμο ενός τραγουδιού από μια παρέα Βίκινγκς για το αγαπημένο τους φαγητό, το spam.

Ο κορεσμός της εποχής από το spam συσχετίστηκε με το σύγχρονο φαινόμενο του spam και ο όρος αυτός υιοθετήθηκε για να δηλώσει την δυσαρέσκεια των χρηστών του Διαδικτύου για την υπερφόρτωση του ηλεκτρονικού τους ταχυδρομείου από τα ανεπιθύμητα μηνύματα.

Η συσχέτιση αυτή προκάλεσε την αντίδραση της εταιρίας Hormed Foods, που εισήγαγε την κονσέρβα με το spam στην αγορά από το 1937. Κάθε προσπάθεια που έκανε η εταιρία για να σταματήσει την χρήση του όρου αυτού δεν απέδωσε και συμβιβάστηκε στην διάκριση μεταξύ του ‘spam’ με πεζούς χαρακτήρες που δηλώνει την ανεπιθύμητη αλληλογραφία και του ‘SPAM’ με κεφαλαίους χαρακτήρες που προσδιορίζουν το συγκεκριμένο προϊόν της.

Η πρώτη εμφάνιση του spam έγινε το 1978 αλλά παρέμεινε σχετικά ανενεργό μέχρι το 1994 όπου έχουμε τις πρώτες προσεγγίσεις spam με σκοπό το οικονομικό κέρδος (commercial spam).

Το 1978,την εποχή που λειτουργούσε το ARPANET, η εταιρία DEC,που σήμερα αποτελεί τμήμα της Hewlett-Packard, έστειλε προσκλήσεις σε όλες τις ηλεκτρονικές διευθύνσεις της δυτικής ακτής των Ηνωμένων Πολιτειών της Αμερικής για την παρουσίαση του νέου της μοντέλου ηλεκτρονικού υπολογιστή. Ωστόσο, η πρακτική αυτή θεωρήθηκε πως παραβίαζε τους κανόνες χρήσης του ARPANET και στάλθηκε απάντηση σε όλους τους χρήστες προκειμένου να τους υπενθυμίσει την υποχρέωση που έχουν να σέβονται το Διαδίκτυο και τους υπόλοιπους χρήστες του.



Εικόνα 2

1.3 Χαρακτηριστικά του spam

Τα βασικότερα χαρακτηριστικά του spam επικεντρώνονται στα εξής τρία σημεία.

Καταρχάς, το Spam χαρακτηρίζεται ως **απρόκλητο,** γιατί δεν υπάρχει κάποια σχέση ανάμεσα σε παραλήπτες και αποστολέα ώστε να δικαιολογείται ή να προκαλείται μία τέτοιου είδους επικοινωνία.

Χαρακτηρίζεται ως **εμπορικό,** διότι τα μηνύματα αυτά αφορούν τις περισσότερες φορές την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

Τέλος, χαρακτηρίζεται και ως **μαζικό,** αφού τα μηνύματα στέλνονται μαζικά από τον αποστολέα σε ένα μεγάλο πλήθος παραληπτών. Συνήθως, το ίδιο μήνυμα ή κάπως διαφοροποιημένο στέλνεται σε μεγάλο πλήθος παραληπτών.

Ωστόσο, εκτός από τα παραπάνω χαρακτηριστικά υπάρχουν και κάποια επιπλέον, όπως:

♦ Δεν υπάρχει η δυνατότητα της διαγραφής από τις λίστες του παραληπτών που έχουν στην κατοχής τους οι αποστολείς. Σε περίπτωση, βέβαια που γίνει διαγραφή, αυτό λειτουργεί ως επιβεβαίωση ότι υπάρχει η συγκεκριμένη ηλεκτρονική διεύθυνση.

♦ Η αποστολή αυτών των μηνυμάτων γίνεται με την χρήση κάποιων τεχνικών, οι οποίες έχουν στόχο την απόκρυψη της πραγματικής ταυτότητας του αποστολέα.

♦ Δεν υπάρχει μία έγκυρη ηλεκτρονική διεύθυνση του αποστολέα του διαφημιστικού μηνύματος για την πραγματοποίηση επικοινωνίας μαζί του.

♦ Στέλνονται χωρίς διάκριση, με αυτοματοποιημένα μέσα.

♦ Περιλαμβάνει ή προωθεί, αρκετές φορές παράνομο ή δυσάρεστο περιεχόμενο.

♦ Το περιεχόμενο αυτών των μηνυμάτων μπορεί να είναι ψευδές ή παραπλανητικό και τέλος

♦ Οι διευθύνσεις των παραληπτών έχουν αποκτηθεί με λογισμικό ανίχνευσης στο Διαδίκτυο για συλλογή ηλεκτρονικών διευθύνσεων (οι λεγόμενες ‘αράχνες’) ή μπορεί να έχουν αγοραστεί από εταιρίες που παράγουν cd με τέτοιου είδους περιεχόμενο έναντι μικρού κόστους.

1.4 Βασικά γνωρίσματα του spam

Τα μηνύματα spam γίνονται αντιληπτά από κάποια βασικά γνωρίσματα, τα οποία αφορούν τόσο το περιεχόμενο των μηνυμάτων αυτών όσο και την κεφαλίδα τους.

Το κείμενο, όπως έχει ήδη αναφερθεί, περιέχει κυρίως διαφημιστικό περιεχόμενο με σκοπό την προώθηση προϊόντων ή υπηρεσιών από επιχειρήσεις με τις οποίες οι παραλήπτες δεν έχουν καμία συναλλαγή και τις περισσότερες φορές, τις αγνοούν παντελώς. Πολλές φορές, τα μηνύματα αυτά περιέχουν

διάφορους συνδέσμους (links) οι οποίοι παραπέμπουν τους παραλήπτες σε κάποια άλλη ιστοσελίδα με σκοπό α) να δηλώσουν πως είναι αντίθετοι στην λήψη τέτοιων μηνυμάτων στην ηλεκτρονική τους διεύθυνση ή β) για περισσότερες πληροφορίες για το προϊόν ή την υπηρεσία που διαφημίζεται. Στις περισσότερες περιπτώσεις όμως, η επιλογή τέτοιου είδους συνδέσμου καθώς και μία απάντηση από τους χρήστες προς αυτό το σύνδεσμο, απλώς επιβεβαιώνει τις ενεργείς ηλεκτρονικές διευθύνσεις των χρηστών και γίνονται στόχοι για την αποστολή περισσότερων spam e-mail μελλοντικά.

Όσο αφορά την κεφαλίδα αυτών των μηνυμάτων, δηλαδή το τμήμα που δίνει πληροφορίες σχετικά με το θέμα, τον αποστολέα, τους παραλήπτες, παρατηρείται ότι η ηλεκτρονική διεύθυνση είτε ότι δεν υπάρχει και είναι φανταστική είτε ότι έχει δημιουργηθεί μόνο για να χρησιμοποιηθεί στην αποστολή των spam.

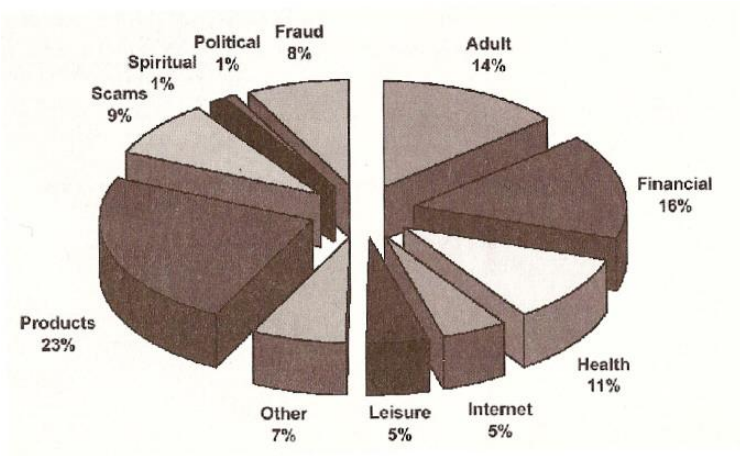
Ενδεικτικό είναι και το θέμα του μηνύματος spam. Προκειμένου, να κεντρίσουν το ενδιαφέρον των παραληπτών, οι spammers χρησιμοποιούν φράσεις οι οποίες υπόσχονται κέρδη, προτάσεις γνωριμίας, δωρεάν πορνογραφικό υλικό κ.ο.κ. Πολλές φορές, στη γραμμή του θέματος υπάρχει και η λέξη «Re:» προκειμένου να πεισθούν οι παραλήπτες πως πρόκειται για απάντηση σε e-mail που είχαν στείλει. Φράσεις που χρησιμοποιούνται συχνά ως θέμα είναι «Επείγουσα Ανακοίνωση», «Ακύρωση συνάντησης », «Έκτακτη Ειδοποίηση» κ.λ.π.

Σύμφωνα με τα παραπάνω, γίνεται φανερό πως οι spammers βασίζονται σε πολύ μεγάλο βαθμό στην αφέλεια ορισμένων χρηστών ανάμεσα στον μεγάλο αριθμό παραληπτών ανεπιθύμητων μηνυμάτων που υπάρχει.

1.5 Είδη spam

Στην έννοια του spam δεν συγκαταλέγονται μόνο τα εμπορικά μηνύματα αλλά μπορεί το περιεχόμενό τους να είναι και πολιτικού, θρησκευτικού, ιδεολογικού, κοινωνικού χαρακτήρα κλπ.

Το παρακάτω διάγραμμα δείχνει σε τι ποσοστό δέχονται οι χρήστες του Διαδικτύου μηνύματα spam, ως προς το περιεχόμενό τους.



Διάγραμμα 1

Στην συνέχεια, παρουσιάζονται τα βασικότερα είδη των μηνυμάτων spam.

1.5.1 Αλυσιδωτά e-mail

Ένα από τα είδη του spam είναι τα **αλυσιδωτά e-mail**, γνωστά ως **hoaxes**, τα οποία ποικίλλουν στο περιεχόμενό τους. Μπορεί να είναι παραδείγματος χάρη προειδοποίηση για επικίνδυνους ιούς, έκκληση βοήθειας για κάποιο κοινωνικό πρόβλημα, προτάσεις φορολόγησης των δεδομένων που διακινούνται μέσω του Διαδικτύου. Τα μηνύματα αυτά προτρέπουν τους παραλήπτες να στείλουν με την σειρά τους σε μεγάλο αριθμό ατόμων, με μοναδικό δέλεαρ κάποιο χρηματικό έπαθλο ή μια υπόσχεση καλοτυχίας.

Ο όρος hoax χρησιμοποιείται για να περιγράψει κάτι ψεύτικο ή μια απάτη. Πιο ακριβής όμως είναι ο όρος Urban Legend (Αστικός Θρύλος) αφού ένα Hoax είναι στην πραγματικότητα μια φήμη, δηλαδή ένας θρύλος ο οποίος "περιφέρεται" μέσα στο δίκτυο.

Ωστόσο, υπάρχουν τρόποι με τους οποίους μπορούμε να καταλάβουμε αν το μήνυμα που λαμβάνουμε είναι πραγματικό ή απλώς αποτελεί ένα θρύλο του Διαδικτύου. Τρόποι αναγνώρισης είναι οι εξής:

- **Τεχνική Διάλεκτος**: Για να γίνουν πιο αξιόπιστα αυτά τα μηνύματα χρησιμοποιούν επιστημονικούς ή τεχνικούς όρους, οι οποίοι με την πρώτη ανάγνωση φαίνονται σοβαροί, αλλά στην πραγματικότητα δεν σημαίνουν τίποτα.
- **Επίκληση μιας αξιόπιστης πηγής**: Για να αυξήσουν την αξιοπιστία τους, τα hoaxes υποστηρίζουν πως αποτελούν μηνύματα, τα οποία στέλνουν μεγάλοι οργανισμοί όπως είναι η Microsoft. Όμως, αυτοί οι οργανισμοί δημοσιεύουν πάντα τις ανακοινώσεις τους στον Τύπο και δεν εμπιστεύονται εύκολα το e-mail,το οποίο μπορεί και να παραποιηθεί.
- **Προτροπή προώθησης του ίδιου μηνύματος σε τρίτους:** Αυτό είναι το σήμα κατατεθέν των Αστικών Θρύλων. Όποτε κάποιο μήνυμα ζητά να προωθηθεί, είναι σίγουρα μήνυμα hoax.
- **Αδυναμία ελέγχου:** Αν το θέμα του μηνύματος είναι σημαντικό, ο αποστολέας θα έχει δημιουργήσει τουλάχιστον μια web σελίδα με περισσότερες πληροφορίες σχετικά με αυτό. Αν αυτή δεν αναφέρεται στο mail ή αν η διεύθυνσή της είναι "ύποπτη" σημαίνει πως το μήνυμα δεν ανταποκρίνεται στην πραγματικότητα.

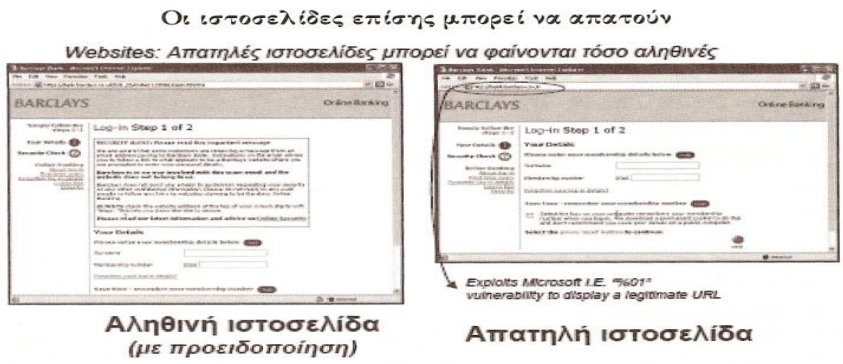
Άλλες τεχνικές αναγνώρισης των Hoaxes είναι ο εκφοβισμός ή η χρήση συγκεκαλυμμένων απειλών, η κακή σύνταξη και ορθογραφία (κολλημένες λέξεις, πολλά κεφαλαία), κ.λπ.

1.5.2 Μηνύματα με σκοπό το Phishing

Ένα είδος ανεπιθύμητου email που εμφανίζεται όλο και πιο συχνά είναι το phishing (ηλεκτρονικό ψάρεμα).

Το phishing είναι ένα μήνυμα που αποστέλλεται σε όσες ηλεκτρονικές διευθύνσεις μπορεί να αποκτήσει ο εγκέφαλος της απάτης και φαίνεται ότι προέρχεται από αξιόπιστους οργανισμούς όπως τράπεζες, υπηρεσίες ηλεκτρονικών πληρωμών, ηλεκτρονικά καταστήματα, κλπ. Το μήνυμα αυτό ζητά από τον παραλήπτη να ενημερώσει ή να επαληθεύσει τα προσωπικά και οικονομικά του στοιχεία, όπως ημερομηνία γέννησης, στοιχεία σύνδεσης, στοιχεία λογαριασμού, αριθμούς πιστωτικών καρτών, PIN, κλπ.

Ορισμένα μηνύματα απειλούν ότι σε περίπτωση που δεν γίνει ενημέρωση ή επαλήθευση των στοιχείων, ο λογαριασμός μπορεί, για παράδειγμα, να δεσμευτεί. Ο σκοπός τους είναι να πείσουν τους ανυποψίαστους παραλήπτες, που τυχαίνει να είναι πελάτες του αξιόπιστου οργανισμού που μιμούνται, να απαντήσουν στο μήνυμα και να αποκαλύψουν τις πληροφορίες που τους ζητούν.



Εικόνα 3

Το μήνυμα περιλαμβάνει μια σύνδεση που οδηγεί τους χρήστες σε μια ιστοσελίδα, η οποία είναι παρόμοια με την πραγματική ιστοσελίδα του οργανισμού. Κάποιες φορές, όταν κάνετε κλικ στη σύνδεση του μηνύματος, μπαίνετε στην πραγματική ιστοσελίδα, η οποία όμως καλύπτεται από ένα μικρότερο παράθυρο με την ιστοσελίδα "μαϊμού", ώστε να γίνεται πιο πιστευτή. Κάνοντας κλικ στη σύνδεση, υπάρχει κίνδυνος να κατεβάσετε στον υπολογιστή σας ύποπτα λογισμικά, γνωστά ως "spyware", τα οποία καταγράφουν τις ενέργειές σας στο Internet και ενδεχομένως παρακολουθούν τις πληκτρολογήσεις σας και διαβιβάζουν τις πληροφορίες αυτές στον εγκέφαλο της απάτης. Οι εγκέφαλοι της απάτης χρησιμοποιούν αυτά τα οικονομικά στοιχεία, εκθέτοντας σε κίνδυνο τραπεζικούς λογαριασμούς, πιστωτικές κάρτες, κλπ.

Μόλις οι εγκέφαλοι της απάτης συγκεντρώσουν τα οικονομικά στοιχεία ατόμων μέσω phishing, είναι σε θέση να καταχραστούν τα στοιχεία αυτά και να υποκλέψουν χρήματα από τους εκτεθειμένους λογαριασμούς. Για να καλύψουν όμως τα ίχνη τους, αναθέτουν σε ανυποψίαστα άτομα να παίξουν το ρόλο μεσολαβητών, δημοσιεύοντας διάφορες δελεαστικές αγγελίες εργασίας στο Internet που υπόσχονται στους ενδιαφερόμενους ότι θα κερδίσουν χρήματα γρήγορα και με λίγη προσπάθεια. Τα άτομα αυτά είναι γνωστά ως «mules».

Οι τραπεζικοί λογαριασμοί των mules χρησιμοποιούνται για την παραλαβή εμβασμάτων από τους εκτεθειμένους λογαριασμούς. Στη συνέχεια, τους ζητείται να αποσύρουν τα χρήματα από το λογαριασμό τους σε μετρητά και να τα αποστείλουν στους εγκέφαλους της απάτης, μείον την προμήθειά τους, χρησιμοποιώντας μια υπηρεσία διεθνών εμβασμάτων. Οι εγκέφαλοι της απάτης διατηρούν έτσι την ανωνυμία τους, αφήνοντας εκτεθειμένους τους phishing mules, τους οποίους μπορούν να παρακολουθήσουν οι αρχές.

1.5.3 Διαδικτυακές Αιτήσεις

Αυτές οι αιτήσεις ζητούν από τους παραλήπτες να τις προωθήσουν και σε άλλους αποδέκτες, κρατώντας συγχρόνως τις ηλεκτρονικές τους διευθύνσεις. Στον τελευταίο αποδέκτη που θα συμπληρώσει τις αιτήσεις, θα ζητηθεί να στείλει αυτές τις αιτήσεις στον αρχικό αποστολέα.

Με αυτόν τον τρόπο, οι αποστολείς τέτοιου είδους spam επιβεβαιώνουν όλες τις υπάρχουσες ηλεκτρονικές διευθύνσεις με ένα μόνο μήνυμα, στις οποίες μετά μπορούν να στείλουν νέα ανεπιθύμητα μηνύματα.

1.5.4 Συμβουλές για τον υπολογιστή

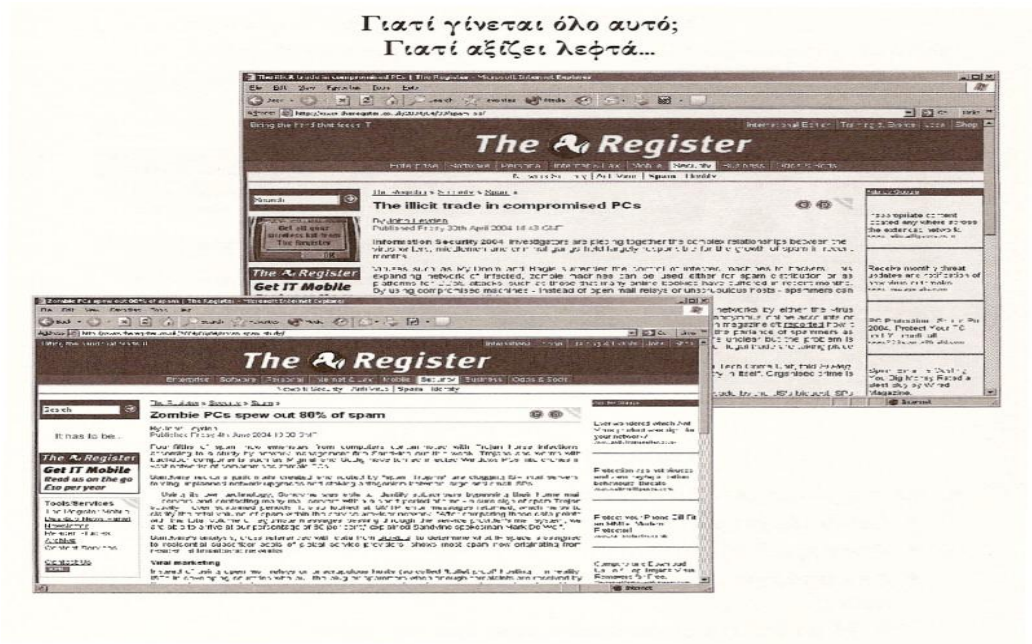
Πρόκειται για υποτιθέμενες φιλικές συμβουλές που έχουν σκοπό την ασφάλεια του υπολογιστή από διάφορους κινδύνους όπως είναι κάποια επικίνδυνα αρχεία που υπάρχουν ήδη τον υπολογιστή. Ενώ στην πραγματικότητα, αυτά τα αρχεία είναι ακίνδυνα η διαγραφή τους από τον υπολογιστή θα προκαλέσει σοβαρά προβλήματα στην μετέπειτα λειτουργία του.

Έτσι πολλοί χρήστες πιστεύοντας πως αυτά τα συμβουλευτικά e-mail είναι χρήσιμα, τα προωθούν σε γνωστούς τους. Γι’αυτό τον λόγο πρέπει όλοι οι παραλήπτες να είναι προσεκτικοί όταν δέχονται τέτοιου είδους μηνύματα.

1.6 Spammers

Τα μηνύματα spam προέρχονται από τους λεγόμενους spammers. Πρόκειται για μία ομάδα χρηστών, οι οποίοι κατέχουν άριστα την τεχνολογία και χρησιμοποιούν ανεπτυγμένο και σύγχρονο λογισμικό για την υλοποίηση των στόχων τους. Σύμφωνα με έρευνες που έχουν γίνει, το 90 % των spam που παράγονται σε παγκόσμιο επίπεδο προέρχεται από 200 ομάδες spammers ενώ το υπόλοιπο 10% από μικρότερες επιχειρήσεις.

Το spamming για τους spammers αποτελεί τη μεγαλύτερη ανακάλυψη μετά τον τροχό (…) κι αυτό γιατί μπορούν να κατακλύσουν ολόκληρη την υφήλιο με δισεκατομμύρια e-mail μέσα σε ελάχιστο χρόνο, με ελάχιστα χρήματα! Με τον τρόπο αυτό, ακόμα κι αν ένα πολύ μικρό ποσοστό (πολύ κάτω του 1%) ανταποκριθεί στο κάλεσμά τους, τους αποφέρει τεράστια **κέρδη**, χωρίς ιδιαίτερη προσπάθεια.



Εικόνα 4

1.7 Τεχνικές που οδηγούν στο spam

Οι spammers για να αποφύγουν τις νομικές επιπτώσεις των πράξεών τους, στέλνουν τα μηνύματα spam από ενδιάμεσα συστήματα ηλεκτρονικών υπολογιστών, στα οποία έχουν αποκτήσει πρόσβαση χωρίς να το γνωρίζουν οι νόμιμοι διαχειριστές τους.

Για να καταφέρουν να αποκτήσουν πρόσβαση σε αυτά τα συστήματα, χρησιμοποιούν τεχνικές όπως είναι:

- Hacking: Οι spammers, έχοντας προχωρημένες γνώσεις για τα λειτουργικά περιβάλλοντα, εισέρχονται στα ενδότερα του υπολογιστικού συστήματος και χρησιμοποιούν τους πόρους του πχ για την αποστολή ηλεκτρονικών μηνυμάτων, σαν να ήταν οι νόμιμοι χρήστες.
- IP Spoofing: είναι μία τεχνική με την οποία δημιουργούνται TCP/IP πακέτα δεδομένα, τα οποία χρησιμοποιούν άλλη IP διεύθυνση αποστολέα και όχι αυτή από την οποία πραγματικά στέλνονται. Έτσι, οι routers (δρομολογητές) λαμβάνουν υπόψη μόνο την IP διεύθυνση «προορισμού» και όχι την IP διεύθυνση «προέλευσης». Η διεύθυνση προέλευσης θα αποκωδικοποιηθεί και θα παρουσιαστεί μόνο στον τελικό προορισμό ώστε αν χρειαστεί απάντηση να είναι γνωστή η διεύθυνση του αποστολέα.
- Packet sniffing: η τεχνική αυτή επιτρέπει την παρακολούθηση των πακέτων πληροφορίας που κινούνται σε ένα δίκτυο. Στα μη κωδικοποιημένα πακέτα υπάρχει ο κίνδυνος αποκάλυψης ευαίσθητων πληροφοριών των χρηστών όπως είναι διάφορα passwords, e-mails. Για την αντιμετώπιση αυτού του προβλήματος προτείνεται ως λύση η κωδικοποίηση των πληροφοριών.

- Phishing: πρόκειται για μια τεχνική κατά την οποία δημιουργείται ένας παράνομος δικτυακός τόπος, ο οποίος όμως μιμείται σε συμπεριφορά έναν νόμιμο. Έτσι, οι χρήστες επισκεπτόμενοι τον παράνομο δικτυακό τόπο και πιστεύοντας πως κάνουν συναλλαγές με τον πραγματικό δικτυακό τόπο, αποκαλύπτουν διάφορα προσωπικά δεδομένα όπως στοιχεία πιστωτικών καρτών, τραπεζικούς λογαριασμούς κ.α.
- Harassment (Παρενόχληση): έχει σχέση με την αποστολή άσεμνων, προσβλητικών ηλεκτρονικών μηνυμάτων σε πρόσωπα ή ομάδες χρηστών.
- Spam filtering: είναι λογισμικό το οποίο χρησιμοποιείται για να φιλτράρει την διάδοση των μηνυμάτων spam κατά την λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Ωστόσο, οι spammers χρησιμοποιούν και τεχνικές για την συλλογή ηλεκτρονικών διευθύνσεων καθώς και για την αποστολή του εκάστοτε περιεχομένου.

Για την συλλογή των ηλεκτρονικών διευθύνσεων χρησιμοποιούν πολλές μεθόδους, ορισμένες από τις οποίες είναι:

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

Οι spammers χρησιμοποιούν ειδικά προγράμματα με τα οποία ψάχνουν σε διάφορους διαδικτυακούς τόπους για την εύρεση ηλεκτρονικών διευθύνσεων. Ορισμένα από αυτά τα προγράμματα ψάχνουν τις ηλεκτρονικές διευθύνσεις στην κεφαλίδα του e-mail,στο σημείο δηλαδή που υπάρχουν οι φράσεις '**From:**' ή '**Reply to**' ενώ άλλα προγράμματα ψάχνουν στο κύριο μέρος των e-mail για την χρήση υπογραφών ή για οτιδήποτε περιέχει το σύμβολο '**@**'.

- **Από λίστες με ηλεκτρονικές διευθύνσεις**

Οι spammers προσπαθούν να πάρουν τις λίστες με τις διευθύνσεις από διάφορους συνδρομητές αφού γνωρίζουν πως οι περισσότερες από τις διευθύνσεις είναι έγκυρες.

Μία ακόμα μέθοδο που χρησιμοποιούν οι spammers είναι να ζητήσουν από κάποιον εξυπηρετητή (server) να τους δώσει την λίστα με τις διευθύνσεις τους (μέθοδος η οποία χρησιμοποιείται συχνά από κάποιους εξυπηρετητές για την ευκολία των νόμιμων χρηστών) και στην συνέχεια να στείλουν αυτοί τα μηνύματα spam σε αυτά τα e-mail.

- **Από Ιστοσελίδες**

Χρησιμοποιούνται αυτοματοποιημένα προγράμματα (spiders), τα οποία ανιχνεύουν τις ιστοσελίδες για διευθύνσεις π.χ. για διευθύνσεις που μπορεί να περιέχονται σε κεφαλίδα της Html.

- **Από sites** τα οποία ζητούν πολλές πληροφορίες μέσω φορμών που χρησιμοποιούν όπως για παράδειγμα σελίδες που ζητούν εγγραφή. Οι spammers μπορούν να βρουν αυτές τις διευθύνσεις είτε γιατί αυτές οι φόρμες είναι διαθέσιμες στο Παγκόσμιο Ιστό είτε γιατί το site πωλεί ή δίνει την λίστα των διευθύνσεων σε άλλους.

- **Από λογισμικά πλοήγησης (web browsers)**

Πολλές φορές, ορισμένα sites προσπαθούν να αποσπάσουν την διεύθυνση του χρήστη καθώς πλοηγείται στο Διαδίκτυο από τον web server, χωρίς ο ίδιος ο χρήστης να το καταλαβαίνει. Ορισμένες τεχνικές που χρησιμοποιούνται για αυτό τον σκοπό είναι:

1. Η χρήση της κεφαλίδας Http_From που τα web browsers στέλνουν στους εξυπηρετητές. Ορισμένοι browsers στέλνουν και μια κεφαλίδα μαζί με

την διεύθυνση του e-mail σε κάθε server (εξυπηρετητή) που επισκέπτονται οι χρήστες,

2. Κάνοντας τον browser να στείλει μια εικόνα της ιστοσελίδας σε ένα ανώνυμο FTP (ανώνυμο πρωτόκολλο μεταφοράς αρχείων) στην ίδια ιστοσελίδα. Ορισμένοι browsers θα μπορούσαν να δώσουν την ηλεκτρονική διεύθυνση του χρήστη ως κωδικό σε αυτό τον ανώνυμο FTP λογαριασμό, ότι δηλαδή έχει εγγραφεί ως μέλος με αυτούς τους κωδικούς. Ο χρήστης ο οποίος δεν είναι ενήμερος με αυτή την τεχνική, δεν θα μπορέσει να καταλάβει ότι έχει παραβιαστεί η ηλεκτρονική του διεύθυνση.

- **Από IRC και chat rooms:**

Πολλοί IRC (Διεθνής Φορέας Εκμετάλλευσης) πελάτες μπορούν να δώσουν τις ηλεκτρονικές διευθύνσεις των χρηστών σε οποιοδήποτε τις ζητήσει. Έτσι, οι spammers παίρνουν τις ηλεκτρονικές διευθύνσεις και γνωρίζοντας πως είναι νόμιμες και ισχύουν, στέλνουν τα μηνύματα spam.

Οι χώροι επικοινωνίας, γνωστά και ως chat rooms, αποτελούν επίσης πηγή εύρεσης ηλεκτρονικών διευθύνσεων ειδικότερα όταν εγγράφονται νέοι χρήστες, οι οποίοι δεν έχουν μεγάλη εμπειρία στην αντιμετώπιση των spam μηνυμάτων και έτσι οι spammers μπορούν εύκολα να βρουν τις ηλεκτρονικές τους διευθύνσεις.

Τέλος, πολλές φορές οι spammers επιστρατεύουν και την **τύχη** τους, δοκιμάζοντας για κάθε domain που θέλουν να στείλουν μηνύματα spam, πιθανούς αλλά και λογικούς παραλήπτες. Στέλνουν δηλαδή κάποιο μήνυμα σε λίστα από διευθύνσεις, τις οποίες έχουν οι ίδιοι επινοήσει, και περιμένουν να τους σταλεί μήνυμα με επιβεβαίωση για το αν ισχύουν ή όχι οι διευθύνσεις αυτές.

Για την αποστολή του περιεχομένου, χωρίς αυτό να μπορεί να εμποδιστεί από τους μηχανισμούς αντιμετώπισης του spam, χρησιμοποιούνται **ψεύτικα και συνεχώς μεταβαλλόμενα στοιχεία αποστολέα (**spoofed e-mail addresses),

περιεχόμενο που έχει ενσωματωθεί σε εικόνες, περιεχόμενο ως attachment, τροποποιημένες λέξεις και πολλές άλλες τεχνικές.

Εικόνα 5

1.8 Η έκταση του spam

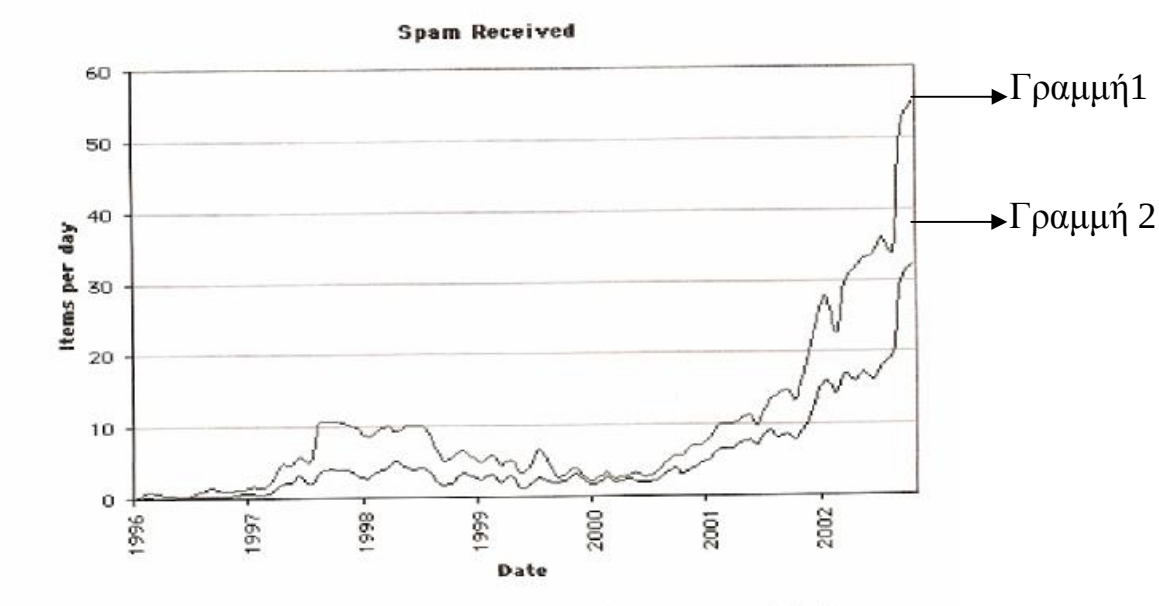
Στατιστικές μελέτες που έγιναν το 2004, συγκεκριμένα στο συνέδριο Internet Measurement Conference που έγινε στην Σικελία, έδειξαν μεγάλη αύξηση στην διακίνηση των μηνυμάτων spam. Υπάρχει μία επιφύλαξη σχετικά με την ακρίβεια των στατιστικών προβλέψεων, με αποτέλεσμα τα νούμερα που έχουν καταγραφεί και αφορούν την διακίνηση spam να είναι ενδεικτικά για το μέγεθος του προβλήματος.

Σύμφωνα με τις μελέτες αυτές, η διακίνηση των μηνυμάτων spam έχει αυξηθεί κατά 1.000% τα τελευταία δύο χρόνια. Επίσης, έχουν εξαχθεί τα εξής συμπεράσματα:

- Ένας μέσος χρήστης του διαδικτύου, λαμβάνει καθημερινά 6 μηνύματα spam. Από αυτά τα μηνύματα, το 24% αφορά απάτες, το 23% προώθηση προϊόντων, το 19% αφορά πορνογραφικά μηνύματα, το 11% αφορά ιατροφαρμακευτικά σκευάσματα και το 1% αφορά πολιτικό περιεχόμενο.
- Το 8% των χρηστών έχει αγοράσει προϊόντα που προωθούνται με αυτά τα μηνύματα.

- Το 28% των χρηστών έχει απαντήσει σε μηνύματα spam ή έχει συμμετάσχει σε πηγές εκπόρευσης τεχνικών προώθησης όπως είναι οι on-line δημοσκοπήσεις.

Στο σχήμα που ακολουθεί, απεικονίζεται η εξέλιξη της διακίνησης των μηνυμάτων spam.



Στο παραπάνω διάγραμμα παρουσιάζεται η διακίνηση των μηνυμάτων spam έως το έτος 2002. Η πρώτη γραφική παράσταση (γραμμή 1) δείχνει τα μηνύματα spam που στάλθηκαν προς όλους τους αποδέκτες του δείγματος ενώ η δεύτερη γραφική παράσταση (γραμμή 2) δείχνει τα μηνύματα spam που στάλθηκαν σε επιλεγμένους χρήστες του δείγματος.

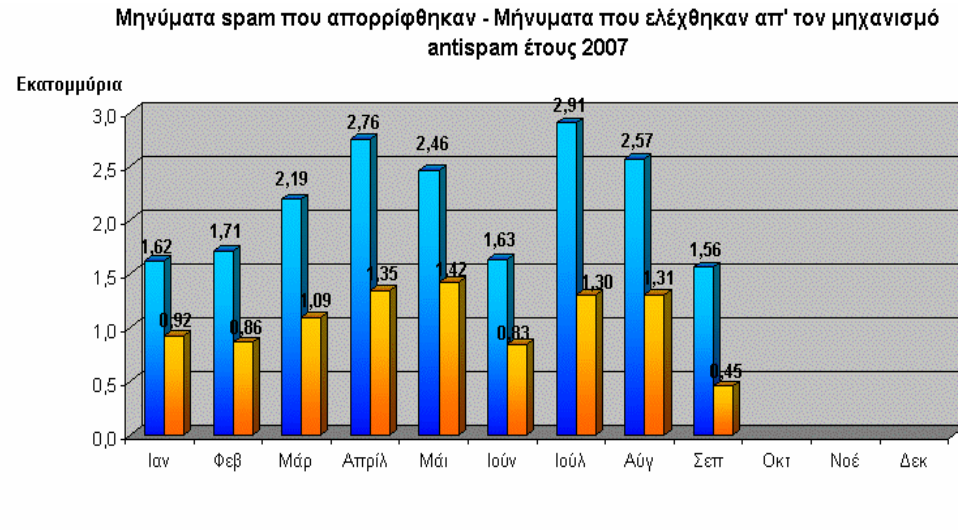
Τέλος, φαίνεται ότι από το 2002 και μετά, το φαινόμενο αυτό έχει αυξηθεί σε πολύ μεγάλο βαθμό.

Αν και από τα παραπάνω, δίνεται η εντύπωση πως ο προσδιορισμός του φαινομένου αυτού είναι απλός, στην πραγματικότητα επικρατεί σύγχυση ως προς τον προσδιορισμό του. **Δύο στους τρεις** χρήστες του ηλεκτρονικού ταχυδρομείου πιστεύουν πως μπορούν να ξεχωρίσουν ένα απλό e-mail από ένα e-mail spam διαβάζοντας μόνο και μόνο το τίτλο του θέματός του. Αντίθετα, το

9% των χρηστών πιστεύει πως πρέπει πρώτα να διαβάσει το e-mail για να καταλάβει αν πρόκειται για spam e-mail ή όχι.

Με την παραπάνω παρατήρηση θίγεται το θέμα του ακριβή προσδιορισμού ενός μηνύματος spam, που αν για τους ίδιους τους ανθρώπους είναι δύσκολο, τότε τα φίλτρα καθώς και οι διάφοροι μηχανισμοί καταστολής που χρησιμοποιούνται θα κρίνονται αναποτελεσματικά. Το 70% των χρηστών που έχουν ηλεκτρονικές διευθύνσεις θεωρούν πως η χρήση του Διαδικτύου έχει γίνει πλέον «ανυπόφορη» λόγω των spam e-mail. Το 27% θεωρεί πως τα spam e-mail είναι «μείζον πρόβλημα» ενώ το 14% πιστεύει πως τα spam e-mail δεν επιδρά σημαντικά στις on-line δραστηριότητές του.

Μερικές πρόσφατες στατιστικές μετρήσεις παρουσιάζονται στο σχήμα που ακολουθεί. Στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης για διάστημα 9 μηνών παρακολουθήθηκαν λογαριασμοί e-mail, όχι ως προς το περιεχόμενό τους αλλά ως προς την συμπεριφορά λογισμικού (spamassasin), το οποίο περιορίζει την είσοδο των spam στο επίπεδο του διακομιστή του ηλεκτρονικού ταχυδρομείου (mail server).



Διάγραμμα 2

Οι μπλε στήλες δείχνουν τα μηνύματα που ελέχθηκαν από το λογισμικό Spamassasin για την ύπαρξη spam e-mail κάθε μήνα, ενώ οι κίτρινες στήλες δείχνουν τα μηνύματα που αναγνωρίστηκαν ως spam.

Το spam επηρεάζει αρνητικά την αύξηση της παραγωγικότητας γιατί ουσιαστικά γεμίζει τις θυρίδες του ηλεκτρονικού ταχυδρομείου με μηνύματα που οι χρήστες δεν επιθυμούν να λαμβάνουν και οι χρήστες εμποδίζονται να διαβάσουν τα μηνύματα που περιέχουν ουσιαστικές πληροφορίες. Στην πράξη, πολλές ώρες χάνονται γιατί χρησιμοποιούνται για την διαγραφή των μηνυμάτων spam ή για τον εντοπισμό της πηγής προέλευσης του spam και την αποστολή ειδικών μηνυμάτων για να διακοπεί η αποστολή spam, σε όσους χρήστες βέβαια παρέχεται η δυνατότητα αυτή.

1.9 Παραλλαγές του spam

Μία παραλλαγή του spam είναι το **spim**. Ορίζεται ως «**αυτόκλητο διαφημιστικό μήνυμα**» το οποίο εμφανίζεται μέσω ενός συστήματος παραγωγής στιγμιαίων μηνυμάτων. Η ονομασία αυτή είναι αρκτικόλεξο των **SP**am **I**nstant **M**essage.

Το spim προήλθε από την τάση των διαφημιστών να διεισδύουν σε κάθε μέσο που προσεγγίζει τους καταναλωτές. Τα spim παράγονται από προγράμματα, τα οποία λέγονται ‘bots’. Όταν οι χρήστες κάνουν περιήγηση στο διαδίκτυο, μεταφέρονται από τους διακομιστές (servers) που φιλοξενούν τις ιστοσελίδες, μέρη του λογισμικού που δημιουργεί τα spim στους υπολογιστές τους, σε ελκυστική μορφή δηλαδή με γραφικά, ήχο κτλ σε προκαθορισμένο ή τυχαίο «παράθυρο» της οθόνης. Το περιεχόμενο των μηνυμάτων αυτών είναι παρόμοιο με αυτό της ιστοσελίδας που τα δημιούργησε, αφού οι διαφημιστές πιστεύουν πως η περιήγηση σε μια σελίδα υποδηλώνει ενδιαφέρον για παρόμοια θέματα, με αυτά που παρουσιάζονται σε αυτήν.

Επίσης, παραλλαγές του spam έχουν εμφανιστεί στις ιστοσελίδες που λειτουργούν ως forum για την καταγραφή on-line συζητήσεων. Αυτή η μορφή ονομάζεται **link spamming** και δεν έχει τον χαρακτήρα της αποστολής ομαδικών μηνυμάτων.

Το spam έχει πλέον αποκτήσει τον κλώνο του και στην **κινητή τηλεφωνία.** Οι περισσότεροι χρήστες το διαπιστώνουν στην πιο συνηθισμένη του μορφή, μέσω δηλαδή ενός σύντομου γραπτού μηνύματος SMS, MMS ή ηλεκτρονικού μηνύματος, το οποίο διαφημίζει κάποια υπηρεσία. Τα μηνύματα αυτά προέρχονται από χώρες όπου η τιμή χρέωσης είναι πολύ χαμηλότερη για προορισμούς όπως είναι η Ευρώπη. Με τα MMS δίνεται η ευκαιρία σε επιτήδειους να κάνουν χρήση απλών φωτογραφιών ή και μικρών σε διάρκεια βίντεο με ένα μήνυμα και να διαφημίζουν ένα ταξίδι σε κάποιο νησί του Ειρηνικού, ενώ ο ήχος της θάλασσας αναπαράγεται την ίδια στιγμή από το κινητό. Πολλές φορές, συνοδεύονται και από διασυνδέσεις σε ιστοσελίδες του Διαδικτύου όπου ο πελάτης μπορεί να δει με λεπτομέρειες το διαφημιζόμενο προϊόν.

Ωστόσο, υπάρχει και μια δεύτερη μορφή, η οποία είναι γνωστή ως **scam**. Μπορεί να είναι είτε για αναπάντητες κλήσεις από προορισμό με υψηλή τιμολόγηση είτε για σύντομο γραπτό μήνυμα το οποίο χρεώνει τον λήπτη με υψηλή τιμολόγηση. Πρόκειται ουσιαστικά, για μια προσπάθεια δημιουργίας παράνομου κέρδους που είναι αποτέλεσμα παραπλανητικών προσπαθειών ώθησης του χρήστη να απαντήσει σε κλήσεις ή μηνύματα που δεν γνωρίζει τον αποστολέα και οι οποίες δεν είναι κατ’ ανάγκη εμπορικού-διαφημιστικού χαρακτήρα.

Για παράδειγμα, η διάρκεια της εισερχόμενης κλήσης σε ένα κινητό τηλέφωνο ρυθμίζεται, έτσι ώστε ο χρήστης να μην προλάβει να απαντήσει. Εμφανίζεται έτσι μια αναπάντητη κλήση στην οθόνη του κινητού. Όταν ο χρήστης καλέσει τον αριθμό της αναπάντητης κλήσης, δεν γνωρίζει πως η κλήση του κατευθύνεται σε γραμμή αυξημένης χρέωσης. Ο απαντών θα

προσπαθήσει να κρατήσει στην γραμμή τον χρήστη όση περισσότερη ώρα μπορεί, προκειμένου να μεγιστοποιήσει τα κέρδη του.

Ανάλογη είναι και η περίπτωση όπου ο χρήστης λαμβάνει ένα SMS του οποίου το περιεχόμενο περιλαμβάνει μια πρόσκληση για να πληκτρολογήσει τον αριθμό που βρίσκεται σε αυτό. Άλλες φορές, ο λήπτης του μηνύματος καλείται να απαντήσει στο περιεχόμενό του, όπου προορισμός του έχει υψηλή χρέωση. Επίσης, ο λήπτης του μηνύματος καλείται αν θέλει να απαλλαγεί από την λήψη παρόμοιων μηνυμάτων, να στείλει κάποιο γραπτό μήνυμα σε προορισμό αυξημένης χρέωσης.

1.10 Γιατί εναντιωνόμαστε στο spam ως χρήστες

Για τους απλούς χρήστες η ανεξέλεγκτη ροή απρόσκλητων μηνυμάτων πέρα από ενόχληση συνιστά και απειλή. Τα μηνύματα αυτά μπορεί να περιέχουν ακατάλληλο αλλά και επικίνδυνο περιεχόμενο για τους χρήστες του e-mail.

Το μεγαλύτερο πρόβλημα αντιμετωπίζουν οι χρήστες που χρησιμοποιούν μεγάλα διαστήματα της ημέρας το ηλεκτρονικό ταχυδρομείο και είναι υποχρεωμένοι να σβήνουν όλη αύτη την ανεπιθύμητη αλληλογραφία. Τα μηνύματα αυτά για πολλούς χρήστες μπορεί να είναι δεκάδες σε μια ημέρα. Η αντιμετώπιση του spam είναι αναγκαία λόγω των ακόλουθων σημείων:

- Είναι ένα φαινόμενο πολύ ενοχλητικό και απαράδεκτο από τους παραλήπτες, καθώς ένας τακτικός χρήστης του Internet μπορεί να λαμβάνει πολλά τέτοια μηνύματα σε καθημερινή βάση. Πολλές φορές προβάλλονται αμφίβολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων. Τέλος, άλλα μηνύματα μπορεί να περιέχουν ή να διαφημίζουν σεξουαλικό περιεχόμενο.

- Κάνει κατάχρηση των πόρων του Internet, δηλ. επιβαρύνει πάρα πολύ τους e-mail servers, χωρίς να προσφέρει κάτι ουσιαστικό. Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με κατανάλωση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στα κεντρικά συστήματα διανομής αλληλογραφίας (e-mail servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και τα συστήματα των χρηστών.
- Βάζει σε κίνδυνο την ασφάλεια και την αξιοπιστία του Internet, καθώς πολλά τέτοια μηνύματα περιέχουν επικίνδυνους ιούς. Οι spammers συνεχώς ψάχνουν συστήματα τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους. Κάποια μηνύματα αυτής της κατηγορίας μεταφέρουν συνημμένα αρχεία τα οποία μπορεί να είναι ιοί ή σκουλήκια και τα οποία θέτουν σε κίνδυνο την ασφάλεια των συστημάτων.

1.11 Πώς επηρεάζει το spam τις επιχειρήσεις

Το spam-mail δεν προβληματίζει μόνο τις μεγάλες επιχειρήσεις αλλά και τις μικρομεσαίες. Ειδικά, τα τελευταία δύο χρόνια το spam-mail τείνει να λάβει διαστάσεις επιδημίας. Στις επιχειρήσεις υπάρχει μεγάλη απώλεια χρόνου για το ξεκαθάρισμα της αλληλογραφίας τους, κάτι που προκαλεί σημαντική επιβάρυνση στους δείκτες παραγωγικότητας των εργαζομένων. Οι εργαζόμενοι θα πρέπει, πολλές φορές την ημέρα, να ελέγχουν το mailbox τους, θα πρέπει δηλαδή να ανοίγουν τα μηνύματα που αφορούν την επιχείρησή τους και να διαγράφουν τα μηνύματα spam (που αρκετές φορές αποτελούν την πλειοψηφία…). Οι περισσότεροι κάνουν πλήρη –και χρονοβόρο- έλεγχο σε ολόκληρη την αλληλογραφία τους (ανοίγουν και εξετάζουν με προσοχή όλα τα μηνύματά τους), ενίοτε από… περιέργεια, συνήθως όμως για να σιγουρευτούν ότι δεν θα διαγράψουν από λάθος κάτι σημαντικό για την εταιρία τους. Επίσης, χρησιμοποιώντας ειδικά φίλτρα για το spam, ώστε να περιορίσουν κάπως τις συνολικές ποσότητες spam mail που λαμβάνουν, κάποια από τα μηνύματα που

θα ήθελαν να διαβάσουν παίρνουν το δρόμο χωρίς γυρισμό… Κι ενώ οι οικιακοί χρήστες έχουν τη δυνατότητα συχνών αλλαγών των e-mail διευθύνσεών τους (μέσω webmail), αυτό δεν είναι εφικτό για τις επιχειρήσεις, οι οποίες για λόγους κύρους δεν μπορούν να χρησιμοποιήσουν webmail λογαριασμούς, ενώ παράλληλα το e-mail τους αποτελεί ένα ακόμα στοιχείο της επιχειρησιακής τους ταυτότητας. Μια αλλαγή της ηλεκτρονικής τους διεύθυνσης μπορεί να τις οδηγήσει σε αρκετά λειτουργικά προβλήματα.

Οι συνολικές απώλειες εργατοωρών και το κόστος στο σύνολο της οικονομίας φθάνουν σε δυσθεώρητα ύψη. Σύμφωνα με τον αρμόδιο Επίτροπο της Ευρωπαϊκής Ένωσης Erkki Liikanen, η απώλεια που προκλήθηκε, λόγω του spam, στην παραγωγικότητα της Ε.Ε. το 2002 ανήλθε στα 2,5 δισεκατομμύρια Ευρώ .

1.12 Μέθοδοι Ελέγχου του spam

Υπάρχουν τρεις μέθοδοι ελέγχου:

1)**Μυστικότητα των προσωπικών δεδομένων**

Με τον περιορισμό στην πρόσβαση και επεξεργασία των προσωπικών δεδομένων, υπάρχουν εμπόδια στην απόκτηση διευθύνσεων και στοιχείων των χρηστών από κάθε φιλόδοξο εισβολέα.

2)**Ταυτοποίηση, πραγματική διεύθυνση και ειλικρίνεια του αποστολέα**

Επιβάλλεται από την νομοθεσία η υποχρέωση αλήθειας, όσο αφορά τον αποστολέα και την φύση του μηνύματος. Επίσης, πρέπει να περιλαμβάνεται και η αληθινή διεύθυνση επιστροφής καθώς και η δυνατότητα άρνησης μελλοντικών μηνυμάτων.

Οι δύο παραπάνω μέθοδοι είναι σημαντικές, αλλά επειδή υπάρχει αμφιβολία για το αν οι δύο παραπάνω αρκούν, ακολουθεί η παρακάτω μέθοδος η οποία είναι η πιο σημαντική.

3)**Απεγκλωβισμός**

Δίνεται η δυνατότητα στον χρήστη του Διαδικτύου να «απαρνηθεί» τέτοιου είδους μηνύματα. Το ερώτημα εδώ είναι αν ο χρήστης θέλει ή όχι τέτοια μηνύματα.

i. **OPT-OUT**

Σε περίπτωση που ο χρήστης θέλει να λαμβάνει μηνύματα spam, η τεκμηρίωση αντιστρέφεται με ένα opt-out, δηλαδή μια δυνατότητα άρνησης. Όμως, ο χρήστης έχει το βάρος της απόδειξης, πράγμα που είναι δύσκολο γιατί δεν μπορεί να καταγράφει την άρνηση προς κάθε αποστολέα.

ii. **OPT-IN**

Στην περίπτωση όπου ο χρήστης δεν επιθυμεί να δέχεται μηνύματα spam, ο κάθε αποστολέας θα πρέπει να αποδείξει πως έχει την προηγούμενη συναίνεση του χρήστη.

Η Ευρώπη, στην νομοθεσία της κινείται ως προς την επιλογή opt-in ενώ η Αμερική προσανατολίζεται ως προς το opt-out. Η διαφορά ανάμεσα σε αυτά τα δύο συστήματα είναι σημαντική, με το opt-in να προσφέρει καλύτερη προστασία στον χρήστη. Βέβαια, στην πράξη τα πράγματα είναι διαφορετικά και το ενδιαφέρον εστιάζεται στο τι είδους opt-in και opt-out χρησιμοποιείται.

Αν, για παράδειγμα, ισχύει το σύστημα opt-in και η άρνηση λειτουργεί μόνο κατά των αποστολέων, που σημαίνει ότι κάθε αποστολέας πρέπει να ζητά την συναίνεση των χρηστών ένας προς έναν, τότε το βάρος της άρνησης ουσιαστικά πέφτει στον χρήστη. Έτσι, προτιμότερο φαίνεται να είναι το σύστημα opt-out όπου ο κάθε χρήστης μπορεί να διατυπώνει μια άρνηση για κάθε μήνυμα spam με την εγγραφή τους σε ένα μητρώο για άτομα που δεν επιθυμούν να λαμβάνουν μηνύματα spam.

ΚΕΦΑΛΑΙΟ 2

2.1 Μη Αιτηθείσα Εμπορική Επικοινωνία (Spamming)

Η ανάπτυξη του Διαδικτύου και η χρήση του από τις επιχειρήσεις για την προσέλκυση των καταναλωτών διεύρυνε τις δυνατότητες των επιχειρήσεων που δραστηριοποιούνται στο χώρο της απευθείας διαφήμισης και άμεσης εμπορίας προϊόντων και υπηρεσιών. Το μεγαλύτερο πρόβλημα αυτής της απευθείας διαφήμισης και προώθησης των προϊόντων αποτελεί η αποστολή **μη αιτηθέντων** διαφημιστικών αιτημάτων ηλεκτρονικού ταχυδρομείου (e-mail), γνωστό ως «Spamming» ή αλλιώς ως «junk e-mail».

Όπως έχει ήδη αναφερθεί, ανεπιθύμητη ηλεκτρονική αλληλογραφία είναι η μαζική αποστολή του ίδιου μηνύματος ηλεκτρονικής αλληλογραφίας σε πολλούς αποδέκτες κυρίως για διαφημιστικούς λόγους. Αποδέκτες αυτής της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας μπορεί να είναι εκτός από τους μεμονωμένους χρήστες και ομάδες συζητήσεων (newsgroups), στις οποίες συμμετέχουν πολλοί χρήστες του Διαδικτύου. Η αποστολή της ανεπιθύμητης αλληλογραφίας είναι ένα από τα σημαντικά εργαλεία του Marketing, αφού το κόστος της αποστολής του είναι πολύ χαμηλό.

Η αποστολή του spamming προκαλεί προβλήματα τόσο στους μεμονωμένους χρήστες, οι οποίοι αντιμετωπίζουν το spamming ως παρενόχληση αλλά και ως απώλεια χρόνου και χρήματος γιατί μπορεί να καταβάλλουν συνδρομή σε φορέα παροχής υπηρεσιών για όση ώρα συνδέονται στο Διαδίκτυο προκειμένου να διαβάσουν τα e-mail τους, όσο και στους παροχείς υπηρεσιών πρόσβασης που λόγω της υπερφόρτωσης του δικτύου από τα μηνύματα spam, δέχονται τα παράπονα των χρηστών αλλά και επιβαρύνονται με αυξημένα έξοδα διαχείρισης του δικτύου.

Επίσης, αντίθετοι στην αποστολή του spamming είναι και οι τρίτοι, οι οποίοι πέφτουν θύματα πλαστογράφησης των ηλεκτρονικών διευθύνσεών τους

για να χρησιμοποιηθούν στην θέση του αποστολέα των μηνυμάτων κυρίως για την κάλυψη της προέλευσης του spam.

Τέλος, όσον αφορά τους μεμονωμένους χρήστες η αποστολή του spamming συνιστά και παραβίαση της ιδιωτικής ζωής τους, αφού με την εισβολή στον προσωπικό «χώρο» παραβιάζεται το δικαίωμα του ατόμου στη μόνωση αλλά καταργείται και το δικαίωμα να μην γίνεται κάποιος αποδέκτης πληροφοριών, εφόσον δεν το επιθυμεί.

Η αύξηση του φαινομένου του spam κινητοποίησε την νομοθετική εξουσία, η οποία προσπαθεί να ρυθμίσει την διαδικτυακή συμπεριφορά, προσπαθώντας να ισορροπήσει μεταξύ της προστασίας των χρηστών και της διασφάλισης των θεμελιωδών ελευθεριών των πολιτών.

Στην συνέχεια, παρουσιάζονται οι ισχύουσες νομοθεσίες για την προστασία των καταναλωτών στο ηλεκτρονικό εμπόριο στις Ηνωμένες Πολιτείες Αμερικής, την Ευρώπη και στην Ελλάδα.

2.2 Νομοθεσία Ηνωμένων Πολιτειών Αμερικής

Can Spam Act 2003

Άρθρο 4 - Απαγόρευση του εξοντωτικού καταχρηστικού εμπορικού ηλεκτρονικού ταχυδρομείου.

«(α) ***Παράβαση***

(1)Γενικά - Το κεφάλαιο 47 του τίτλου 18, Κώδικα Ηνωμένων Πολιτειών, τροποποιείται με την πρόσθεση στο τέλος του εξής νέου τμήματος:

Τμ. 1037. Απάτη και σχετική δραστηριότητα αναφορικά με το ηλεκτρονικό ταχυδρομείο.

(α) Γενικά – Οποιοσδήποτε σχετιζόμενος με το διακρατικό ή ξένο εμπόριο, εσκεμμένα:

(1) αποκτά πρόσβαση σε ένα προστατευμένο υπολογιστή χωρίς έγκριση, και σκοπίμως αρχίζει την μετάδοση πολλαπλών εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από ή μέσω τέτοιου υπολογιστή,

(2) χρησιμοποιεί έναν προστατευμένο υπολογιστή για την αποστολή ή την αναμετάδοση πολλαπλών εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, με την πρόθεση να εξαπατήσει ή να παραπλανήσει τους παραλήπτες, ή οποιαδήποτε υπηρεσία πρόσβασης του Διαδικτύου, ως προς την προέλευση τέτοιων μηνυμάτων,

(3) πλαστογραφεί με υλικά μέσα τις κεφαλίδες στα πολλαπλά εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου και σκοπίμως αρχίζει την μετάδοση τέτοιων μηνυμάτων,

(4) καταχωρεί τον εαυτό του, χρησιμοποιώντας πληροφορίες που πλαστογραφούν με υλικά μέσα την ταυτότητα του πραγματικού καταχωρούμενου, για πέντε ή περισσότερους λογαριασμούς ηλεκτρονικού ταχυδρομείου, ή λογαριασμούς χρηστών σε απευθείας σύνδεση, ή δύο ή περισσότερες ονομασίες

domain, *και αρχίζει σκόπιμα την μετάδοση πολλαπλών μηνυμάτων ηλεκτρονικού ταχυδρομείου από οποιοδήποτε συνδυασμό τέτοιων λογαριασμών ή* domain *ονομασιών, ή*

(5) ψευδώς αυτοπαρουσιάζεται ως ο καταχωρούμενος ή ο νόμιμος διάδοχος συμφερόντων του καταχωρούμενου πέντε ή περισσοτέρων Διευθύνσεων Πρωτοκόλλου του Διαδικτύου, και σκοπίμως αρχίζει την μετάδοση πολλαπλών εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από τέτοιες διευθύνσεις, ή συνωμοτεί για να το κάνει, θα τιμωρηθεί όπως αναφέρεται στην ενότητα (β).

(β)Ποινές – *Η τιμωρία για μία παράβαση της ενότητας (α) είναι:*

(1) ένα πρόστιμο υπό αυτόν τον τίτλο, φυλάκιση όχι για περισσότερο από 5 χρόνια, ή και τα δύο μαζί, εάν:

(Α) η παράβαση διαπράττεται σε συνέχεια οποιουδήποτε κακουργήματος βάσει των νόμων των Ηνωμένων Πολιτειών ή οποιασδήποτε πολιτείας, ή

(Β) ο κατηγορούμενος έχει προηγουμένως καταδικαστεί στο πλαίσιο αυτής της ενότητας ή της ενότητας 1030, ή βάσει του νόμου οποιασδήποτε Πολιτείας για συμπεριφορά που περιλαμβάνει την μετάδοση πολλαπλών εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή την χωρίς άδεια πρόσβαση σε σύστημα υπολογιστών,

(2) ένα πρόστιμο υπό αυτόν τον τίτλο, φυλάκιση όχι για περισσότερο από 3 χρόνια, ή και τα δύο μαζί, εάν:

(Α) η παράβαση είναι παράβαση της υποενότητας (α)(1),

(Β)η παράβαση είναι παράβαση της υποενότητας (α)(4) και αφορά 20 ή περισσότερες πλαστογραφημένες διευθύνσεις ηλεκτρονικού ταχυδρομείου ή λογαριασμούς χρηστών σε απευθείας σύνδεση, ή 10 ή περισσότερες πλαστογραφημένες εγγραφές domain *ονομασιών,*

(Γ) ο όγκος των μηνυμάτων ηλεκτρονικού ταχυδρομείου που μεταφέρθηκαν σε συνέχεια της παράβασης, υπερέβη τα 2.500 κατά την διάρκεια 24ωρης περιόδου, τα 25.000 κατά την διάρκεια οποιασδήποτε περιόδου 30 ημερών, τα 250.000 κατά την διάρκεια μιας ετήσιας περιόδου,

(Δ) η παράβαση προκάλεσε την απώλεια σε ένα ή περισσότερα άτομα μαζί 5.000 δολαρίων ή περισσοτέρων κατά τη διάρκεια οποιασδήποτε ετήσιας περιόδου,

(Ε) σαν αποτέλεσμα της παράβασης οποιοδήποτε άτομο που την διαπράττει, αποκτήσει οτιδήποτε συνολικής αξίας 5.000 δολαρίων ή περισσότερο κατά την διάρκεια μίας ετήσιας περιόδου, ή

(ΣΤ) η παράβαση έγινε από τον κατηγορούμενο σε συντονισμό με τρία ή περισσότερα άτομα, σε σχέση με τα οποία ο κατηγορούμενος κατείχε την θέση του διοργανωτή ή του αρχηγού, και

(3) ένα πρόστιμο υπό αυτόν τον τίτλο ή φυλάκιση όχι για περισσότερο από 1 χρόνο, ή και τα δύο μαζί, σε οποιαδήποτε άλλη περίπτωση.»

Άρθρο 5 – Τρόποι προστασίας για τους χρήστες εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου.

«Παρ 3 – Ένταξη διεύθυνσης επιστροφής ή συγκρίσιμου μηχανισμού στα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου.

(Α) ***Γενικά*** *- Είναι παράνομο για κάθε άτομο να αρχίζει την μεταφορά των εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε ένα προστατευμένο υπολογιστή εάν αυτά δεν περιέχουν μία λειτουργούσα διεύθυνση επιστροφής ηλεκτρονικού ταχυδρομείου ή μηχανισμό βασισμένο στο Διαδίκτυο, σαφώς και εμφανώς παρουσιασμένο, όπου:*

(1) ο παραλήπτης μπορεί να χρησιμοποιήσει για να υποβάλει, με έναν τρόπο που διευκρινίζεται στο μήνυμα, ένα ηλεκτρονικό μήνυμα απάντησης ή με άλλο βασισμένο στο Διαδίκτυο τρόπο επικοινωνίας, ζητώντας να μην λαμβάνει στο μέλλον εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου από εκείνο τον αποστολέα στην ηλεκτρονική διεύθυνση όπου το μήνυμα παραλήφθηκε, και

(2) παραμένει ικανός να λαμβάνει τέτοια μηνύματα ή επικοινωνίες για όχι λιγότερο από 30 ημέρες μετά την μετάδοση του αρχικού μηνύματος.

(Β) ***Περισσότερες εφικτές, λεπτομερείς επιλογές-*** *Το άτομο που αρχίζει ένα εμπορικό μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να συμμορφωθεί σύμφωνα με την υποπαράγραφο (Α)(1), παρέχοντας στον παραλήπτη μία λίστα ή μενού σύμφωνα με το οποίο ο παραλήπτης μπορεί να επιλέξει συγκεκριμένους τύπους εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου που θέλει να λαμβάνει ή δεν θέλει να λαμβάνει από τον αποστολέα, εάν στην λίστα ή στο μενού υπάρχει επιλογή κάτω από την οποία ο παραλήπτης μπορεί να επιλέξει να μην λαμβάνει κανένα εμπορικό μήνυμα ηλεκτρονικού ταχυδρομείου από τον αποστολέα.»*

«Παρ 5 - Ένταξη αναγνωριστικού, ρήτρα απαλλαγής και φυσική διεύθυνση στα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου.

(Α) Είναι παράνομο για κάθε άτομο να αρχίζει την μεταφορά των εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε ένα προστατευμένο υπολογιστή αν το μήνυμα δεν παρέχει:

(1) σαφή και ευδιάκριτο προσδιορισμό πως το μήνυμα αποτελεί διαφήμιση,

(2) σαφή και ευδιάκριτη παρατήρηση για την ευκαιρία στο πλαίσιο της παραγράφου 3 να αρνείται περαιτέρω την λήψη εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον αποστολέα, και

(3) μία έγκυρη ηλεκτρονική διεύθυνση του αποστολέα.

(Β) Η υποπαράγραφος (Α)(1) δεν εφαρμόζεται κατά την μεταφορά εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου εάν ο παραλήπτης έχει δώσει προγενέστερη καταφατική άδεια για την λήψη αυτών των μηνυμάτων.»

Άρθρο 9 – Μη λήψη ηλεκτρονικής αλληλογραφίας

«(α) Γενικά – Όχι αργότερα από 6 μήνες από την θέσπιση αυτού του νόμου, η Επιτροπή θα στείλει στην Συγκλητική Επιτροπή για το Εμπόριο, τις Επιστήμες και τις Συγκοινωνίες και στην Επιτροπή της Βουλής των Αντιπροσώπων για την Ενέργεια και το Εμπόριο μια έκθεση, η οποία:

(1) εκθέτει ένα σχέδιο και ένα χρονοδιάγραμμα για μία, σε εθνικό επίπεδο, πολιτική μη λήψης ηλεκτρονικής αλληλογραφίας,

(2) περιλαμβάνει μία εξήγηση για κάθε ζήτημα πρακτικό, τεχνικό, ασφάλειας, ιδιωτικότητας, δυνατότητας επιβολής, ή για κάθε ανησυχία που έχει η Επιτροπή σχετικά με κάθε πολιτική τέτοιου είδους, και

(3) περιλαμβάνει μία εξήγηση για το πώς η πολιτική αυτή θα εφαρμοζόταν με σεβασμό σε παιδιά που έχουν λογαριασμούς ηλεκτρονικού ταχυδρομείου.

*(β) **Αρμοδιότητα για εφαρμογή** – Η Επιτροπή μπορεί να καθιερώσει και να εφαρμόσει το σχέδιο, αλλά όχι νωρίτερα από 9 μήνες μετά την θέσπιση του νόμου.»*

Άρθρο 11 – Βελτίωση τις επιβολής με την παροχή ανταμοιβών για πληροφορίες σχετικά με τις παραβιάσεις, μαρκάρισμα.

«Η Επιτροπή θα στείλει στην Επιτροπή Συγκλήτου του Εμπορίου, Επιστήμης, και της Μεταφοράς και της Επιτροπής της Βουλής των Αντιπροσώπων –

(1) μία έκθεση, μέσα σε 9 μήνες από την θέσπιση αυτού του νόμου, η οποία εκθέτει ένα σύστημα ανταμοιβών αυτών που παρέχουν πληροφορίες για παραβάσεις αυτού του νόμου, περιλαμβάνοντας:

(Α) Διαδικασίες για την Επιτροπή να χορηγήσει μια ανταμοιβή όχι μικρότερη από το 20 % του συνολικού ποσού των προστίμων των πολιτών για παράβαση του νόμου αυτού στο άτομο που:

(1) αναγνωρίζει το άτομο που έκανε παράβαση του νόμου αυτού, και

(2) παρέχει πληροφορίες που οδηγούν σε επιτυχημένη συλλογή συνολικού προστίμου από την Επιτροπή, και

(Β) Διαδικασίες για να ελαχιστοποιήσει την ταλαιπωρία της υποβολής ενός παραπόνου στην Επιτροπή σχετικά με παραβάσεις του νόμου, συμπεριλαμβανομένων των διαδικασιών που επιτρέπουν την ηλεκτρονική υποβολή παραπόνων στην Επιτροπή, και

(2) μία έκθεση, μέσα σε 18 μήνες από την θέσπιση αυτού του νόμου, η οποία εκθέτει ένα σχέδιο για την απαίτηση τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου να μπορούν να προσδιοριστούν από την γραμμή του θέματος, μέσω της συμμόρφωσης με τα Δεδομένα της Ομάδας Εργασίας Μελέτης Internet, την χρήση των χαρακτήρων 'ADV' στην γραμμή του θέματος, ή άλλο συγκρίσιμο προσδιορισμό, ή μία εξήγηση για τις ανησυχίες που η Επιτροπή έχει και μπορεί να συστήσει ενάντια στο σχέδιο.»

Οι Η.Π.Α θεωρούνται η πατρίδα του Διαδικτύου αφού αποτελεί την βασική πηγή του spam (το 90% των spam που λαμβάνει η Ευρώπη προέρχονται από την Αμερική). Το 1996 τα αμερικάνικα δικαστήρια κλήθηκαν να πάρουν μια σειρά αποφάσεων σε υποθέσεις που αφορούσαν μεγάλες εταιρίες του διαδικτύου όπως οι Hotmail Corporation, America Online Inc κ.α. και τους spammers. Το αντικείμενο της διαφοράς τους ήταν η εκμετάλλευση των διακομιστών των παροχέων για την μαζική αποστολή μηνυμάτων ή η χρήση της επωνυμίας τους σε παραποιημένες κεφαλίδες e-mail. Σε κάθε περίπτωση, οι spammers χρησιμοποιούσαν για υπεράσπιση το επιχείρημα της ελευθερίας διάδοσης των ιδεών, πράγμα που δεν έγινε δεκτό από κανένα δικαστήριο.

Για να αντιμετωπιστεί το φαινόμενο του spam ψηφίστηκε το 2003 νομοθέτημα για την καταστολή του, γνωστό ως «**CAN SPAM Act 2003**» και τέθηκε σε ισχύ από την 01 Ιανουαρίου 2004.

Ο νόμος αυτός περιλαμβάνει μέτρα για την πρόληψη και τον περιορισμό του προβλήματος της ανεπιθύμητης αλληλογραφίας καθώς και κυρώσεις για

τους αποστολείς ανεπιθύμητης αλληλογραφίας και τις εταιρίες που παραβιάζουν τον νόμο και τα προϊόντα των οποίων διαφημίζονται σε μηνύματα ανεπιθύμητης αλληλογραφίας.

Συγκεκριμένα, προβλέπει ποινές φυλάκισης έως 5 χρόνια και υψηλές χρηματικές ποινές, αφού ποινικοποιεί πολλές από τις δραστηριότητες των spammer όπως είναι η αλλαγή των στοιχείων του αποστολέα, η συγκέντρωση ηλεκτρονικών διευθύνσεων και η εκμετάλλευση ξένων υπολογιστών και διακομιστών.

Επιπλέον, επιβάλλει την παροχή της δυνατότητας 'Opt-out' σε κάθε διαφημιστικό e-mail. Αυτό σημαίνει πως ο κάθε ένας παραλήπτης των junk e-mail πρέπει να έχει την επιλογή να δηλώσει ότι δεν επιθυμεί την περαιτέρω λήψη τέτοιου είδους αλληλογραφίας από τον συγκεκριμένο αποστολέα.

Ακόμα, προβλέπεται η δημιουργία μιας λίστας « μη λήψης ηλεκτρονικής αλληλογραφίας» ("Do-Not-E-mail registry"), στην οποία μπορούν να εγγραφούν όσοι χρήστες επιθυμούν να μην λαμβάνουν εμπορική ηλεκτρονική αλληλογραφία. Οι διαφημιζόμενοι πρέπει, πριν ξεκινήσουν μια ηλεκτρονική διαφημιστική καμπάνια, να λαμβάνουν υπόψη αυτού του είδους τις λίστες.

Τέλος, προωθείται η ετικετοποίηση των διαφημιστικών e-mail με την προσθήκη των αρχικών 'ADV' (Advertisement) στο θέμα, για να μπορούν οι χρήστες να τα αναγνωρίζουν άμεσα.

Βάσει του νόμου Can-Spam Act δύο άντρες κρίθηκαν ένοχοι και καταδικάστηκαν να εκτίσουν **ποινή φυλάκισης** για την αποστολή **πορνογραφικών spam e-mails**. Ο Jeffrey A. Kilbride και ο James R.Schaffer καταδικάστηκαν σε 72 και 63 μήνες αντίστοιχα, καθώς ο πρώτος κρίθηκε ένοχος και για προσπάθεια παρεμπόδισης της δικαιοσύνης, αφού απείλησε μάρτυρες, ώστε αυτοί να μην καταθέσουν στη δίκη. Στους δύο spammers επιβλήθηκε επίσης και **πρόστιμο 100.000 δολαρίων**, ενώ ακόμα θα πληρώσουν στην AOL άλλα 77.500 δολάρια και θα κατασχεθούν και τα κέρδη τους από την παράνομη επιχείρηση, τα οποία φτάνουν το 1,1 εκατομμύριο δολάρια.

Οι δύο spammers ξεκίνησαν την αποστολή των spam e-mails το 2003, ενώ η δίωξη εναντίον τους, άρχισε τον Ιούνιο του 2007.

Αν και το νομοθέτημα αυτό έχει βοηθήσει τις εταιρίες να αντιμετωπίσουν τους spammers, ωστόσο έχει δεχθεί και αυστηρές κριτικές γιατί δεν παρέχει νομική κάλυψη σε μεμονωμένους χρήστες για την έγερση αξιώσεων εναντίον των spammers ενώ συγχρόνως δεν εμποδίζει την αποστολή όλων των ενοχλητικών μηνυμάτων.

2.3 Νομοθεσία Ευρώπης

Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

Άρθρο 10-Περιορισμοί χρήσεως ορισμένων μέσων επικοινωνίας εξ αποστάσεως.

«1. Απαιτείται η προηγούμενη συγκατάθεση του καταναλωτή για τη χρήση από έναν προμηθευτή των ακόλουθων μέσων:

- *αυτοματοποιημένου συστήματος κλήσεως χωρίς ανθρώπινη παρέμβαση (συσκευής αυτόματης κλήσεως),*
- *μηχανήματος τηλεομοιοτυπίας (φαξ).*

2. *Τα κράτη μέλη μεριμνούν ώστε τα μέσα εξ αποστάσεως επικοινωνίας, εκτός από εκείνα που αναφέρει η παράγραφος 1, εφόσον καθιστούν δυνατή μια ατομική επικοινωνία, να επιτρέπεται να χρησιμοποιηθούν μόνον εάν ο καταναλωτής δεν έχει εκδηλώσει την αντίθεσή του»*

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

Άρθρο 13 – Αυτόκλητες κλήσεις

«1.Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης

επιτρέπεται μόνο στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.

2. Παρά την παράγραφο 1, αν ένα φυσικό ή νομικό πρόσωπο αποκτά από τους πελάτες του στοιχεία επαφής του ηλεκτρονικού ταχυδρομείου τους στο πλαίσιο της πώλησης ενός προϊόντος ή μιας υπηρεσίας, σύμφωνα με την οδηγία 95/46/ΕΚ, μπορεί να χρησιμοποιεί τα εν λόγω στοιχεία για την απευθείας εμπορική προώθηση των δικών του παρόμοιων προϊόντων ή υπηρεσιών, υπό την προϋπόθεση ότι οι πελάτες του έχουν σαφώς και ευδιάκριτα την ευκαιρία να αντιτάσσονται, δωρεάν και εύκολα, σε αυτή τη συλλογή και χρησιμοποίηση ηλεκτρονικών στοιχείων επαφής, και αυτό με κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή τη χρήση.

3. Τα κράτη μέλη λαμβάνουν τα ενδεδειγμένα μέτρα προκειμένου να εξασφαλίζεται, ατελώς, ότι οι αυτόκλητες κλήσεις με σκοπό την απευθείας εμπορική προώθηση, σε άλλες, εκτός των προβλεπόμενων στις παραγράφους 1 και 2, περιπτώσεις, δεν επιτρέπονται χωρίς τη συγκατάθεση των ενδιαφερόμενων συνδρομητών ή όταν πρόκειται για συνδρομητές οι οποίοι δεν επιθυμούν να λαμβάνουν αυτές τις κλήσεις. Η σχετική επιλογή καθορίζεται από την εθνική νομοθεσία.

4. Εν πάση περιπτώσει, απαγορεύεται η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση, τα οποία συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, ή δίχως έγκυρη διεύθυνση στην οποία ο αποδέκτης να μπορεί να ζητήσει τον τερματισμό της επικοινωνίας αυτής.

5. Οι παράγραφοι 1 και 3 ισχύουν για τους συνδρομητές που είναι φυσικά πρόσωπα. Τα κράτη μέλη εξασφαλίζουν επίσης, στο πλαίσιο του κοινοτικού δικαίου και της εφαρμοστέας εθνικής νομοθεσίας, ότι προστατεύονται επαρκώς τα έννομα συμφέροντα των συνδρομητών που δεν είναι φυσικά πρόσωπα σε ό,τι αφορά τις αυτόκλητες κλήσεις.»

Η Ευρωπαϊκή Ένωση θέλοντας να δείξει πως προτεραιότητά της είναι η προστασία των καταναλωτών εξέδωσε το 1997 την οδηγία **1997/7/ΕΚ** με σκοπό την «προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις », για να περιοριστεί η χρήση ορισμένων μέσων επικοινωνίας. Σύμφωνα με αυτή την οδηγία εμποδίζεται η εμπορική επικοινωνία με φαξ ή αυτοποιημένα συστήματα κλήσεων τηλεφώνου, δίχως την συγκατάθεση του καταναλωτή.

Ύστερα από πέντε χρόνια, το Ευρωπαϊκό Κοινοβούλιο εξέδωσε την οδηγία **2002/58/ΕΚ** με σκοπό την «προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ». Το άρθρο 13 της οδηγίας αυτής αναφέρεται στα μηνύματα του ηλεκτρονικού ταχυδρομείου με σκοπό την απευθείας εμπορική προώθηση. Η επικοινωνία αυτή θεωρείται αποδεκτή μόνο μετά την συγκατάθεση των καταναλωτών ή μέσω μια προηγούμενης συναλλαγής (πώληση προϊόντος ή υπηρεσίας). Σε κάθε, πάντως, διαφημιστική αποστολή πρέπει να δίνεται η δυνατότητα στους παραλήπτες να δηλώσουν την αντίθεσή τους στην λήψη αυτών των μηνυμάτων. Τέλος, απαγορεύεται η απόκρυψη της ταυτότητας του αποστολέα καθώς και η χρήση μη έγκυρης διεύθυνσης στην οποία οι παραλήπτες μπορούν να ζητήσουν να διακοπεί αυτή η επικοινωνία.

Αν και η οδηγία αυτή μοιάζει σε αρκετά σημεία με τον νόμο ‘CAN SPAM Act 2003’ υπάρχει μία βασική διαφορά. Επιλέγει την μέθοδο ‘Soft Opt-in’ δηλαδή θεωρεί απαραίτητη την συγκατάθεση των παραληπτών για την συνέχιση αυτού του είδους επικοινωνίας. Δεν νομιμοποιείται δηλαδή ένα τμήμα του spam αφού τηρούνται κάποιες προϋποθέσεις. Μοναδική προϋπόθεση αποτελεί η σύμφωνη ή όχι γνώμη των παραληπτών. Έτσι, σε αυτό το σημείο παρουσιάζεται το πρόβλημα της έννοιας του spam. Η συγκεκριμένη οδηγία εστιάζει μόνο στην απευθείας εμπορική προώθηση, δημιουργώντας έτσι ένα νομικό κενό όσο αφορά ένα μεγάλο αριθμό μηνυμάτων spam, τα οποία διαφέρουν ως προς το περιεχόμενο και την μορφή.

Σύμφωνα με την παραπάνω οδηγία της Ευρωπαϊκής Ένωσης, όλα τα κράτη-μέλη είναι υποχρεωμένα να προσαρμόσουν τις εσωτερικές τους νομοθεσίες. Κάποια κράτη-μέλη έχουν ήδη προσαρμόσει τη νομοθεσία τους, ενώ σε κάποιες άλλες η διαδικασία αυτή βρίσκεται σε εξέλιξη.

2.4 Νομοθεσία Ελλάδας

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.»

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

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.»

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

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 ζητηθεισών 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 ζητηθεισών 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 υπηρεσιών υποχρεούται να καταχωρεί τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου.

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.»

<u>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)</u>

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 (Ά 50) για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και των διατάξεων του Ν. 2774/99 (Ά 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.»

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

Άρθρο 11- Μη ζητηθείσα επικοινωνία

« 1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών 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 ζητηθεισών 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 ενδιαφερομένου.

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.»

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.

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 ζητηθεισών 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.

ΚΕΦΑΛΑΙΟ 3

3.1 Το spam φορέας κινδύνων

Το spam δεν είναι απλά ένα παρενοχλητικό φαινόμενο, ικανό να καθυστερήσει ή και να εκνευρίσει τον μέσο χρήστη του Διαδικτύου. Οι επιπτώσεις του γίνονται πιο κατανοητές όταν το περιεχόμενό του είναι ικανό να βλάψει την λειτουργία των ηλεκτρονικών υπολογιστών. Έτσι, πολλές φορές οι μαζικές αποστολές ηλεκτρονικών μηνυμάτων εξυπηρετούν τους hacker για την μετάδοση επικίνδυνων ιών (Viruses), επικίνδυνου λογισμικού (Spyware), προγραμμάτων αυτόματης κλήσης (Dialers), δούρειους ίππους (Trojans) κλπ. Με τον ίδιο τρόπο πολλά κυκλώματα οργανώνουν απάτες και απευθύνονται σε χιλιάδες ανθρώπους μέσω του διαδικτύου, προκειμένου να εκμεταλλευτούν την αφέλεια έστω και ενός ατόμου. Το πιο χαρακτηριστικό παράδειγμα αποτελεί η λεγόμενη απάτη του «νιγηριανού συνδέσμου» (Nigeria connection), σύμφωνα με την οποία ένας πρώην πρόξενος μιας Αφρικανικής χώρας ζητούσε βοήθεια για την εξαγωγή μεγάλων χρηματικών ποσών, μη ελεγχόμενων από την κυβέρνησή του, με αντάλλαγμα μεγάλη χρηματική βοήθεια. Άλλες περιπτώσεις απατών αποτελούν τα μηνύματα, τα οποία έχουν ως θέμα τις παρακάτω φράσεις: «Υπάρχει κάποιο πρόβλημα με τον λογαριασμό σας», «Αποκτήστε αυτό το πρόγραμμα και περιηγηθείτε στο Διαδίκτυο με μεγαλύτερη ταχύτητα» κ.λπ. Όταν στο πρόσωπο ενός κυβερνοπειρατή δεν απαντάται μόνο η ανάγκη επίδειξης γνώσης και υπεροχής αλλά υπερτερεί η ηθική ενός κοινού απατεώνα, τότε οι συνέπειες για τον ανυποψίαστο χρήστη μπορεί να είναι απρόβλεπτες. Η υποκλοπή των κωδικών τραπεζικών λογαριασμών ή των αριθμών πιστωτικών καρτών αποτελούν την πιο ενδεικτική έκφραση του οικονομικού εγκλήματος στο Διαδίκτυο. Όλες αυτές οι μορφές κινδύνου της ψηφιακής πραγματικότητας, υποβοηθούνται όλο και περισσότερο από τους μηχανισμούς του spamming.

3.2 Απόψεις σχετικά με το spam και την αντιμετώπισή του

Στο διαδικτυακή κοινότητα επικρατούν τρεις απόψεις που αφορούν την ανεπιθύμητη ηλεκτρονική αλληλογραφία καθώς και τους τρόπους αντιμετώπισής της.

- Η πρώτη άποψη αναφέρεται στην δυσκολία της ταυτοποίησης ενός μηνύματος spam με ακρίβεια. Οι υποστηρικτές της, πιστεύουν πως πρέπει να δέχονται όλη την αλληλογραφία που απευθύνεται προς αυτούς, για να μην χάσουν ποτέ χρήσιμα μηνύματα.

«***Το spam δεν μπορεί να σταματήσει.*** *Είναι δύσκολη η ταυτοποίηση ενός μηνύματος* **spam** *με ακρίβεια. Η προσπάθεια αντιμετώπισης του* **spam** *είναι σπατάλη πόρων και χρόνου και οδηγεί σε απώλεια και χρήσιμων μηνυμάτων.*»

- Η δεύτερη άποψη αναφέρεται στο γεγονός ότι η απόρριψη των μηνυμάτων πρέπει να είναι επιλογή του τελικού χρήστη. Η άποψη αυτή ενισχύεται και από την Αρχή της ιδιωτικότητας της επικοινωνίας καθώς απόρριψη μηνυμάτων χωρίς την εξουσιοδότηση του χρήστη αποτελεί παράβαση της παραπάνω αρχής. Οι υποστηρικτές της, πιστεύουν πως η απώλεια των μηνυμάτων σε σχέση με τα μηνύματα spam που θα απορριφθούν πρέπει να είναι προσωπική επιλογή και ευθύνη του τελικού χρήστη.

«***Η αντιμετώπιση του spam είναι ευθύνη των τελικών χρηστών.*** *Επειδή η ταυτοποίηση του* **spam** *είναι τόσο δύσκολη ας αφήσουμε την αντιμετώπισή του στις επιλογές του τελικού χρήστη. Ας αφήσουμε τον τελικό χρήστη να επιλέγει και να διαμορφώνει τα φίλτρα βάσει των οποιών θα επιλέγονται τα μηνύματα που θα περνάνε ή θα αποκλείονται από το γραμματοκιβώτιο του.*»

- Η τρίτη άποψη αναφέρει πως «***η αντιμετώπιση των μηνυμάτων spam είναι είναι ευθύνη των διαχειριστών mail servers***». Η άποψη αυτή ενισχύεται από την ύπαρξη εργαλείων που αφορούν την απόρριψη μηνυμάτων σε επίπεδο κεντρικών συστημάτων. Η καταπολέμηση των μηνυμάτων spam

πρέπει να γίνεται στα κεντρικά συστήματα διακίνησης της αλληλογραφίας (mail server) για να εξασφαλιστούν έτσι οι πόροι των κεντρικών συστημάτων καθώς και του δικτύου. Ακόμα, πολλές φορές οι υπεύθυνοι των δικτύων πιστεύουν πως είναι απαράδεκτο το γεγονός να φτάνει μέσω του δικτύου τους επικίνδυνη αλληλογραφία. Οι υποστηρικτές της, πιστεύουν πως με αυτόν τον τρόπο η απώλεια των χρήσιμων μηνυμάτων σε σχέση με τα μηνύματα spam που θα απορριφθούν μπορεί να κρατηθεί σε αποδεκτά χαμηλά επίπεδα.

Ωστόσο, στις παραπάνω απόψεις υπάρχουν δύο βασικές παραλλαγές.

Πρώτον, τα μηνύματα που προέρχονται από αποστολείς, οι οποίοι έχουν καταχωρηθεί σε λίστες RBL (Real Time Black Hole Lists) πρέπει να διαγράφονται από το γραμματοκιβώτιο χωρίς καμία εξαίρεση. Υπάρχουν όμως κάποιοι που υποστηρίζουν πως οι λίστες αυτές δεν είναι πάντα δίκαιες ως προς την καταγραφή ή όχι των αποστολέων λόγω της ποικιλίας των κριτηρίων που υπάρχουν στις λίστες. Όλο αυτό έχει σαν αποτέλεσμα, την απόρριψη αποδεκτών μηνυμάτων και τους χρήστες να παραπονούνται για τα μηνύματα που απορρίφθηκαν.

Δεύτερον, τα μηνύματα που ικανοποιούν κάποια συγκεκριμένα standards, πρέπει να απορρίπτονται ή να χαρακτηρίζονται ως πιθανά μηνύματα spam. Ο έλεγχος που γίνεται στα μηνύματα αυτά αφορά την επικεφαλίδα «From» ή τον φάκελο «envelope» που υπάρχει στο μήνυμα. Για διάφορους λόγους τα μηνύματα spam δεν έχουν έγκυρες επικεφαλίδες. Σε αυτό το σημείο κάποιοι πιστεύουν πως τα μηνύματα αυτά πρέπει να απορρίπτονται ενώ άλλοι πιστεύουν πως δεν πρέπει, γιατί λάθη σε επικεφαλίδες υπάρχουν συχνά και σε μηνύματα τα οποία είναι αποδεκτά ως προς το περιεχόμενο.

3.3 Μέθοδοι Antispam

Το φαινόμενο του spam δεν αποτελεί πλέον αποκλειστικό πρόβλημα των χρηστών αλλά και των παροχέων διαδικτυακών υπηρεσιών (Internet Service Providers-ISP), οι οποίοι καλούνται να προστατεύσουν τους πελάτες τους και να θωρακίσουν τους διακομιστές τους (servers) για να μην γίνουν θύματα των spammers. Οι εταιρίες λογισμικού ασφαλείας επιστράτευσαν όλη τους την τεχνογνωσία για να αναπτύξουν ασπίδες προστασίας για τους διακομιστές αλλά και να δημιουργήσουν τις πιο αποτελεσματικές μεθόδους φιλτραρίσματος της ηλεκτρονικής αλληλογραφίας. Οι σημαντικότερες μέθοδοι είναι η «**ευρετική**», σύμφωνα με την οποία ελέγχονται η κεφαλίδα και το σώμα του μηνύματος με την χρήση λέξεων και φράσεων-κλειδιών και η «**στατιστική**», η οποία ουσιαστικά «διαβάζει και μαθαίνει» με το χρόνο τι συνιστά spam. Παράλληλα χρησιμοποιείται και η καταχώριση των ηλεκτρονικών διευθύνσεων σε «λευκές» και «μαύρες» λίστες, διακρίνοντας αντίστοιχα σε αποδεκτή και μη αλληλογραφία. Το ζητούμενο της κάθε μεθόδου είναι η αποφυγή λαθών, για να μην αποκλείσουν κάποιο μήνυμα που μπορεί να είναι σημαντικό για τον παραλήπτη.

Παρά την διαρκή εξέλιξη της τεχνολογίας antispam, οι spammer βρίσκουν πάντα λύσεις για να παρακάμπτουν τα εμπόδια προκαλώντας έτσι όλο και πιο ευφάνταστες αντιδράσεις εκ μέρους των παροχέων υπηρεσιών Internet. Το 2004 παρουσιάστηλε από την εταιρία Lycos μια μέθοδος με τίτλο ‘make love, not spam’. Η μέθοδος αυτή θα εφοδίαζε τους χρήστες με ένα πρόγραμμα, το οποίο θα έστελνε στους αποστολείς spam μεγάλο όγκο δεδομένων για να θέσει εκτός λειτουργίας τους διακομιστές τους. Επειδή όμως τα αποτελέσματα αυτής της τακτικής κρίθηκαν επικίνδυνα, αποσύρθηκε η πρόταση αυτή. Μια ακόμα λύση που προτάθηκε από την Microsoft για τον περιορισμό της μαζικής αποστολής μηνυμάτων ήταν η επιβολή ενός είδους γραμματόσημου, αλλά απορρίφθηκε επειδή προσέκρουσε στην φιλοσοφία της εύκολης και ανέξοδης

επικοινωνίας που χαρακτηρίζει τον κυβερνοχώρο. Για την αντιμετώπιση του spam χρησιμοποιήθηκαν και εργαλεία της βιοπληροφορικής, όπως ο αλγόριθμος Chung-Kwei, που είχε αναπτυχθεί από την IBM για την έρευνα των αλληλουχιών του DNA. Σύμφωνα με τις πρώτες δοκιμές η χρήση του αλγορίθμου σημείωσε 97% επιτυχία στο φιλτράρισμα των μηνυμάτων spam.

Η πιο ελπιδοφόρα λύση προήλθε από την συνεργασία πέντε εκ των κυριότερων παροχέων στις Η.Π.Α (Aol, Yahoo, Hotmail, Comcast, Earthlink), οι οποίοι έθεσαν σε ισχύ δύο νέα πρότυπα πιστοποίησης της ηλεκτρονικής αλληλογραφίας. Πρόκειται για τις τεχνολογίες "**SPF**" (Sender Policy Framework) και "**Sender ID**", που χρησιμοποιούν την λογική αναγνώρισης καλούντος των τηλεφωνικών συνδιαλέξεων. Η χρήση προηγμένων τεχνολογικών παραμέτρων, δίνει την δυνατότητα πιστοποίησης της πηγής προέλευσης ενός εισερχόμενου μηνύματος. Αν ένα μήνυμα δεν πληρεί συγκεκριμένες τεχνικές απαιτήσεις, απορρίπτεται ως spam. Η πρωτοβουλία αυτή, αναμένεται να επιφέρει άμεσα αποτελέσματα στην καταπολέμηση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας.

3.4 Εργαλεία Anti-spamming

Υπάρχουν δύο κύριες κατηγορίες εργαλείων, με την μορφή λογισμικού, που αφορούν την καταπολέμηση των μηνυμάτων spam:

α) Τα εργαλεία που απευθύνονται στους τελικούς χρήστες και β) τα εργαλεία που εγκαθίστανται στους διακομιστές του ηλεκτρονικού ταχυδρομείου.

Τα τελευταία εγκαθίστονται κεντρικά στους διακομιστές του ηλεκτρονικού ταχυδρομείου που διαθέτουν οι παροχείς υπηρεσιών ηλεκτρονικού ταχυδρομείου, οι διάφορες εταιρίες και οργανισμοί ενώ πιο διαδεδομένα είναι τα εργαλεία που μπορούν να εγκαταστήσουν οι τελικοί

χρήστες για να προστατεύσουν την ηλεκτρονική τους αλληλογραφία σε επίπεδο προσωπικού υπολογιστή.

3.4.1 Τεχνικές και εργαλεία για τους τελικούς χρήστες

Οι απλοί χρήστες του Διαδικτύου για να αποφύγουν τα ανεπιθύμητα email, μπορούν να καταφύγουν σε απλές λύσεις. Καταρχάς, οι χρήστες πρέπει να αποφεύγουν την δημοσίευση της ηλεκτρονικής τους διεύθυνσης σε δικτυακούς τόπους, αν αυτό είναι εφικτό. Έχει παρατηρηθεί πως οι διευθύνσεις που κοινοποιούνται στο Διαδίκτυο δέχονται περισσότερα μηνύματα spam σε σχέση με τις διευθύνσεις που δεν κοινοποιούνται. Για τον λόγο αυτό, καλό είναι να γίνεται χρήση δύο ηλεκτρονικών διευθύνσεων. Η μία διεύθυνση να χρησιμοποιείται για την επικοινωνία με γνωστούς, συγγενείς, φίλους και η δεύτερη θα χρησιμοποιείται για απόκτηση πρόσβασης σε διάφορους ιστοχώρους, ηλεκτρονικές κοινότητες και γενικώς σε ιστοσελίδες που θεωρούνται «ύποπτες» ως προς τα στοιχεία που ζητούν.

Σε περίπτωση βέβαια, που είναι απαραίτητη η δημοσίευση του email σε δικτυακούς τόπους, καλό είναι να γίνεται χρήση είτε εικόνων που θα εμφανίζουν την διεύθυνση είτε κάποιου κωδικοποιημένου κειμένου, ώστε να μην είναι εφικτή η καταγραφή του από τους spammers. Η παραποίηση της ηλεκτρονικής διεύθυνσης μπορεί να γίνει με τους εξής τρόπους:

1. με την αντικατάσταση του χαρακτήρα ‘@’ με ‘@’,
2. με την αντικατάσταση όλων των χαρακτήρων με τις HTML οντότητες,
3. με την χρήση JavaScript.

Για παράδειγμα, η διεύθυνση asxetos@hotmail.com σύμφωνα με τους τρεις παραπάνω τρόπους μπορεί να γραφτεί ως εξής :

α) asxetos@hotmail..com

β)Με χρήση **HTML**:

<a href="mailto:asxetos@
hotmail..co
m">asxetos@h
otmail..com

γ) Με χρήση **JavaScript** στο σημείο της σελίδας που θέλουμε να εμφανίζεται η ηλεκτρονική διεύθυνση γράφουμε το εξής:

```
<Script>
  <!..
     document.write(" a href=" + "mail" +  "to :" + "asxetos" + "@" +
"hotmail.com" + ">" + "asxetos <b> @ </b> hotmail.com" </a>)
  --> </Script>
```

Όσο αφορά την χρήση εικόνας, πρέπει να δημιουργηθεί μία εικόνα τύπου GIF ή JPG η οποία θα αποτυπώνει την ηλεκτρονική διεύθυνση που εμφανίζεται στις ιστοσελίδες. Με αυτό τον τρόπο ο αναγνώστης της σελίδας θα μπορεί να την δει αλλά οι μηχανές αναζήτησης των spammers όχι.

Έπειτα, οι χρήστες δεν πρέπει να απαντούν σε μηνύματα spam γιατί γίνονται στόχος για την αποστολή περισσότερων μηνυμάτων. Οι spammers βλέποντας την απάντηση των χρηστών, διαπιστώνουν την εγκυρότητα της διεύθυνσής τους.

Οι χρήστες πρέπει να αποφεύγουν να κάνουν αίτηση για διαγραφή (remove) για τον παραπάνω λόγο. Η διαγραφή των μηνυμάτων αυτών πρέπει να γίνεται χωρίς να τα ανοίγουν. Επίσης, η εγγραφή σε λίστες αλληλογραφίας (mailing lists) πρέπει να αποφεύγεται γιατί οι spammers χρησιμοποιούν προγράμματα για την συλλογή διευθύνσεων από τέτοιου είδους λίστες σε επίσημους δικτυακούς τόπους.

Πρέπει να είναι προσεκτικοί όταν ανοίγουν συνημμένα αρχεία και κάνουν κλικ σε συνδέσμους που περιέχονται στα email, ακόμα και αν γνωρίζουν τον αποστολέα. Εάν, ο αποστολέας δεν μπορεί να επιβεβαιώσει ότι το συνημμένο αρχείο ή ο σύνδεσμος που υπάρχει στο μήνυμα είναι ασφαλή, τότε το καλύτερο είναι να διαγραφεί το μήνυμα.

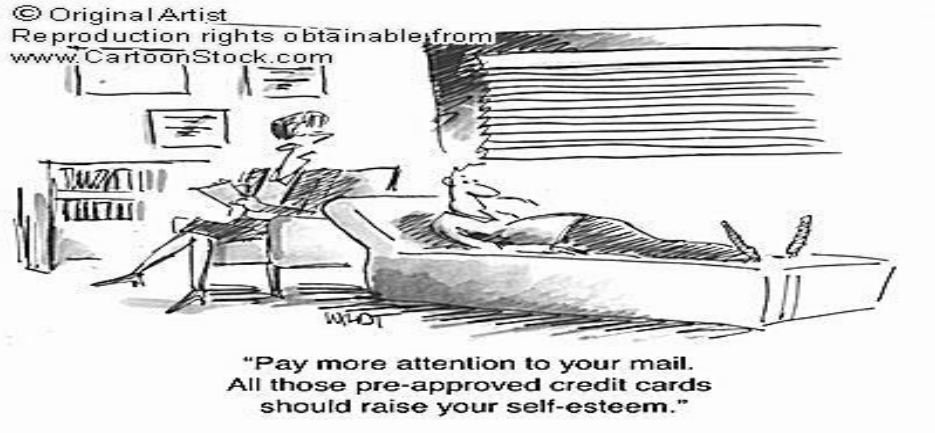
Με την χρήση αντιπροσωπευτικών θεμάτων (subjects) στα μηνύματα που στέλνονται, οι χρήστες κερδίζουν πάρα πολλά αφού είναι απίθανο να θεωρηθεί το μήνυμά τους ως spam από τους παραλήπτες του αλλά και από τα φίλτρα anti-spamming. Αν κάποιος παραλήπτης απαντήσει, ο αποστολέας θα γνωρίζει πως δεν πρόκειται για μήνυμα spam, αφού η απάντηση περιέχει το αρχικό θέμα με την ένδειξη Re:.Έτσι, διευκολύνεται ο χρήστης αλλά και ο αποδέκτης.

Ακόμα, οι χρήστες δεν πρέπει να προωθούν αλυσιδωτά email γιατί από την μία αποκαλύπτουν έτσι την ηλεκτρονική τους διεύθυνση σε άτομα που δεν γνωρίζουν και από την άλλη υπάρχει κίνδυνος να διασπείρουν μία απάτη ή να μεταδίδουν κάποιο ιό. Επιπλέον. Έχουν γίνει αναφορές πως οι spammers χρησιμοποιούν αλυσιδωτά μηνύματα για να συλλέξουν διευθύνσεις email.

Επιπροσθέτως, οι χρήστες δεν πρέπει να αγοράζουν τίποτα από πηγές που δεν είναι αξιόπιστες. Οι spammers συχνά ανταλλάσσουν ή πωλούν τις διευθύνσεις όσων έχουν αγοράσει κάτι από αυτούς. Επιπλέον, πρέπει να δίνεται μεγάλη προσοχή σε μηνύματα, τα οποία υποτίθεται πως στέλνουν γνωστές εταιρίες όπως η Microsoft. Τα μηνύματα αυτά είναι πλαστά και προσπαθούν, εκμεταλλευόμενα την εμπιστοσύνη των χρηστών στο πρόσωπο της εταιρίας, να τους παρασύρουν για να κάνουν κλικ σε κάποιο σύνδεσμο που υπάρχει στο μήνυμα. Κάνοντας κλικ όμως, είτε κατεβάζουν κάποιο επικίνδυνο ιό είτε οδηγούνται στην αποκάλυψη εμπιστευτικών πληροφοριών όπως ο αριθμός πιστωτικής κάρτας κλπ.

Ωφέλιμο για την λύση του προβλήματος του spam θα ήταν οι χρήστες να αναφέρουν τα μηνύματα που λαμβάνουν σε υπηρεσίες του Διαδικτύου και μέσω των λιστών αναφορών για τους spammers που διατηρούν, επιτυγχάνεται ο

περιορισμός του προβλήματος με την βοήθεια των εξυπηρετητών του ηλεκτρονικού ταχυδρομείου.



Εικόνα 6

Ωστόσο, πέρα από τις ενέργειες που μπορεί να κάνει ο κάθε χρήστης για να προστατευτεί από τα μηνύματα spam, υπάρχουν αξιόλογα προϊόντα λογισμικού προστασίας από ιούς (antivirus), τα οποία συμβάλλουν στην προστασία των συστημάτων απέναντι αυτών, αλλά παρέχουν ακόμα και ειδικό λογισμικό τύπου firewall για την προστασία του δικτύου ή του μεμονωμένου υπολογιστή. Υπάρχουν, επίσης και προϊόντα λογισμικού, τα οποία μπορούν και φιλτράρουν τα μηνύματα spam με την χρήση διάφορων τεχνικών.

Στην συνέχεια, θα αναφερθούν κάποια γνωστά προγράμματα που χρησιμοποιούνται για την αποφυγή των μηνυμάτων spam (ή αλλιώς ονομαζόμενα προγράμματα anti-spamming).

Σε αυτό το σημείο πρέπει να τονιστεί πως αν κάποιος χρησιμοποιεί το Web για την διαχείριση των μηνυμάτων του, όπως για παράδειγμα τις υπηρεσίες Hotmail, Yahoo!, In.gr, Gmail κ.α, δεν μπορεί να γίνει χρήση κανενός από τα παρακάτω προγράμματα, αλλά πρέπει να αρκεστεί στην anti-spamming προστασία που προσφέρει ο εκάστοτε παροχέας.

Τα περισσότερα anti-spamming προγράμματα ενσωματώνονται στα γνωστά προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου ως plug-ins,

όπως είναι τα Mozilla Thunderbirb, Eudora, Microsoft Outlook Express κ.α, για να μην χρειαστεί να αλλάξουν οι χρήστες το αγαπημένο τους πρόγραμμα λήψης και αποστολής των ηλεκτρονικών μηνυμάτων τους. Αντίθετα, κάποια άλλα προγράμματα anti-spamming λειτουργούν ανεξάρτητα, παίζοντας τον ρόλο του ενδιάμεσου φίλτρου ανάμεσα στο πρόγραμμα που χρησιμοποιούν οι χρήστες και στους διακομιστές ηλεκτρονικών μηνυμάτων. Σε αυτή την περίπτωση, οι χρήστες πρέπει να κάνουν τις απαραίτητες ρυθμίσεις τόσο στο πρόγραμμα που θα εγκαταστήσουν όσο και στο πρόγραμμα διαχείρισης των μηνυμάτων τους.

3.4.1.1 Τεχνικές / Μέθοδοι για anti-spamming

Όσο αφορά τον τρόπο με τον οποίο τα εργαλεία αυτά κάνουν ανίχνευση των μηνυμάτων spam, χρησιμοποιούνται διάφορες μέθοδοι όπως:

Whitelists/Blacklists: Δίνεται η δυνατότητα στους χρήστες να ορίζουν ποιες ηλεκτρονικές διευθύνσεις δεν αποτελούν πηγή spamming (Whitelist) και ποιες ηλεκτρονικές διευθύνσεις στέλνουν μηνύματα spam (Blacklist). Η τεχνική αυτή είναι χρήσιμη γιατί δεν χάνονται μηνύματα από άτομα που έχουν καταχωρηθεί στις Whitelists, αλλά δεν είναι αποτελεσματική στην ανίχνευση των μηνυμάτων spam που δεν έχουν σταθερή διεύθυνση αλληλογραφίας.

Regular expressions (Συνήθεις Εκφράσεις): Είναι μία από τις παλαιότερες μέθοδοι καταπολέμησης του spam. Τα διάφορα πεδία του email ελέγχονται για ύποπτες λέξεις ή φράσεις που χρησιμοποιούνται από spammers. Τώρα πια όμως, αυτή η τεχνική χρησιμοποιείται είτε συμπληρωματικά είτε καθόλου, γιατί οδηγεί σε μεγάλο αριθμό false negatives (spam που λανθασμένα αναγνωρίζεται ως κανονική αλληλογραφία) αλλά και false positives (κανονική αλληλογραφία, η οποία λανθασμένα θεωρείται spam).

Real Time Block Lists: Πρόκειται για καταλόγους που διατηρούνται και ανανεώνονται από δικτυακούς οργανισμούς. Ανάλογα με το τι περιέχει ο κάθε κατάλογος, διαχωρίζονται σε:

1) spam URL Real Time Block List (sURBL): Κατάλογοι που περιέχουν URL links, τα οποία χρησιμοποιούν οι spammers.
2) Domain Name Servers Block Lists (DNSBL): Κατάλογοι με διευθύνσεις IP και domain names που είναι υπεύθυνα για αποστολή μηνυμάτων spam.
3) Άλλοι κατάλογοι όπως Policy Block Lists (PBL) και Exploit Block Lists (XBL).

Τα στοιχεία του εκάστοτε μηνύματος email συγκρίνονται με τα δεδομένα που περιέχονται στους παραπάνω καταλόγους για να διαπιστωθεί αν πρόκειται για spam ή όχι. Παρόλο που οι RLB χρησιμοποιούνται ευρέως και περιορίζουν αισθητά τα μηνύματα spam, οδηγούν αρκετές φορές σε μαζικά false positives.

Challenge/Response (Πρόκληση / Ανταπόκριση): Μία τεχνική, κατά την οποία σε κάθε νέο email που λαμβάνεται και δεν βρίσκεται σε Whitelist, το πρόγραμμα στέλνει αυτομάτως ένα μήνυμα στον αποστολέα του για την επιβεβαίωση της ταυτότητάς του (challenge) και μόνο όταν αυτός ανταποκριθεί (responce) εμφανίζεται το μήνυμα στον παραλήπτη. Διαφορετικά, το μήνυμα θεωρείται ύποπτο και μπαίνει σε καραντίνα (quarantine). Τα προγράμματα αυτά διασφαλίζουν πως το μήνυμα επιβεβαίωσης δεν μπορεί να απαντηθεί με αυτοματοποιημένο τρόπο, αλλά μόνο από κάποιο άνθρωπο. Τα αποτελέσματα αυτής της τεχνικής είναι ιδιαίτερα καλά αφού οι spammers δεν μπαίνουν στον κόπο να ανταποκριθούν. Ωστόσο, η τεχνική αυτή δημιουργεί προβλήματα όταν τα μηνύματα στέλνονται από λίστες (mailing lists) και στην περίπτωση όπου αποστολέας και παραλήπτης περιμένουν ανταπόκριση ο ένας από τον άλλον!.

Συμπληρωματικές Τεχνικές: Αυτές εξετάζουν αν το domain name του αποστολέα είναι υπαρκτό (Reverse DNS Lookup), αν υπάρχει ο παραλήπτης και αν η διεύθυνση του αποστολέα είναι πραγματική (Spoof Blocking).

Bayesian Content Detection: Μία τεχνική ιδιαίτερα πρωτοποριακή αφού μέσω της στατιστικής και των πιθανοτήτων, εκπαιδεύεται το εκάστοτε φίλτρο για να κατανοήσει τι είναι το spam και στην συνέχεια να μπορέσει να προστατέψει από αυτό. Αν και είναι ευρέως διαδεδομένη εμπορικά τεχνική, στην πράξη απαιτεί πολλή και συνεχή παραμετροποίηση για να λειτουργήσει σωστά.

Signature Content Detection: Μία νέα προσέγγιση είναι να αντιμετωπίζεται το μήνυμα spam ως ιός και να εφαρμόζονται εναντίον του οι ίδιες τεχνικές που εφαρμόζονται από τα προγράμματα antivirus. Η συγκεκριμένη προσέγγιση μηδενίζει σχεδόν τα false positives αλλά απαιτεί συνεχή updates.

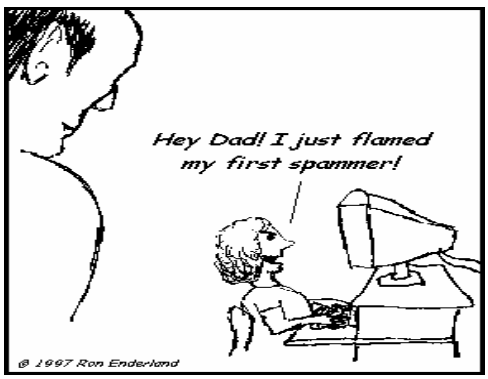
IP Reputation Analysis: Εδώ εξετάζεται η ‘φήμη’ της IP διεύθυνσης του αποστολέα. Ουσιαστικά, αποτελεί μία νέα προσέγγιση των RBL που αναφέρθηκαν παραπάνω.

OCR Readers (Αναγνώστες Οπτικής Αναγνώρισης): Μία νέα και αρκετά διαδεδομένη μορφή spam χρησιμοποιεί εικόνες στις οποίες απεικονίζεται το μήνυμα του spammer. Η καταπολέμηση αυτής της μορφής spam είναι ιδιαίτερα δύσκολη και επίπονη. Ορισμένες προσεγγίσεις αντιμετώπισης του spam χρησιμοποιούν ενσωματωμένους OCR Readers για να «διαβάσουν» το περιεχόμενο της εκάστοτε εικόνας και στην συνέχεια να αποφαίνονται αν πρόκειται για spam ή όχι.

Απόδειξη Εργασίας: Σύμφωνα με αυτή την προσέγγιση, οι νόμιμοι αποστολείς έχουν ουσιαστικά «δουλέψει» για την συγγραφή του email ενώ οι spammers έχουν αυτοματοποιήσει πλέον την διαδικασία αποστολής του. Η βασική ιδέα λοιπόν είναι να συμπεριληφθεί μια απόδειξη εργασίας στο εκάστοτε email.

Κρυπτογραφικές Λύσεις: Η κρυπτογραφία θα χρησιμοποιηθεί για να δώσει λύση και σε αυτό το πληροφοριακό πρόβλημα. Έτσι μέσα από προσεγγίσεις Public Key Infastructure (PKI), ψηφιακές υπογραφές, sender authentication schemes και άλλα κρυπτογραφικά frameworks, υπάρχει η ελπίδα πως θα εξαλειφθεί το spam.

3.4.1.2 Εργαλεία anti-spamming



Εικόνα 7

Για μεγαλύτερη βοήθεια των χρηστών υπάρχουν κάποια γνωστά προγράμματα anti-spamming και αυτά είναι τα εξής:

ØChoice Mail: Οι χρήστες παίζουν μεγάλο ρόλο εφόσον θέτουν τους κανόνες με τους οποίους θα λειτουργήσει το πρόγραμμα. Μπορούν να φτιάξουν φράσεις ή λέξεις κλειδιά για να δέχονται αλλά και να απορρίπτουν μηνύματα που τις περιέχουν. Το πρόγραμμα αυτό χρησιμοποιεί την τεχνική Challenge/Response δηλαδή στέλνει στον αποστολέα ένα μήνυμα στο οποίο ζητά τα στοιχεία του καθώς και τον λόγο που επικοινωνεί με τον χρήστη. Επίσης, τους ζητά να συμπληρώσουν ένα πεδίο, πράγμα εύκολο για άνθρωπο αλλά όχι για

υπολογιστή. Αυτή η διαδικασία περιορίζει σε μεγάλο βαθμό τα μηνύματα spam αφού οι spammers δεν ανταποκρίνονται στο αίτημα του προγράμματος. Αν ο αποστολέας απαντήσει, τότε το πρόγραμμα στέλνει στον χρήστη ένα μήνυμα και ο χρήστης αποφασίζει αν θα δεχτεί ή όχι το μήνυμα αυτό.

ØMailWasher Pro: Με την βοήθεια του προγράμματος αυτού, οι χρήστες μπορούν να δουν τα μηνύματά τους στον mail server. Μπορούν να δουν δηλαδή τους αποστολείς των μηνυμάτων, το θέμα τους και πριν τα κατεβάσουν στην ηλεκτρονική τους θυρίδα, να αποφασίσουν ποια μηνύματα θέλουν και ποιά όχι ώστε να διαγραφούν. Με αυτό τον τρόπο, προστατεύονται από τα spam, τους ιούς και οποιαδήποτε άλλη απειλή μπορεί να παρουσιαστεί. Επίσης, το πρόγραμμα αυτό χρησιμοποιεί Blacklists για να εντοπίζουν τους spammers. Το πρόγραμμα αυτό είναι συμβατό με POP3, IMAP, Hotmail, AOL, MSN λογαριασμούς ηλεκτρονικού ταχυδρομείου.

ØspamBayes: Είναι ένα έξυπνο φίλτρο, το οποίο κατηγοριοποιεί τα μηνύματα που δέχονται οι χρήστες ως «spam», «good», «unsure» και τα τοποθετεί στους αντίστοιχους φακέλους. Χρησιμοποιεί την μέθοδο Bayesian analysis και γίνεται όλο και καλύτερο καθώς αυξάνονται τα μηνύματα που δέχονται οι χρήστες. Πρέπει να εκπαιδευτεί από τον κάθε χρήστη για το ποια μηνύματα θεωρούνται spam και ποια όχι. Στην συνέχεια, το πρόγραμμα αναλύει αυτές τις πληροφορίες όπως ευδιάκριτες λέξεις και φράσεις στην επικεφαλίδα και στο περιεχόμενο και στην συνέχεια χρησιμοποιεί αυτά τα στοιχεία για να εξετάσει τα νέα μηνύματα. Χρησιμοποιείται μόνο με το Outlook και διανέμεται δωρεάν.

ØspamPal: Αυτό το πρόγραμμα, εγκαθίσταται μεταξύ του προγράμματος ηλεκτρονικού ταχυδρομείου και της ταχυδρομικής θυρίδας και ελέγχει τα email όταν ο χρήστης θελήσει να τα ανακτήσει. Τα μηνύματα, που θεωρεί πως είναι spam, ‘βαφτίζονται’ με μία ειδική κεφαλίδα και τοποθετούνται σε ξεχωριστό

φάκελο σε σχέση με τα υπόλοιπα μηνύματα. Για την λειτουργία του χρησιμοποιεί DNSBL λίστες. Οποιοδήποτε email που δεχόμαστε και έχει σταλεί από IP διεύθυνση που βρίσκεται σε αυτές τις λίστες, έχει πολύ μεγάλες πιθανότητες να είναι spam. Οι χρήστες μπορούν να διαλέξουν ποιες από τις υπάρχουσες DNSBL λίστες θα χρησιμοποιήσουν και έτσι το πρόγραμμα ελέγχει τις IP διευθύνσεις των email που υπάρχουν στη θυρίδα, για να δει αν πρόκειται για spam ή όχι. Επίσης, το πρόγραμμα αυτό διαθέτει whitelists για να μην ελέγχονται τα email που λαμβάνονται από συγκεκριμένους αποστολείς και τέλος, διανέμεται δωρεάν.

ØspamBully: Βασίζεται στην τεχνική Bayesian analysis και είναι συμβατό μόνο με Outlook και Outlook Express. Παρέχει Allow/block λίστες για κατηγοριοποίηση των μηνυμάτων ως spam ή όχι ανάλογα με λέξεις ή φράσεις κλειδιά, με την χώρα προέλευσης και με την γλώσσα που χρησιμοποιείται. Το πρόγραμμα απαιτεί μια αρχική εκπαίδευση για το τι θεωρεί ο χρήστης spam και τι όχι και στην συνέχεια το πρόγραμμα «μαθαίνει» μόνο του από τα νέα μηνύματα που λαμβάνει. Ακόμα παρέχει και στατιστική απεικόνιση των μηνυμάτων που δέχθηκε σε σχέση με το είδος τους. Τέλος, με την επιλογή ενός μηνύματος από τον χρήστη υπάρχει στο πρόγραμμα το πλαίσιο ‘Message Details’, το οποίο εξηγεί για ποιο λόγο το μήνυμα χαρακτηρίστηκε ως spam και δείχνει την IP διεύθυνση του αποστολέα καθώς και την τοποθεσία από την οποία το έστειλε μέσω ενός μικρού παγκόσμιου χάρτη.

ØspamWeasel: Το spamWeasel είναι ένα από τα πιο ισχυρά εργαλεία antispam καθώς χρησιμοποιεί μία ολοκληρωμένη scripting γλώσσα για φίλτρα. Λειτουργεί ως εξυπηρετητής μεταξύ του προγράμματος ηλεκτρονικού ταχυδρομείου και του POP server όπου συλλέγονται τα εισερχόμενα μηνύματα. Χρησιμοποιεί κάποια προκαθορισμένα φίλτρα, τα οποία αρχειοθετούν, χαρακτηρίζουν, μπλοκάρουν και διαγράφουν τα μηνύματα spam και θέλουν

απλώς κάποιες ρυθμίσεις από τους χρήστες. Χρησιμοποιείται μόνο με POP λογαριασμούς και διανέμεται δωρεάν.

Øspamihilator: Με την εγκατάσταση του, εμφανίζεται ο βοηθός του προγράμματος ο οποίος βοηθά στην επιλογή του προγράμματος ηλεκτρονικού ταχυδρομείου και επιβεβαιώνει την ηλεκτρονική διεύθυνση του χρήστη. Παρέχει την δυνατότητα δημιουργίας λίστας γνωστών αποστολέων καθώς και αποστολέων μηνυμάτων spam. Χρησιμοποιεί την μέθοδο Bayesian analysis και με την εκπαίδευση του χρήστη, γίνεται όλο και καλύτερο. Παρέχει ήδη φίλτρο διαχωρισμού των μηνυμάτων με βάση λέξεις κλειδιά, στο οποίο ο χρήστης μπορεί να προσθέσει και καινούργιες λέξεις. Τα μηνύματα spam διαχωρίζονται αμέσως από τα υπόλοιπα μηνύματα αφού τοποθετούνται στον κάδο απορριμμάτων του προγράμματος. Το πλεονέκτημα αυτού του προγράμματος είναι ότι εκτός από τα ήδη εγκατεστημένα φίλτρα σε αυτό, μπορεί να ενσωματώσει και άλλα ως plug-ins όπως φίλτρα Blacklist, Alphabetpoup κ.α. Διανέμεται δωρεάν.

ØspamFighter: Με την εγκατάσταση του προγράμματος, εμφανίζεται στο Outlook το εικονίδιό του και τα κουμπιά «Block» και «Unblock». Με μία σειρά βημάτων το πρόγραμμα βοηθά στην ρύθμιση του τείχου προστασίας (firewall) και των λογαριασμών email καθώς και στην δημιουργία black και white λιστών. Όταν ο χρήστης ελέγχει την αλληλογραφία του, το σύστημα αυτόματα την ελέγχει για το αν υπάρχουν spam, σύμφωνα πάντα με τα δεδομένα του διακομιστή του spamfighter. Αν κάποιο μήνυμα αναγνωριστεί ως spam, μετακινείται αυτόματα στον φάκελο spam. Στα θετικά αυτού του προγράμματος είναι και η υποστήριξη πολλών γλωσσών μεταξύ αυτών και τα Ελληνικά καθώς και η πολύ καλή on-line βοήθεια του διαθέτει.

ØMcAfee spamKiller: Είναι συμβατό με Hotmail, MSN, POP3 και IMAP λογαριασμούς ηλεκτρονικού ταχυδρομείου. Με την εγκατάστασή του επιλέγεται ο λογαριασμός του ηλεκτρονικού ταχυδρομείου που θα ελέγχεται. Το πρόγραμμα αυτό μπλοκάρει τα μηνύματα spam με την χρήση των ήδη υπάρχοντων φίλτρων ελέγχοντας την διεύθυνση του αποστολέα, την κεφαλίδα και το περιεχόμενο του μηνύματος καθώς και την χώρα προέλευσης. Τα φίλτρα αυτά ανανεώνονται καθημερινώς και τέλος οι χρήστες μπορούν να δημιουργήσουν νέα φίλτρα με την βοήθεια ενός οδηγού που παρέχει το πρόγραμμα. Τα μηνύματα spam που εντοπίζονται, τοποθετούνται στο φάκελο 'Killed Mail' και διαγράφονται αυτόματα. Σε περίπτωση που οι χρήστες θέλουν να 'πολεμήσουν' τους spammers με την βοήθεια αυτού του προγράμματος μπορούν να στείλουν μηνύματα παραπόνων. Στέλνοντας αυτοματοποιημένα μηνύματα παραπόνων, οι spammers πιστεύουν πως οι διευθύνσεις των χρηστών είναι άκυρες. Το πρόγραμμα αυτομάτως βρίσκει και προτείνει τις ηλεκτρονικές διευθύνσεις των spammers, ιστότοπων, παροχέων υπηρεσιών internet και η αποστολή των παραπόνων γίνεται ουσιαστικά με το πάτημα λίγων κουμπιών. Το αποτέλεσμα των παραπόνων αυτών είναι η ακύρωση των ηλεκτρονικών λογαριασμών των spammers.

Ø*E*-Trust *Anti*-Spam:Το e-trust antispam είναι ένα ασφαλές, αποτελεσματικό και το εύχρηστο φίλτρο spam. Χρησιμοποιώντας μία whitelist εμποδίζει τα μηνύματα spam και επιτρέπει να φθάσουν στον υπολογιστή μόνο τα μηνύματα από εγκεκριμένους αποστολείς. Τα εισερχόμενα μηνύματα μπαίνουν σε φάκελο καραντίνας από το e-trust antispam. Μόλις εγκριθεί ένας αποστολέας τότε τα μηνύματά του κινούνται προς το Inbox. Επίσης, μπορεί να χτίσει έναν κατάλογο εγκεκριμένων αποστολέων από τα ηλεκτρονικά ταχυδρομεία βιβλίων διευθύνσεων. Τέλος, ενημερώνει τον εγκεκριμένο κατάλογο με την ανίχνευση του εξερχόμενου ηλεκτρονικού ταχυδρομείου για τους παραλήπτες. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου μπορούν να εγκριθούν ή να

αφαιρεθούν από το whitelist με το χέρι και από τα υπάρχοντα μηνύματα. Προαιρετικά, μπορεί να στείλει ένα προκλητικό μήνυμα στους άγνωστους αποστολείς. Τα μηνύματα Quarantined μπορούν να διαγραφούν αυτόματα μετά από έναν καθορισμένο χρόνο στο φάκελο καραντίνας. Η απάντηση στην πρόκληση θα τους εγκρίνει. Αυτό μπορεί να είναι λίγο ενοχλητικό, αν και είναι αρκετά έξυπνο για τους καταλόγους διευθύνσεων και σιγουρεύεται για την έγκριση ενός μηνύματος.

Ø**K9:** Το K9 είναι μια εφαρμογή φιλτραρίσματος ηλεκτρονικού ταχυδρομείου που λειτουργεί από κοινού με το κανονικό POP3 πρόγραμμα ηλεκτρονικού ταχυδρομείου και ταξινομεί αυτόματα τα εισερχόμενα ηλεκτρονικά μηνύματα ως spam ή μη spam. Χρησιμοποιεί την ευφυή στατιστική ανάλυση που μπορεί να οδηγήσει στην εξαιρετικά υψηλή ακρίβεια κατά τη διάρκεια του χρόνου. Το K9 μαθαίνει από τα λάθη του και γίνεται όλο και καλύτερο ώστε να είναι σε θέση να προσδιορίσει τα spam. Δεν υποστηρίζει άμεσα Hotmail, AOL ή οποιοδήποτε άλλο είδος συστημάτων τύπων webmail, ούτε υποστηρίζει τη SSL ή την ασφαλή επικύρωση όπως χρησιμοποιείται από MSN.

Ø**Mailfilter:** Το Mailfilter είναι ένα πολύ χρήσιμο εργαλείο για τα λειτουργικά συστήματα Unix, επειδή μπορεί να ξεφορτωθεί τα spam e-mail, πριν αυτά περάσουν στον τοπικό υπολογιστή. Το Mailfilter συνδέεται με οποιοδήποτε γραμματοκιβώτιο και συγκρίνει μέρος του περιεχομένου του με ένα σύνολο καθορισμένων κανόνων που έχει θέσει ο χρήστης. Με το Mailfilter ο χρήστης μπορεί να καθορίσει τα φίλτρα (κανόνες) ώστε να γίνει διαχωρισμός μεταξύ των μηνυμάτων που πρέπει να παραδοθούν και αυτών που θεωρούνται απόβλητα. Οι κανόνες που χρησιμοποιούνται είναι κανονικές εκφράσεις, έτσι ώστε να μπορεί ο χρήστης να χρησιμοποιεί τις γνωστές επιλογές από άλλα προγράμματα παράδοσης ταχυδρομείου όπως π.χ. procmail.

Ø<u>Spamfire:</u> Το Spamfire είναι ένα antispam φίλτρο που αφαιρεί τα ανεπιθύμητα, εμπορικού και πορνογραφικού περιεχομένου, μηνύματα από το ηλεκτρονικό ταχυδρομείο. Εάν ένα μήνυμα μοιάζει με spam τότε το μεταφορτώνει έτσι ώστε να μπορεί ο χρήστης να αναθεωρήσει αργότερα και να το διαγράψει από τον κεντρικό υπολογιστή. Όταν το Spamfire τελειώνει τον έλεγχο, ενεργοποιεί το πρόγραμμα ηλεκτρονικού ταχυδρομείου και παραδίδει τα "καλά" μηνύματα στο γραμματοκιβώτιο του χρήστη. Το Spamfire έχει επίσης έναν κατάλογο φίλων που μπορεί να εισαχθεί από το βιβλίο διευθύνσεων του προγράμματος ηλεκτρονικού ταχυδρομείου και δέχεται πάντα τα μηνύματα από τις διευθύνσεις σε εκείνο τον κατάλογο.

3.4.2 Εργαλεία για διακομιστές ηλεκτρονικού ταχυδρομείου

Εκτός τις ενέργειες και τα εργαλεία που μπορούν να χρησιμοποιήσουν οι χρήστες για την προστασία τους από την ανεπιθύμητη αλληλογραφία σε προσωπικό επίπεδο, υπάρχουν λύσεις όσο αφορά την προστασία των χρηστών που εφαρμόζονται στους διακομιστές ηλεκτρονικής αλληλογραφίας. Οι λύσεις αυτές εφαρμόζονται είτε πριν την είσοδο των μηνυμάτων spam στα γραμματοκιβώτια των χρηστών είτε δεν αφήνουν μηνύματα που πρόερχονται από spammers να εισέρχονται στους διακομιστές.

Οι λύσεις που υπάρχουν, συγκεντρώνονται στα ακόλουθα σημεία:

1. **Έλεγχος εγκυρότητας στο DNS και στους headers:** Αν τα μηνύματα προέρχονται από εξυπηρετητές email, οι οποίοι δεν έχουν έγκυρες δηλώσεις DNS απορρίπτονται. Επίσης, τα μηνύματα διαγράφονται αυτόματα αν στην ηλεκτρονική τους διεύθυνση το domain name (τμήμα μετά το @) δεν υπάρχει στο DNS.
2. **Χρήση SMTP server για την απόρριψη γνωστών spammers**: Ο διακομιστής εισερχόμενης αλληλογραφίας (SMTP) αρνείται να λάβει και απορρίπτει τα μηνύματα που προέρχονται από servers οι οποίοι είτε διακινούν

spam είτε δεν ικανοποιούν τις απαιτούμενες προδιαγραφές ασφάλειας, οπότε μπορούν να χρησιμοποιηθούν από spammers για διακίνηση μηνυμάτων spam. Η λύση αυτή βασίζεται στην χρήση Real Time Block Lists (RBL) και είναι μία πρακτική που εφαρμόζεται από πολλούς παροχείς υπηρεσιών ηλεκτρονικού ταχυδρομείου.

3. Παρακολούθηση: Παρακολουθείται η κίνηση των email με στόχο να εντοπιστεί η αποστολή μεγάλου αριθμού μηνυμάτων από συγκεκριμένους αποστολείς, οι οποίοι θα μπορούσαν να είναι spammers, ειδικά αν το φαινόμενο είναι επαναλαμβανόμενο.

4. Φιλτράρισμα των SMTP συνδέσεων: Γίνεται χρήση φίλτρων, τα οποία δεν επιτρέπουν την σύνδεση στους διακομιστές αλληλογραφίες από γνωστούς εξυπηρετητές που διακινούν μηνύματα spam.

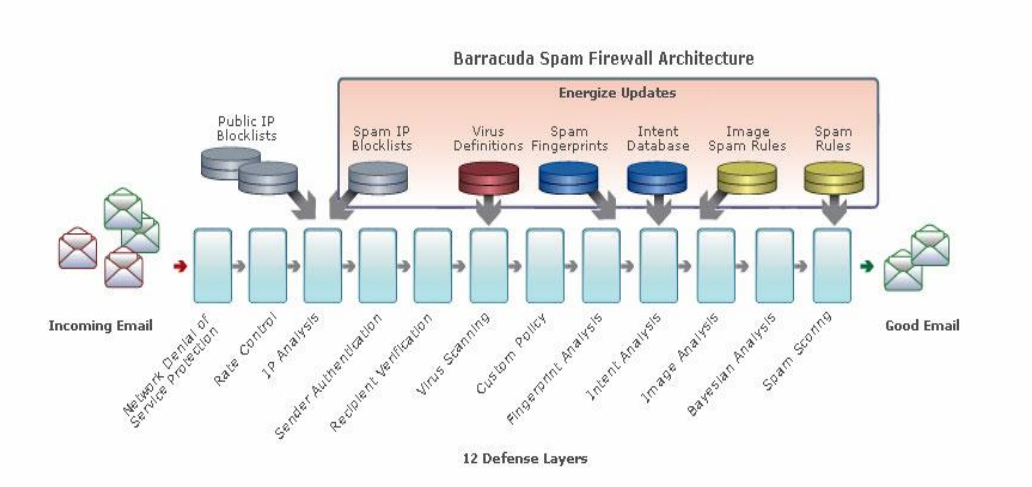
5. Χρήση προγραμμάτων προστασίας στον διακομιστή: Μια σειρά από λύσεις προστασίας με φίλτρα και εξελιγμένες τεχνικές όπως Bayesian filtering μπορούν να εφαρμοστούν στους διακομιστές. Τέτοιου είδους εργαλεία είναι είτε εμπορικά είτε ελεύθερου λογισμικού, που είναι διαθέσιμα και μπορούν να χρησιμοποιηθούν.

Στην συνέχεια, παρουσιάζονται ορισμένα anti-spamming προγράμματα για την προστασία διάφορων οργανισμών ή εταιριών. Αυτά είναι τα εξής:

1. **Barracuda Spam Firewall:** Πρόκειται για μία ολοκληρωμένη λύση προστασίας για τους διακομιστές ηλεκτρονικού ταχυδρομείου. Παρέχει μια ισχυρή και εύκολη στην χρήση λύση για την εξάλειψη των μηνυμάτων spam και των ιών αφού περιλαμβάνει anti-spam, anti-virus, anti-spoofing, anti-phishing, anti-spyware και denial of service. Το προϊόν αυτό προστατεύει τους διακομιστές των επιχειρήσεων με την χρήση δύο κατηγοριών από τεχνικές, οι οποίες αναλύονται σε δώδεκα αμυντικά επίπεδα. Οι κατηγορίες αυτές είναι:

α) Τεχνικές Διαχείρισης Σύνδεσης (**Connection Management**), οι οποίες ελέγχουν τις εισερχόμενες συνδέσεις πριν ακόμα ληφθούνε τα μηνύματα και β) Τεχνικές Ανίχνευσης Μηνυμάτων (**Mail Scanning**), οι οποίες ελέγχουν τα μηνύματα από την στιγμή που ληφθούν.

Το σχήμα που ακολουθεί, απεικονίζει αυτά τα αμυντικά επίπεδα.



Διάγραμμα 3

Αυτά είναι τα εξής:

Network Denial of Service Protection: Λαμβάνει όλα τα μηνύματα εξ'ονόματος της επιχείρησης και έτσι ο διακομιστής της επιχείρησης δεν λαμβάνει απευθείας τα επικίνδυνα μηνύματα.

***Rate control*:** Αυτοματοποιημένα συστήματα μπορούν να στείλουν μεγάλο αριθμό μηνυμάτων σε μόνο ένα διακομιστή. Για την προστασία του ηλεκτρονικού ταχυδρομείου, το προϊόν αυτό μετρά τις εισερχόμενες συνδέσεις από συγκεκριμένες IP διευθύνσεις και όταν αυτές ξεπεράσουν ένα ορισμένο όριο, τις κόβει.

***IP analysis*:** Μόλις ολοκληρωθεί ο έλεγχος ποσοστού εμφάνισης των IP διευθύνσεων, το πρόγραμμα ελέγχει τις IP διευθύνσεις για το ποια μηνύματα θα δεχτεί και ποια όχι. Ελέγχει δηλαδή ποια μηνύματα πελατών θα δεχθεί με βάση τις white και black λίστες που έχει δημιουργήσει η εκάστοτε εταιρία. Επίσης, η κεντρική εταιρία (Baraccuda Central) διαθέτει λίστες με

διευθύνσεις IP από γνωστούς spammers και είναι διαθέσιμες για το προϊόν αυτό μέσω των συνεχών ανανεώσεων (updates).

***Sender Authentication*:** Επειδή οι spammers στα μηνύματα που στέλνουν χρησιμοποιούν άκυρες διευθύνσεις, το προϊόν αυτό χρησιμοποιεί κάποιες τεχνικές για να επικυρώσει την διεύθυνση του αποστολέα. Καταρχάς, ελέγχει αν το πρωτόκολλο που χρησιμοποιεί ο αποστολέας είναι έγκυρο. Έπειτα, ελέγχει αν το domain name που χρησιμοποιεί ο αποστολέας είναι πραγματικό και προστατεύει από μηνύματα με σκοπό το spoofing.

***Recipient Verification*:** Το προϊόν αυτό ελέγχει αν ισχύουν οι διευθύνσεις των μηνυμάτων που λαμβάνει, χρησιμοποιώντας τεχνικές όπως είναι η πιστοποίηση μέσω πρωτοκόλλων όπως είναι τα LDAP και SMTP.

Τα προαναφερθέντα επίπεδα ανήκουν στις τεχνικές διαχείρισης σύνδεσης. Παρακάτω, αναφέρονται τα επίπεδα που ανήκουν στις τεχνικές ανίχνευσης μηνυμάτων.

Virus Scanning: Το πιο βασικό επίπεδο στον έλεγχο των μηνυμάτων είναι ο έλεγχος για την ύπαρξη ιών. Το προϊόν αυτό, ελέγχει τα εισερχόμενα μηνύματα κατά την διάρκεια των τεχνικών διαχείρισης σύνδεσης ακόμα και όταν αυτά στέλνονται από IP διευθύνσεις που βρίσκονται σε white λίστες και μπλοκάρονται αν ανιχνευθεί σε αυτά ιός.

***Custom policy*:** Ο κάθε χρήστης μπορεί, εκτός από τους ήδη ισχύοντες κανόνες προστασίας από τα μηνύματα spam που χρησιμοποιεί το προϊόν μέσω των διαρκών ανανεώσεων από την κεντρική εταιρία (Barracuda Central), να θέσει σε λειτουργία φίλτρα που θα ελέγχουν το θέμα, τις κεφαλίδες και το περιεχόμενο των μηνυμάτων καθώς και τα συνημμένα σε αυτά αρχεία.

***Fingerprint Analysis*:** Ελέγχονται τα μηνύματα για το αν περιέχουν τμήματα, όπως είναι οι εικόνες, που συνήθως βρίσκονται σε μηνύματα spam.

***Intent Analysis*:** Επειδή όλα τα μηνύματα spam περιέχουν διάφορους συνδέσμους, αν στα εισερχόμενα μηνύματα υπάρχουν σύνδεσμοι για

ιστοσελίδες ή για τηλεφωνική επικοινωνία, αυτοί οι σύνδεσμοι ελέγχονται για το αν σχετίζονται με ισχύουσες τοποθεσίες. Συνήθως, σε αυτό το επίπεδο εντοπίζονται μηνύματα που έχουν σκοπό το phishing.

***Image Analysis*:** Τα μηνύματα spam που περιέχουν εικόνες αποτελούν το 1/3 του συνόλου των μηνυμάτων που κυκλοφορούν στο Διαδίκτυο. Ουσιαστικά, ελέγχονται οι εικόνες για το αν περιέχουν κείμενο που μπορεί να αποτελεί spam.Επίσης, περιέχει ειδικούς αλγόριθμους για την ανάλυση τρισδιάστατων σχεδίων, αν αποτελούν κίνδυνο ή όχι.

***Bayesian Analysis*:** Είναι ένας αλγόριθμος που χρησιμοποιείται και σε μηνύματα spam αλλά και σε νόμιμα μηνύματα. Ελέγχει και συγκρίνει συγκεκριμένες λέξεις και φράσεις που έχουν χρησιμοποιηθεί στο νέο εισερχόμενο μήνυμα σε σχέση με τα προηγούμενα μηνύματα που έχουν ληφθεί. Το προϊόν αυτό, χρησιμοποιεί αυτή την τεχνική μόνο αν ο κάθε χρήστης έχουν δεχθεί προηγουμένως τουλάχιστον 200 νόμιμα και 200 spam μηνύματα.

***Spam Scoring*:** Εκτός από τους φραγμούς που μπορεί κάθε φίλτρο να πραγματοποιήσει, το προϊόν περιλαμβάνει και ένα μηχανισμό, ο οποίος βαθμολογεί τους παράγοντες με τους οποίους λειτουργεί το κάθε φίλτρο ξεχωριστά. Ο συνδυασμός των κανόνων με τις βαθμολογίες μπορεί να δώσει ένα δυνατό αποτέλεσμα ως προς τα μηνύματα spam.

2. Spam Assassin: Το πρόγραμμα αυτό διανέμεται δωρεάν. Εγκαθίσταται στον διακομιστεί και ελέγχει τα μηνύματα πριν φτάσουν στην ταχυδρομική θυρίδα. Πρόκειται για ένα ευρέως διατιθέμενο και ανοικτού λογισμικού πρόγραμμα, το οποίο με βάση κάποιους κανόνες βαθμολογεί τα μηνύματα και χρησιμοποιείται για την ταυτοποίηση των μηνυμάτων spam. Η ταυτοποίηση αυτή γίνεται με την χρήση μιας ποικιλίας τεχνικών, όπως είναι:

Email Header Analysis: Ελέγχονται οι κεφαλίδες των μηνυμάτων για το αν περιέχουν στοιχεία που να οδηγούν στο συμπέρασμα πως πρόκειται για spam.

Keyword Checking and Text Analysis: Ελέγχεται το περιεχόμενο του μηνύματος για στοιχεία που υποδηλώνουν πως είναι spam όπως ύποπτες λέξεις που χρησιμοποιούν οι spammers ή σύνδεσμοι σε άλλες ιστοσελίδες ή προσκλήσεις για αγορές.

Bayesian Spam Filtering: Υπολογίζεται με στατιστικές μεθόδους η πιθανότητα ένα εισερχόμενο μήνυμα να είναι spam. Αυτά τα φίλτρα μπορούν να εκπαιδευτούν, για να μπορούν να εντοπίσουν τα μηνύματα spam πιο εύκολα στο μέλλον.

Realtime DNS Blacklist Checking: Γίνεται έλεγχος σε blacklists για να διαπιστωθεί αν το εισερχόμενο μήνυμα έχει σταλεί από γνωστό spammer ή αν πρόκειται για αναμετάδοση γνωστού μηνύματος spam.

Multiple SURBL Checking: Επειδή οι spammers επιδιώκουν οι χρήστες να κλικάρουν σε υπερσυνδέσεις που οδηγούν στους δικούς τους ιστότοπους, μία έρευνα σε μια βάση δεδομένων με γνωστούς ιστότοπους που περιέχουν διαφημίσεις αποτελεί τον καλύτερο τρόπο για την ταυτοποίηση των μηνυμάτων spam. Παρομοίως, οι SURBL λίστες μπλοκάρουν τα μηνύματα που περιέχουν υπερσυνδέσεις σε γνωστούς ιστότοπους με spam.

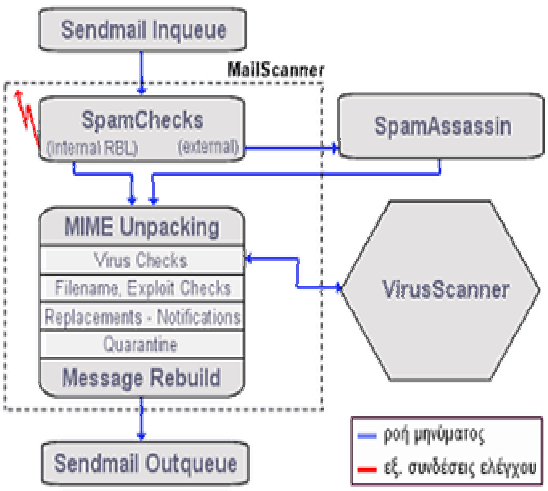
SPF (Sender Policy Framework) Support: Ανιχνεύονται λανθασμένες διευθύνσεις αποστολέων στα μηνύματα.

Automatic Whitelist Management: Αναγνωρίζει αυτόματα τις νόμιμες διευθύνσεις αποστολέων.

White and Black Lists: Αυτές οι λίστες χρησιμοποιούνται γιατί ορίζονται ποιες ηλεκτρονικές διευθύνσεις είναι νόμιμες και ποιες όχι.

Τα αποτελέσματα αυτών των τεχνικών προστίθενται και καταλήγει στην τελική βαθμολογία. Ένα μήνυμα θεωρείται spam εάν η βαθμολογία του ξεπεράσει μία καθορισμένη τιμή.

3. MailScanner: Πρόκειται για μια εφαρμογή ανοικτού λογισμικού, η οποία διατίθεται δωρεάν και λόγω της σταθερότητάς του, της επεκτασιμότητάς του και γενικότερα της απόδοσής του έγινε πολύ σύντομα δημοφιλές στους κύκλους των open source εγαρμογών ασφαλείας για email gateways, με αποτέλεσμα να χρησιμοποιείται σήμερα σε πάνω από 20.000 ιστοσελίδες παγκοσμίως, συμπεριλαμβανομένων γνωστών κυβερνητικών, εκπαιδευτικών και εμπορικών ιστοσελίδων.



Ως προς την λειτουργία του, το πρόγραμμα υλοποιεί τα τρία φίλτρα προστασίας (virus, attachment και spam). Η ουρά μηνυμάτων, η οποία αποτελείται από μηνύματα που είτε θα προωθηθούν σε τοπικό χρήστη είτε θα αναμεταδοθούν σε κάποιον άλλο εξωτερικό domain, διασπάται σε δύο μέρη, το τμήμα της λήψης (sendmail inqueue) και το τμήμα αποστολής (sendmail Outqueue). Το Mailscanner ανιχνεύει την ουρά λήψης και παίρνει το πρώτο μήνυμα για να ελέγξει αν πρόκειται για spam ή όχι. Ο έλεγχος αυτός γίνεται είτε με την ενσωματωμένη στο πρόγραμμα δυνατότητα επικοινωνίας με δημόσιες λίστες που περιλαμβάνουν servers που έχουν καταχωρηθεί για προώθηση μηνυμάτων spam (RBL check) είτε μέσω εξωτερικών προγραμμάτων για έλεγχο spam όπως είναι τα spamAssassin, ClamAV.

Αφού το μήνυμα ελεγχθεί και χαρακτηριστεί ως spam ή not spam, αποσυντίθεται από την δομή MIME στην οποία βρίσκεται, ξεχωρίζονται δηλαδή και αποκωδικοποιούνται τα επισυναπτόμενα αρχεία και το κυρίως μήνυμα. Κάθε επισυναπτόμενο αρχείο ελέγχεται από το anti-virus και αν αυτό δώσει αναφορά πως κάποιο από τα αρχεία βρέθηκε μολυσμένο, τότε το αρχείο αυτό τοποθετείται σε καραντίνα (Quarantine) στο δίσκο του

mailserver, έχοντας ταξινομηθεί κατά ημερομηνία λήψης και message ID του συγκεκριμένου μηνύματος, ενώ ταυτόχρονα ετοιμάζεται αναφορά προς τον αποστολέα και τον παραλήπτη. Στην συνέχεια γίνεται ο έλεγχος των extension των αρχείων σε σχέση με την λίστα των μη αποδεκτών filename extensions. Παρόμοια με τα παραπάνω, αν κάποιο αρχείο έχει extension που δεν είναι αποδεκτό, τοποθετείται σε καραντίνα και ετοιμάζεται αναφορά προς τον αποστολέα και τον παραλήπτη για τους λόγους κατακράτησης του συγκεκριμένου αρχείου.

Στο τελικό στάδιο το μήνυμα επανασυντίθεται σε δομή MIME, περιλαμβάνοντας όμως μόνο τα αρχεία που δεν υπήρξε κάποια αναφορά ενώ για όσα υπήρξε γίνεται αντικατάσταση με ένα επισυναπτόμενο αρχείο κειμένου το οποίο εξηγεί για ποιους λόγους παρακρατήθηκαν καθώς και τους τρόπους που μπορούν να ανακτηθούν. Το μήνυμα τοποθετείται στην ουρά μηνυμάτων για αποστολή ώστε να φτάσει στον παραλήπτη και ταυτόχρονα στέλνονται η αναφορά στον αποστολέα του μηνύματος και η ειδοποίηση στον διαχειριστή του συστήματος.

4. **Sender Policy Framework**: Πρόκειται για επέκταση του πρωτοκόλλου SMTP, η οποία εμποδίζει τους spammers να πλαστογραφήσουν τις διευθύνσεις των ηλεκτρονικών μηνυμάτων. Επειδή το πρωτόκολλο SMTP δεν περιέχει μηχανισμούς επικύρωσης, το SPF σαν προέκτασή του παρέχει σχέδια επικύρωσης προσδιορίζοντας ποιοι υπολογιστές μπορούν να στέλνουν ηλεκτρονικά μηνύματα από ένα συγκεκριμένο τομέα (domain). Για να χρησιμοποιηθεί το SPF χρειάζονται δύο μέρη:
α) ο ιδιοκτήτης του domain, ο οποίος δημοσιεύει αυτές τις πληροφορίες σε μία SPF αναφορά στις DNS εγγραφές και όταν ένας άλλος εξυπηρετητής (server) λαμβάνει ένα μήνυμα το οποίο ενδέχεται να έχει σταλεί από αυτόν τον domain, τότε ο β) ο παραλήπτης εξυπηρετητής (server) μπορεί να ελέγξει αν το μήνυμα έχει σταλεί από ηλεκτρονική διεύθυνση

εξουσιοδοτημένου αποστολέα που ανήκει στον συγκεκριμένο domain. Σε περίπτωση, που το μήνυμα προέρχεται από μη εξουσιοδοτημένο domain, ο εξυπηρετητής δεν θα διαβιβάσει το μήνυμα στον προορισμό του.

Το SPF είναι μια μέθοδος η οποία χρησιμοποιείται για να σταματήσει η αποστολή μηνυμάτων spam από μη εξουσιοδοτημένους domains. Παρ'όλα αυτά, πρέπει να σημειωθεί πως το SPF εμποδίζει τους spammers μόνο ως προς την πλαστογράφηση των ηλεκτρονικών διευθύνσεων και δεν όχι ως προς την αποστολή μηνυμάτων spam από τους domain που είναι εγγεγραμμένοι.

5. Mailwasher Server: Πρόκειται για μία εφαρμογή ανοιχτού λογισμικού, η οποία υποστηρίζει πλήρως τα συστήματα Windows Server/Exchange Server καθώς και συστήματα βασισμένα στην Unix όπως είναι τα Linux και Solaris με ενσωματωμένα τα Sendmail και Qmail. Μόλις το μήνυμα εισέλθει στον Mailwasher Server ελέγχεται πρώτα με βάση τις παγκόσμιες και ατομικές white και black λίστες και έπειτα ελέγχεται από την κεντρική βάση δεδομένων (FirstAlert!) της κατασκευάστριας εταιρίας Firetrust. Τέλος, αν δίνεται αυτή η δυνατότητα, το μήνυμα μπορεί να ελεγχεί με βάση RBL λίστες και φίλτρα που χρησιμοποιούν τεχνικές Bayesian analysis. Σε κάθε περίπτωση, αν το μήνυμα χαρακτηριστεί ως spam τοποθετείται σε καραντίνα.

6. Spamstats: Διανέμεται δωρεάν. Το πρόγραμμα αυτό αναλύει τα δεδομένα απο το spamassassin, το γραμματοκιβώτιο κάθε χρήστη (εταιρίας) καθώς και τα δεδομένα που έχει συγκεντρώσει ο server με σκοπό την εξαγωγή χρήσιμων πληροφοριών με την κυκλοφορία των μηνυμάτων spam στο διαδίκτυο. Δίνει αναφορά σχετικά με το σύνολο των μηνυμάτων spam και των νόμιμων μηνυμάτων που λαμβάνει το γραμματοκιβώτιο της. Δίνει και άλλες χρήσιμες πληροφορίες όπως λίστες με ηλεκτρονικές διευθύνσεις

που είναι spam και ανήκουν στο domain της εταιρίας κλπ.

Συμπεράσματα

Με την ολοκλήρωση της εργασίας, καταλήξαμε στα ακόλουθα συμπεράσματα:

Με την συνεχή εξέλιξη του ηλεκτρονικού εμπορίου, τα θέματα ασφάλειας και η προστασία των προσωπικών δεδομένων θα αποτελούν πάντα αχίλλειο πτέρνα του συστήματος, με αποτέλεσμα οι περισσότεροι καταναλωτές–χρήστες να φοβούνται να προβούν σε τέτοιου είδους συναλλαγές. Βέβαια, η ισχύουσα νομοθεσία για το ηλεκτρονικό εμπόριο και για την μη ζητηθείσα ηλεκτρονική αλληλογραφία δημιουργούν ένα ασφαλές περιβάλλον για τις ηλεκτρονικές συναλλαγές. Παράλληλα, έχουν αναπτυχθεί αρκετά λογισμικά για την ασφάλεια των πληροφοριών και την προστασία των προσωπικών δεδομένων σε επίπεδο χρήστη, παροχέων υπηρεσιών Διαδικτύου και όσων εμπλέκονται στις ηλεκτρονικές συναλλαγές, που κάνουν πιο εύκολη την όλη διαδικασία.

Αν και το Διαδίκτυο αποτελεί ένα πολύ σημαντικό εργαλείο για όλους μας, οι κίνδυνοι που ελλοχεύουν καθημερινά κάνουν την χρήση του όλο και πιο δύσκολη. Οι spammers βρίσκουν συνεχώς καινούργιους τρόπους για να εισβάλλουν στους υπολογιστές των χρηστών με σκοπό την συγκομιδή πληροφοριών όπως κωδικούς τραπεζικών λογαριασμών αλλά και να τους παραπλανούν μέσω του ηλεκτρονικού ταχυδρομείου κλπ.

Έτσι, για να μην φτάσουμε στο σημείο να πιστεύουμε πως οι υπηρεσίες του Διαδικτύου είναι επικίνδυνες για τα προσωπικά μας δεδομένα και να φοβόμαστε να τις χρησιμοποιήσουμε, πρέπει οι χρήστες να εκπαιδευτούν για να μπορούν να αντεπεξέλθουν στους κινδύνους που παρουσιάζονται. Η εκπαίδευση των χρηστών αποτελεί την βασικότερη γραμμή άμυνας εναντίον στην μη ζητηθείσα ηλεκτρονική αλληλογραφία (spam) και αυτό γιατί υπάρχουν πολλοί χρήστες, οι οποίοι δεν έχουν πολλές γνώσεις σχετικά με τις υπηρεσίες

του Διαδικτύου και πολλές φορές πέφτουν θύματα απατών από τους spammers. Πρέπει όλοι οι χρήστες να είναι σε θέση να αναγνωρίσουν την κακόβουλη και ανεπιθύμητη αλληλογραφία για να μπορούν να αμυνθούν κατάλληλα.

Τέλος, όλη η προσπάθεια που γίνεται για την αντιμετώπιση της ανεπιθύμητης αλληλογραφίας είναι μία προσπάθεια για να διατηρηθεί ο ηλεκτρονικός τρόπος επικοινωνίας, ένα σημαντικό εργαλείο στην καθημερινότητά μας.

Παράρτημα Α

Antivirus	Λογισμικό που χρησιμοποιείται για την προστασία του υπολογιστή από τους ιούς και από άλλο βλαβερό υλικό.
DNS server	Κάθε υπολογιστής στο Διαδίκτυο έχει μία μοναδική IP διεύθυνση και ένα μοναδικό όνομα. Η αντιστοιχία του ονόματος του υπολογιστή με την **IP** διεύθυνση γίνεται από το DNS.
FTP	Πρωτόκολλο μεταφοράς αρχείων μέσω δικτύου.
HTML	Η γλώσσα συγγραφής Web σελίδων, ώστε να μπορούν να διαβαστούν από τους φυλλομετρητές.
IMAP	Πρωτόκολλο που χρησιμοποιείται για την ανάγνωση των ηλεκτρονικών μηνυμάτων ενώ βρίσκονται ακόμα στον mail server.
IRC	Internet Relay Chat:Είναι ένα σύστημα όπου άτομα από όλο τον κόσμο είναι συνδεμένα σε εξυπηρετητές (servers) σε όλο τον κόσμο και επικοινωνούν αμφίδρομα σε πραγματικό χρόνο.
Opt in /Opt out	Η αποδοχή από τον χρήστη να λαμβάνει διαφημιστικά email από ένα δικτυακό τόπο (opt in), και η επιλογή που του παρέχει ο δικτυακός τόπος να ζητήσει διαγραφή της ηλεκτρονικής

	του διεύθυνσης από τη λίστα αποδεκτών του προωθητικού υλικού (opt out).
POP3	Πρωτόκολλο που χρησιμοποιείται για τη μεταφορά της εισερχόμενης αλληλογραφίας του χρήστη από το γραμματοκιβώτιο του mail server στον υπολογιστή του χρήστη.
Server	Εξυπηρετητής ή διακομιστής. Το σύστημα που διαχειρίζεται και διαμοιράζει δεδομένα σε εφαρμογές πελάτες.
SSL	Secure Sockets Layer: πρωτόκολλο που χρησιμοποιείται για τη διαβίβαση ιδιωτικών εγγράφων μέσω του Διαδικτύου.
TCP/IP	Πρωτόκολλο ελέγχου επικοινωνίας
Firewall	Τείχος προστασίας. Πρόκειται για συσκευή ή λογισμικό, το οποίο αποτρέπει μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση στον υπολογιστή.
SMTP	Simple Mail Transport Protocol. Αποτελεί ένα από τα θεμελιώδη πρωτόκολλα του Διαδικτύου για μεταφορά email μεταξύ των διαφόρων εξυπηρετητών.

Παράρτημα Β

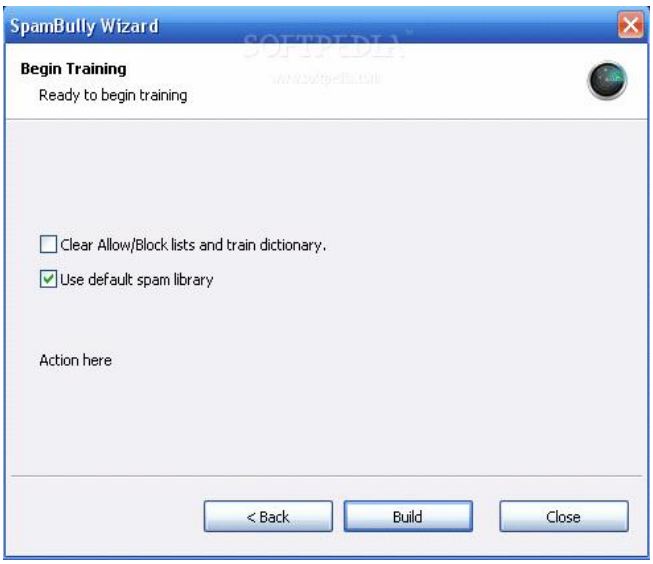
Σε αυτό το παράρτημα θα αναφερθούμε στην εφαρμογή κάποιων φίλτρων antispam, τα οποία ενσωματώνονται στο Outlook ή Outlook Express ως plug-ins.

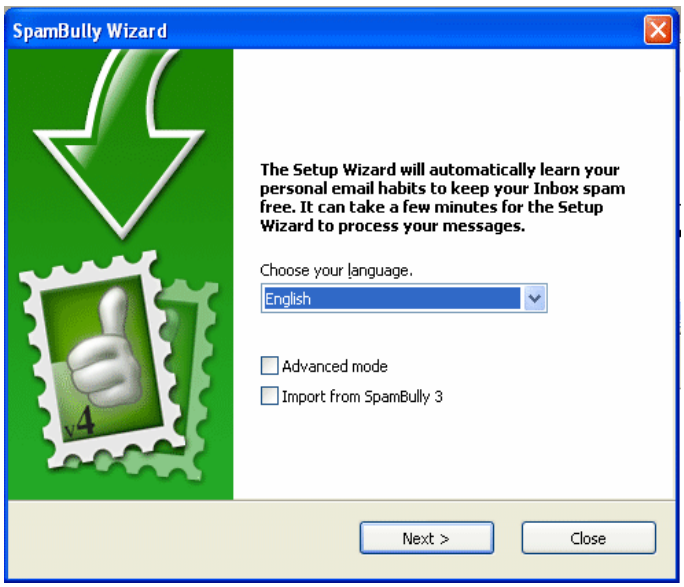
Πιο συγκεκριμένα αναλύουμε την λειτουργία τριών φίλτρων spam, τα οποία είναι τα εξής: spam Bully, spam Fighter και spamihilator.

spamBully

Το πρόγραμμα αυτό, ο κάθε χρήστης μπορεί να το βρει στον δικτυακό τόπο http://www.spambully.com και κλικάροντας τον σύνδεσμο Download να κατεβάσει την έκδοση του προγράμματος που τον ενδιαφέρει.

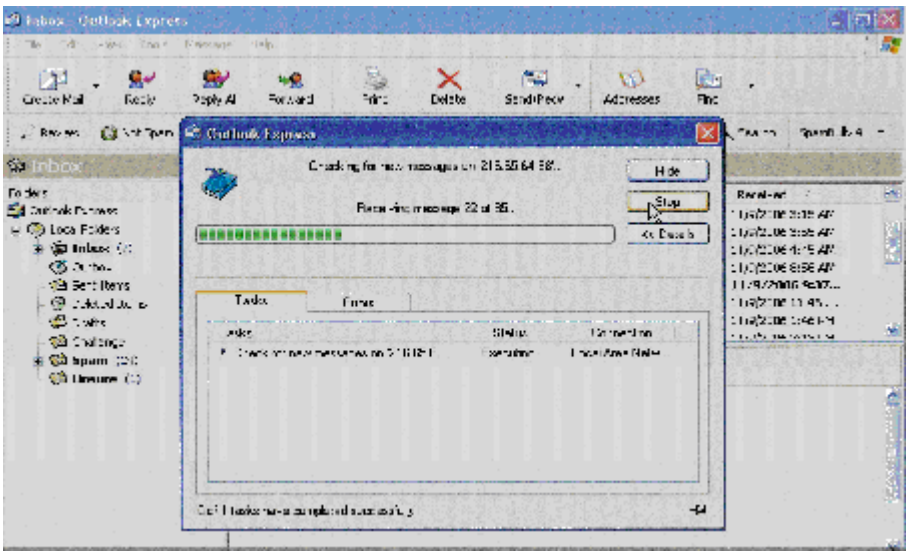
Κατά την εμφάνιση του Οδηγού εγκατάστασης επιλέγεται η γλώσσα στην οποία θα λειτουργήσει το πρόγραμμα και ολοκληρώνεται η εγκατάσταση. Ταυτοχρόνως ξεκινά και η 'εκπαίδευση' του προγράμματος για το ποιο μήνυμα θεωρείται spam και ποιο όχι.



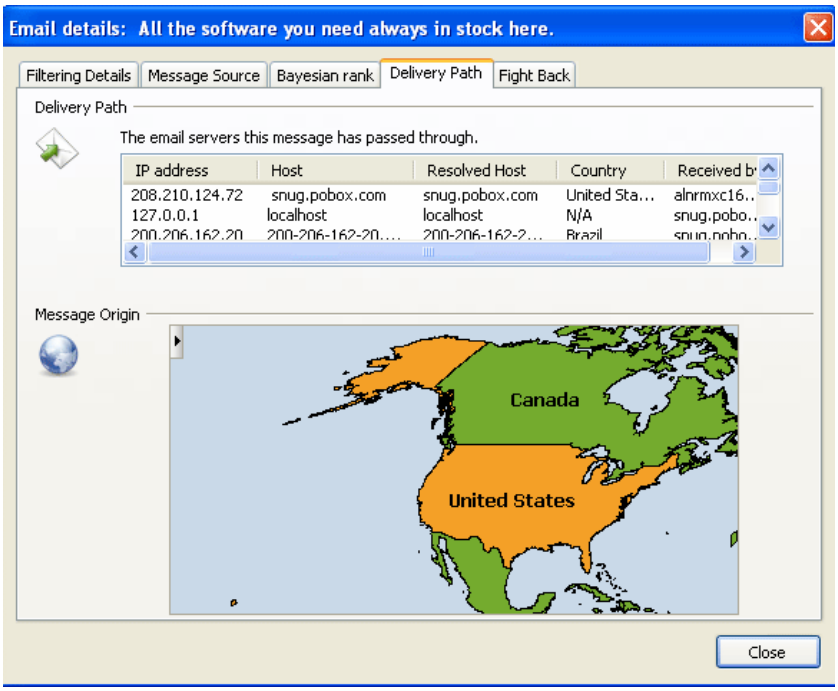


Με το άνοιγμα του προγράμματος ηλεκτρονικού ταχυδρομείου Outlook ή Outllook Express εμφανίζονται στην γραμμή εργαλείων ορισμένα κουμπιά που χρησιμοποιεί το spamBully.

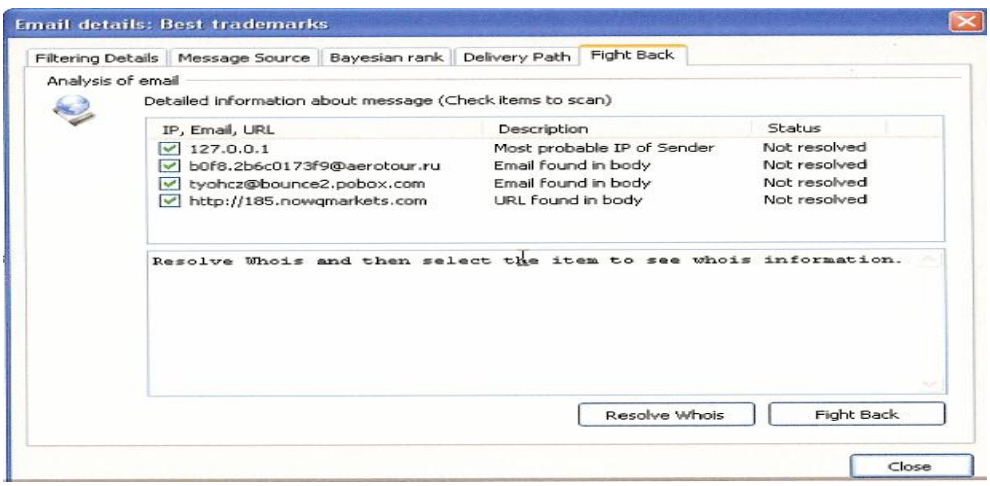
Το πρόγραμμα αναγνωρίζει και τοποθετεί τα εισερχόμενα μηνύματα στον φάκελο «Unsure» και με την βοήθεια των κουμπιών «Spam» και «Not Spam» μπορούν οι χρήστες να τα ξεχωρίσουν και να τα βάλουν στους φακέλους «inbox» και «spam».

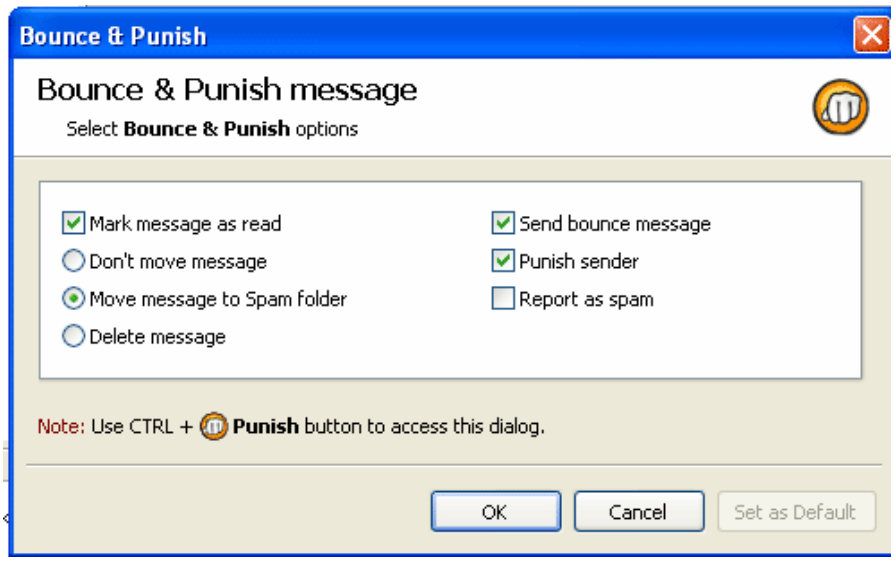


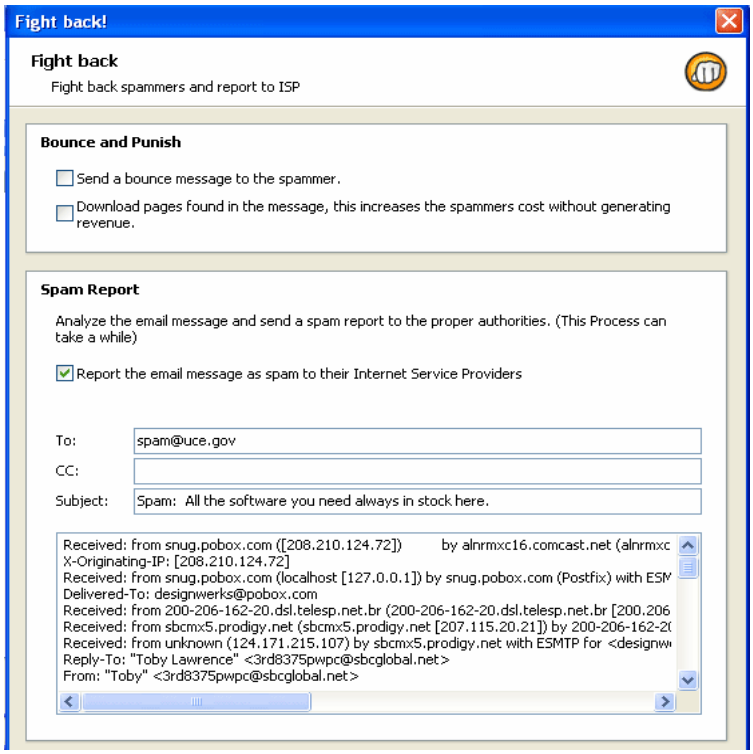
Με την επιλογή του πλαισίου « Email Details» ο χρήστης μπορεί να δει τον λόγο για τον οποίο ένα μήνυμα χαρακτηρίστηκε ως spam και δείχνει την IP διεύθυνση του αποστολέα καθώς και την τοποθεσία από την οποία το έστειλε μέσω ενός μικρού παγκόσμιου χάρτη.



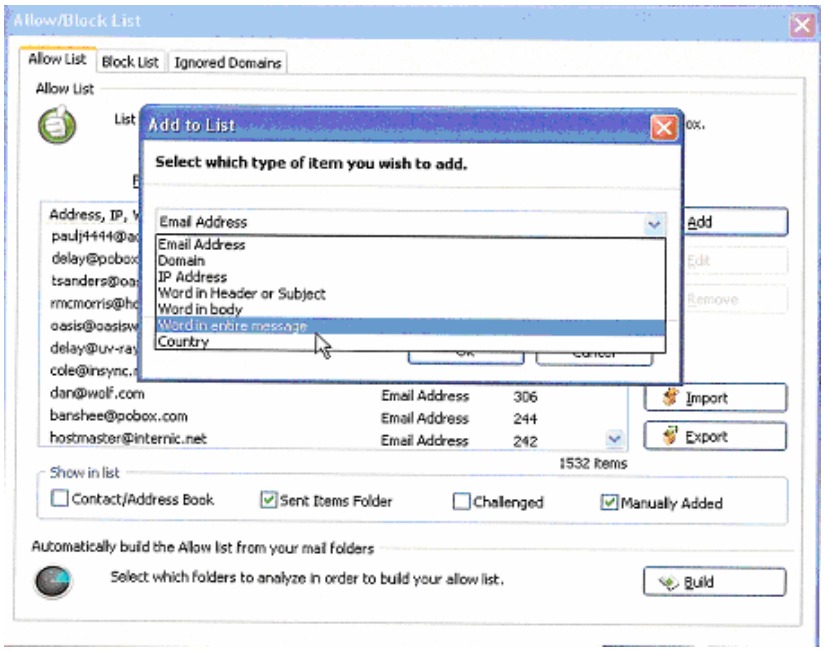
Το πρόγραμμα δίνει την δυνατότητα στον χρήστη να καταπολεμήσει τους spammers με την επιλογή του πλαισίου «Fight Back», στέλνοντας μηνύματα παραπόνων στους ISP(παροχείς υπηρεσιών internet). Το αποτέλεσμα των μηνυμάτων αυτών είναι η ακύρωση των ηλεκτρονικών διευθύνσεων των spammers.

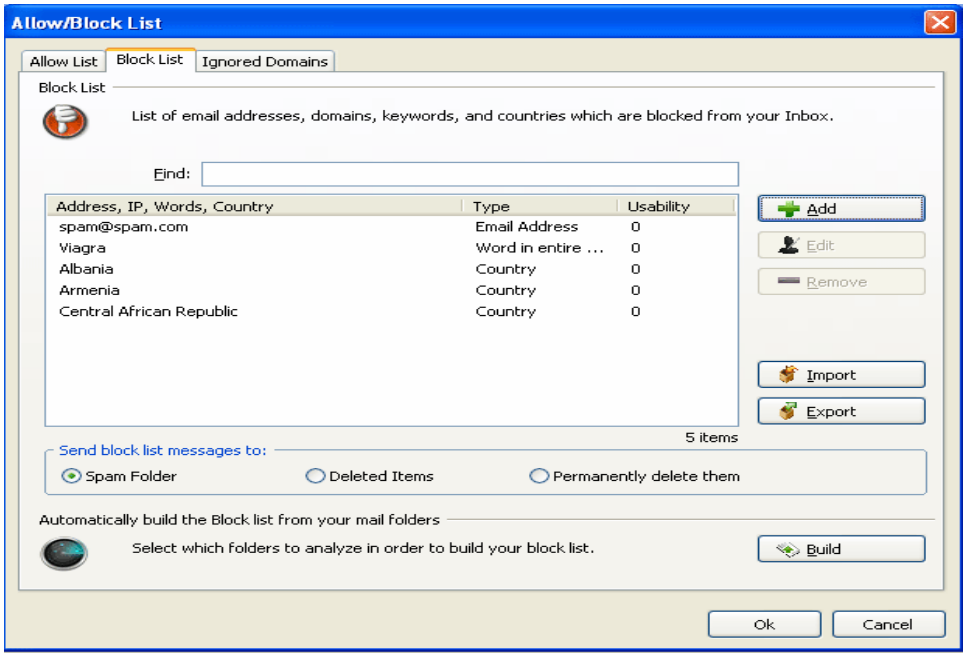




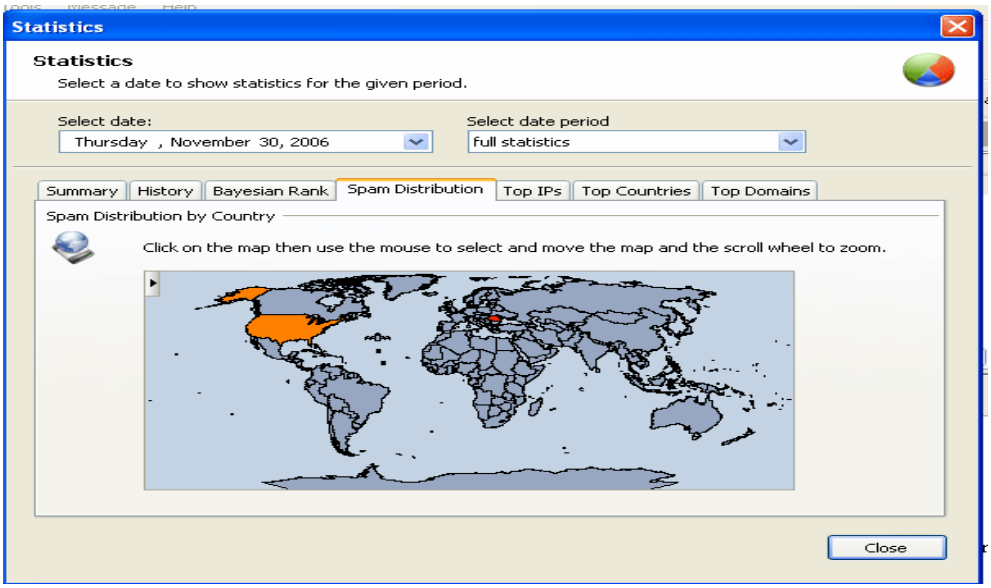


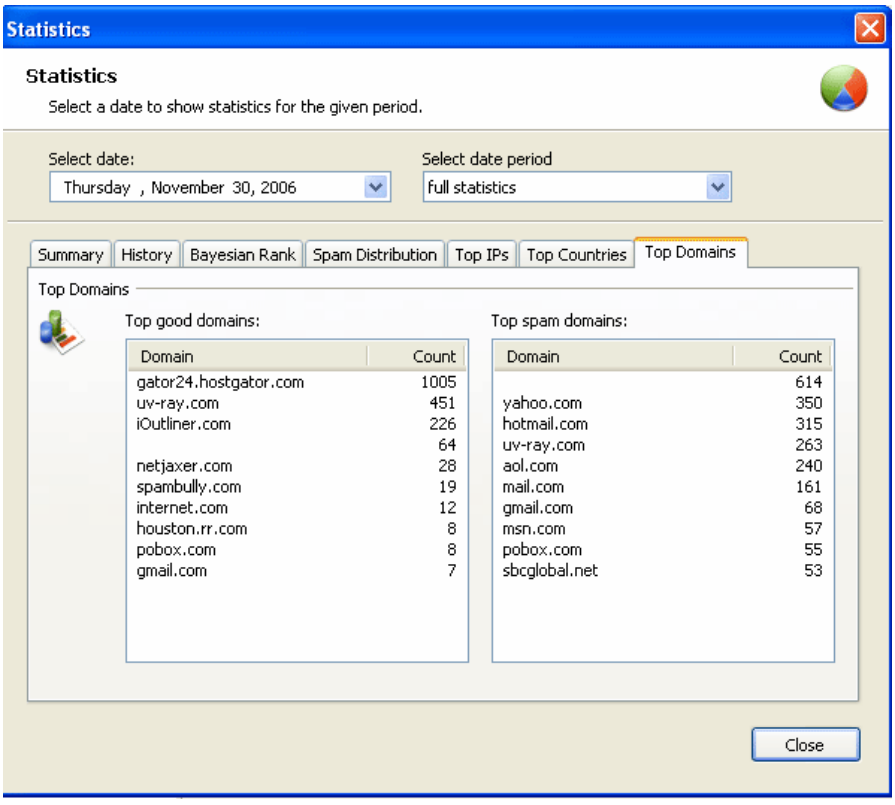
Με την χρήση του πλαισίου «Allow/Block List» ο χρήστης καθορίζει ποια μηνύματα θα δέχεται και ποια όχι με βάση την ηλεκτρονική διεύθυνση, την διεύθυνση IP, λέξεις που έχουν βρεθεί στο μήνυμα, την χώρα προέλευσης κ.λ.π.

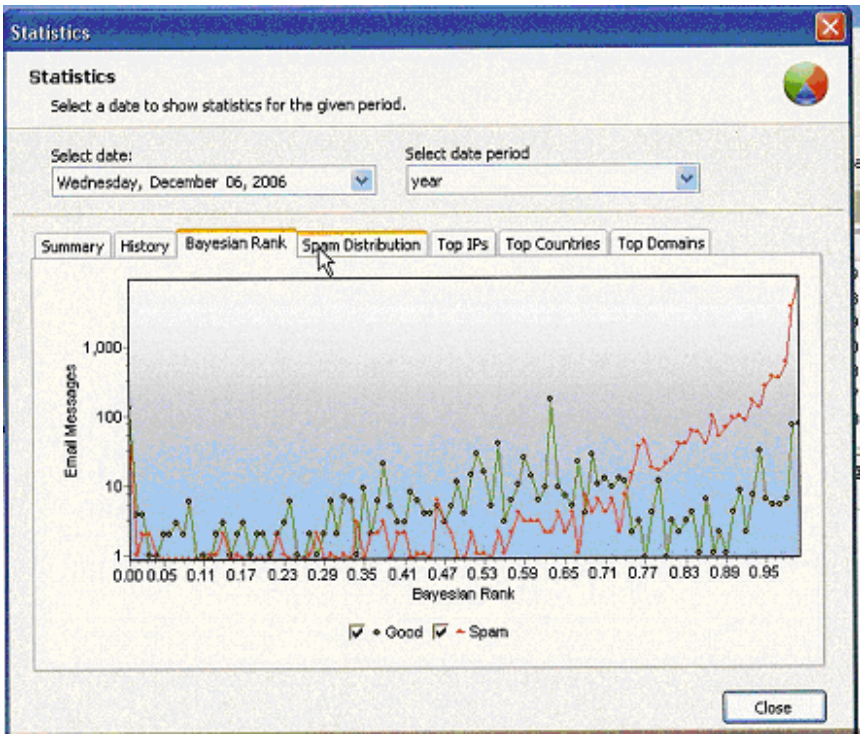




Τέλος, αυτό το πρόγραμμα παρέχει και στατιστική απεικόνιση των μηνυμάτων που έχει δεχθεί σε σχέση με το είδος τους.


Statistics
Statistics
Select a date to show statistics for the given period.
Select date:
Thursday , November 30, 2006
Select date period
full statistics
Summary
History
Bayesian Rank
Spam Distribution
Top IPs
Top Countries
Top Domains
Spam Distribution by Country
Click on the map then use the mouse to select and move the map and the scroll wheel to zoom.
Close


Statistics
Statistics
Select a date to show statistics for the given period.
Select date:
Thursday , November 30, 2006
Select date period
full statistics
Summary
History
Bayesian Rank
Spam Distribution
Top IPs
Top Countries
Top Domains
Top Domains
Top good domains:
Domain
Count
gator24.hostgator.com 1005
uv-ray.com 451
iOutliner.com 226
64
netjaxer.com 28
spambully.com 19
internet.com 12
houston.rr.com 8
pobox.com 8
gmail.com 7
Top spam domains:
Domain
Count
614
yahoo.com 350
hotmail.com 315
uv-ray.com 263
aol.com 240
mail.com 161
gmail.com 68
msn.com 57
pobox.com 55
sbcglobal.net 53
Close



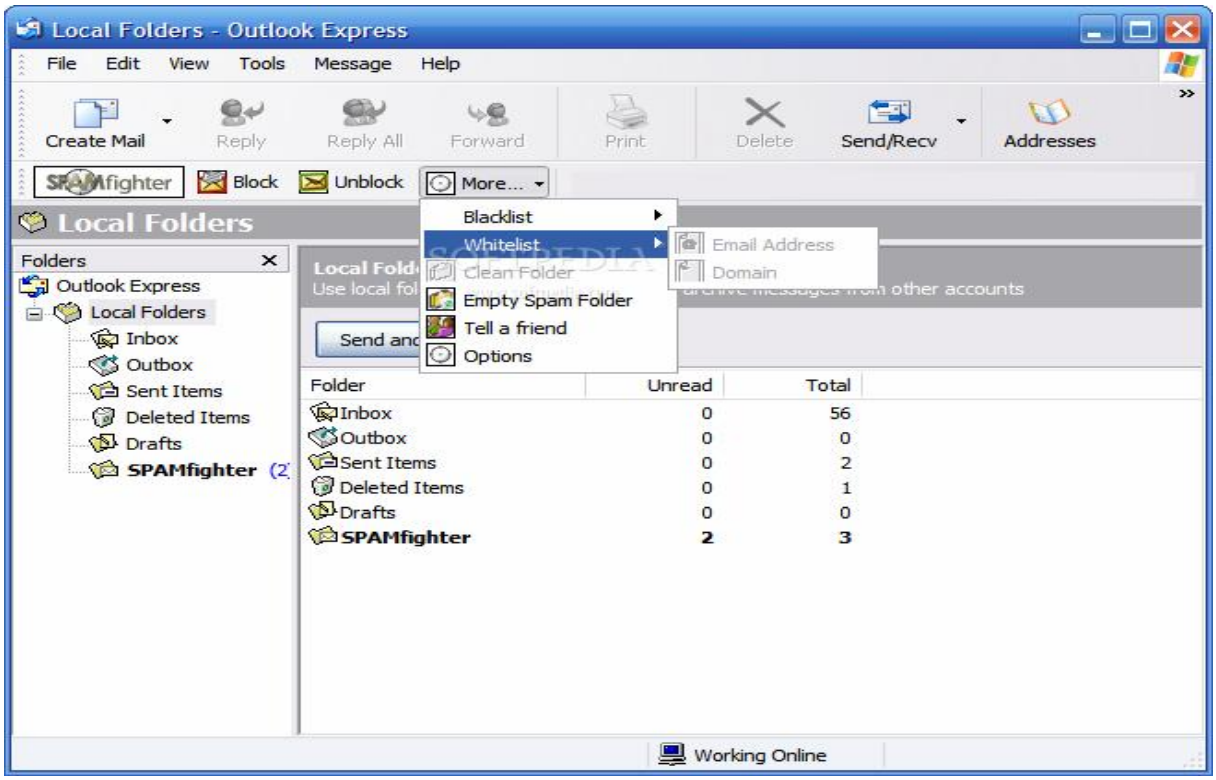
spamFighter

Το πρόγραμμα αυτό, ο κάθε χρήστης μπορεί να το βρει στον δικτυακό τόπο http://www.spamfighter.com/Lang_EL και κλικάροντας τον σύνδεσμο «Λήψη προγράμματος» να κατεβάσει την τελευταία έκδοση του προγράμματος.

Κατά την διάρκεια της εγκατάστασης επιλέγεται η γλώσσα με την οποία θα λειτουργήσει το πρόγραμμα και εμφανίζεται ο οδηγός του spamFighter όπου μέσω τριών βημάτων ολοκληρώνει την εγκατάσταση.

Δίνεται η δυνατότητα στον κάθε χρήστη να ρυθμίσει το πρόγραμμα σύμφωνα με τις ανάγκες του και αυτό γίνεται μέσω των βασικών εργαλειών που του παρέχονται.

Με το άνοιγμα του προγράμματος ηλεκτρονικού ταχυδρομείου Outlook ή Outllook Express εμφανίζονται στην γραμμή εργαλείων ορισμένα κουμπιά που χρησιμοποιεί το spamFighter.



Η γραμμή εργαλείων περιλαμβάνει τα κουμπιά “spamfighter”, “block”, “unblock” και “more”.

Το πρόγραμμα αυτό λειτουργεί με την βοήθεια των χρηστών δηλαδή εάν ένας από τους χρήστες spamfighter προσδιορίζει ότι το μήνυμα είναι spam, το πρόγραμμα αυτόματα ανανεώνει την βάση δεδομένων του, για να μην παίρνουν τέτοια μηνύματα οι υπόλοιποι χρήστες.

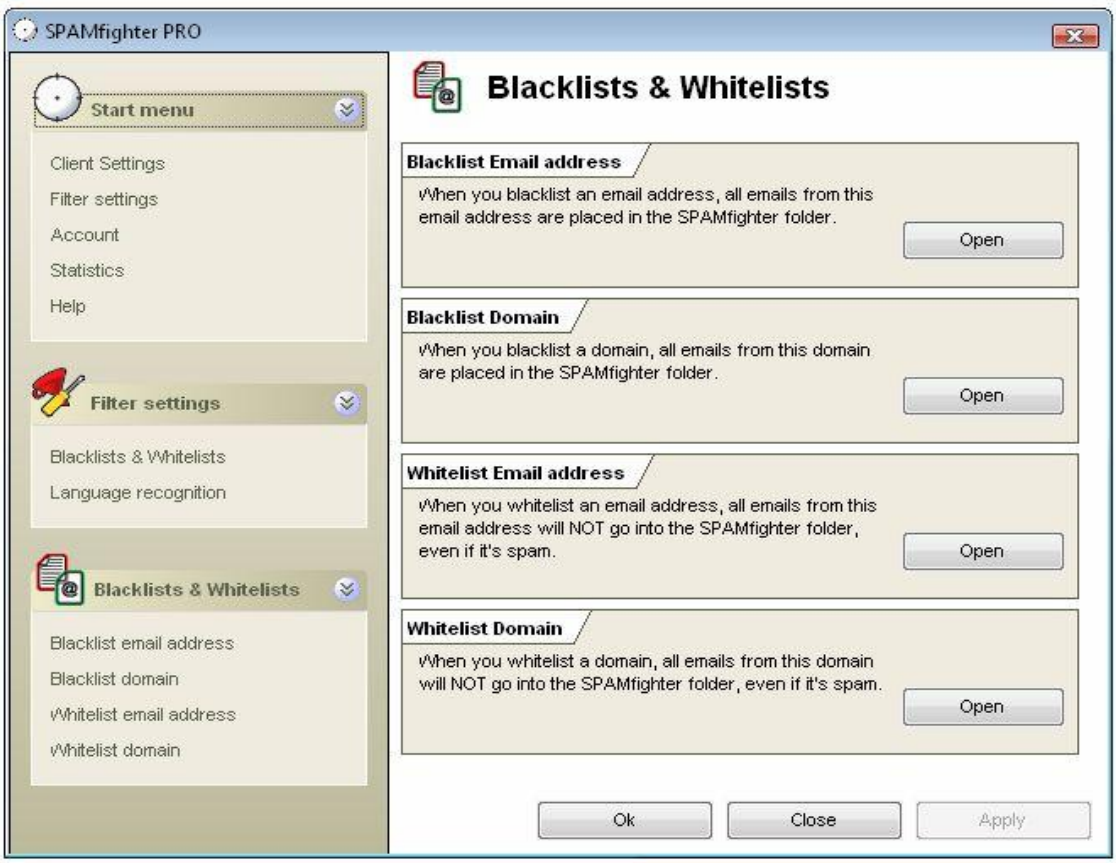
Κάθε νέο εισερχόμενο μήνυμα ελέγχεται από το spamfighter και αν πρόκειται για μήνυμα spam τοποθετείται αυτόματα στον φάκελο ‘Junk e-mail’.

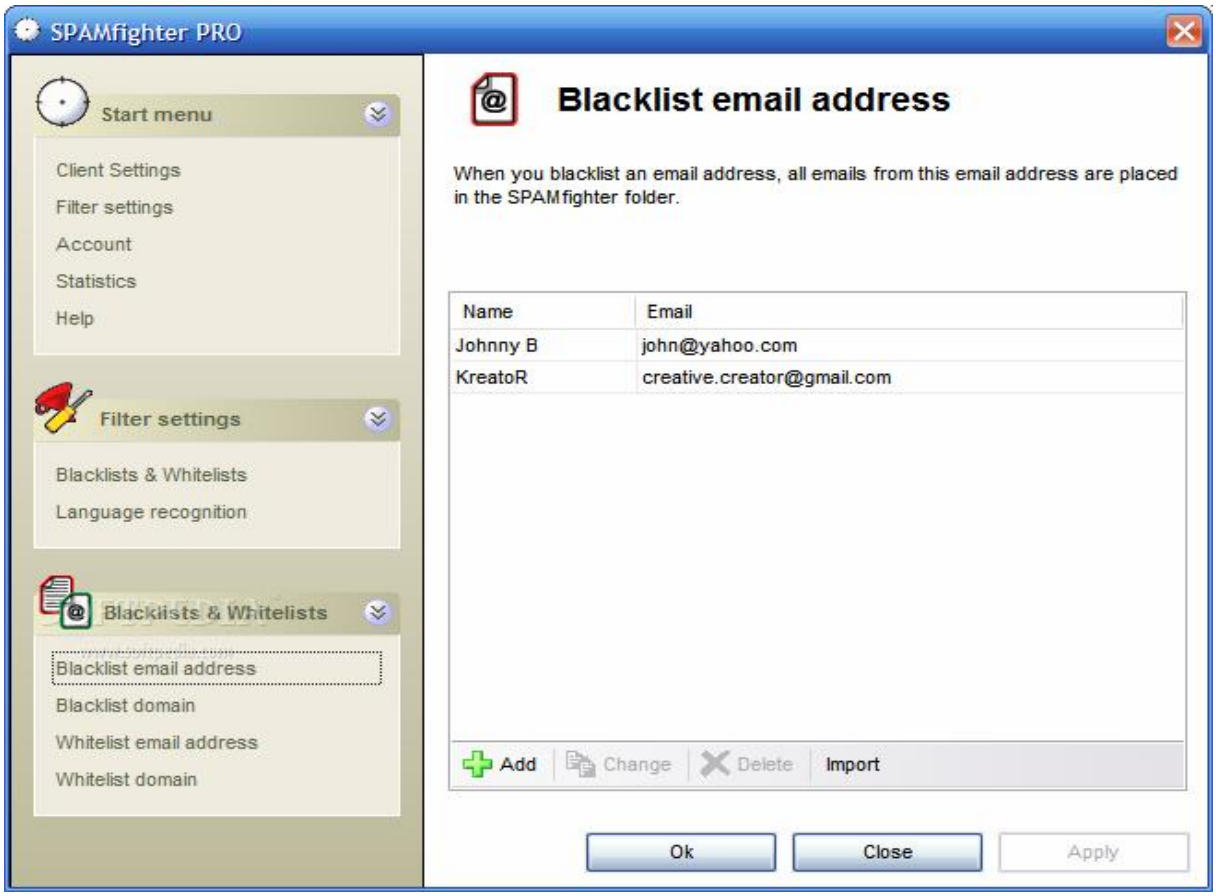
Στην περίπτωση που ο χρήστης λάβει ένα μήνυμα spam στο φάκελο ‘inbox’, μπορεί να ενημερώσει τα υπόλοιπα μέλη του spamfighter με την αποστολή ενός email στον διακομιστή του spamfighter. Αυτό γίνεται με την

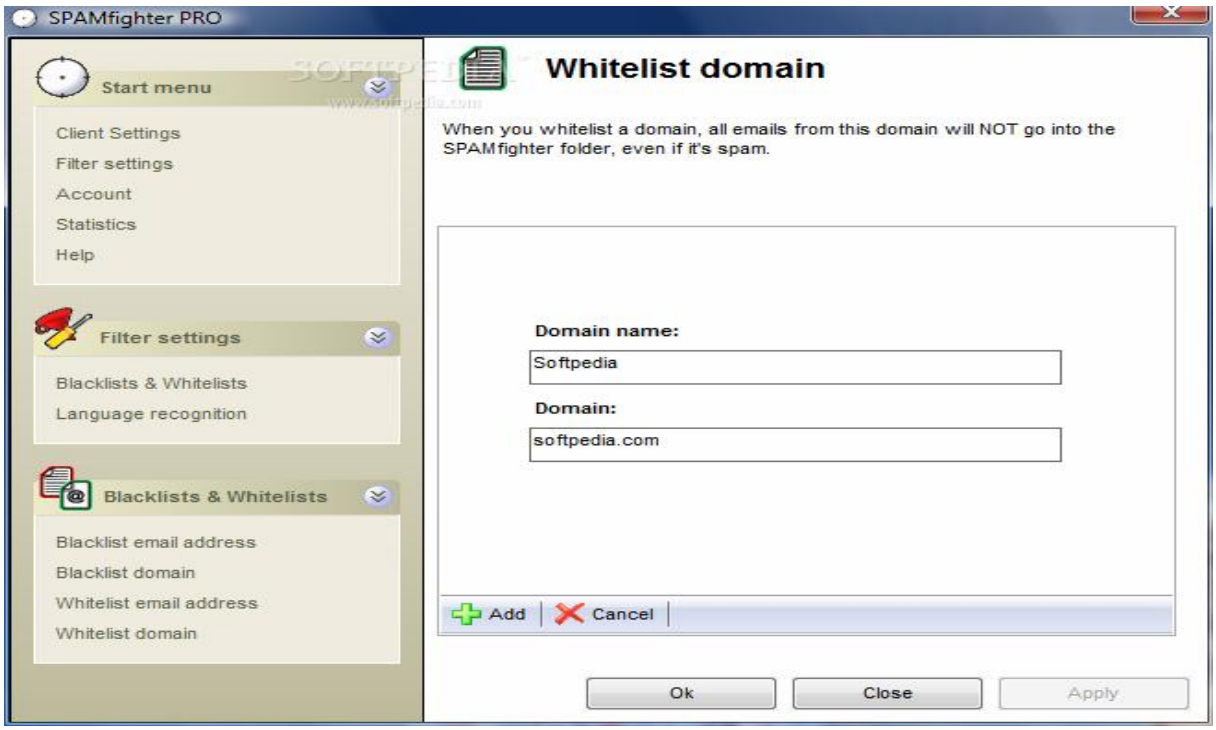
επιλογή του συγκεκριμένου μηνύματος spam και κλικάροντας το κουμπί “**block**” στην γραμμή εργαλείων. Με αυτό τον τρόπο το μήνυμα spam μεταφέρεται στον φάκελο “SPAMfighter”, ενημερώνεται ο διακομιστής του spamfighter και αυτόματα το μήνυμα αυτό μπλοκάρεται από τους υπόλοιπους χρήστες του προγράμματος.

Επίσης, στην περίπτωση που ένα no-spam μήνυμα βρεθεί στον φάκελο “SPAMfighter” ο χρήστης μπορεί να το επαναφέρει στον φάκελο “inbox” αλλά και να το αποσύρει από τον διακομιστή του spamfighter, απλώς επιλέγοντας το μήνυμα αυτό και κλικάροντας το κουμπί “**unblock**”.

Με την χρήση των “Allow/Block List” ο χρήστης καθορίζει ποια μηνύματα θα δέχεται και ποια όχι με βάση τις ηλεκτρονικές διευθύνσεις και τους domain servers.

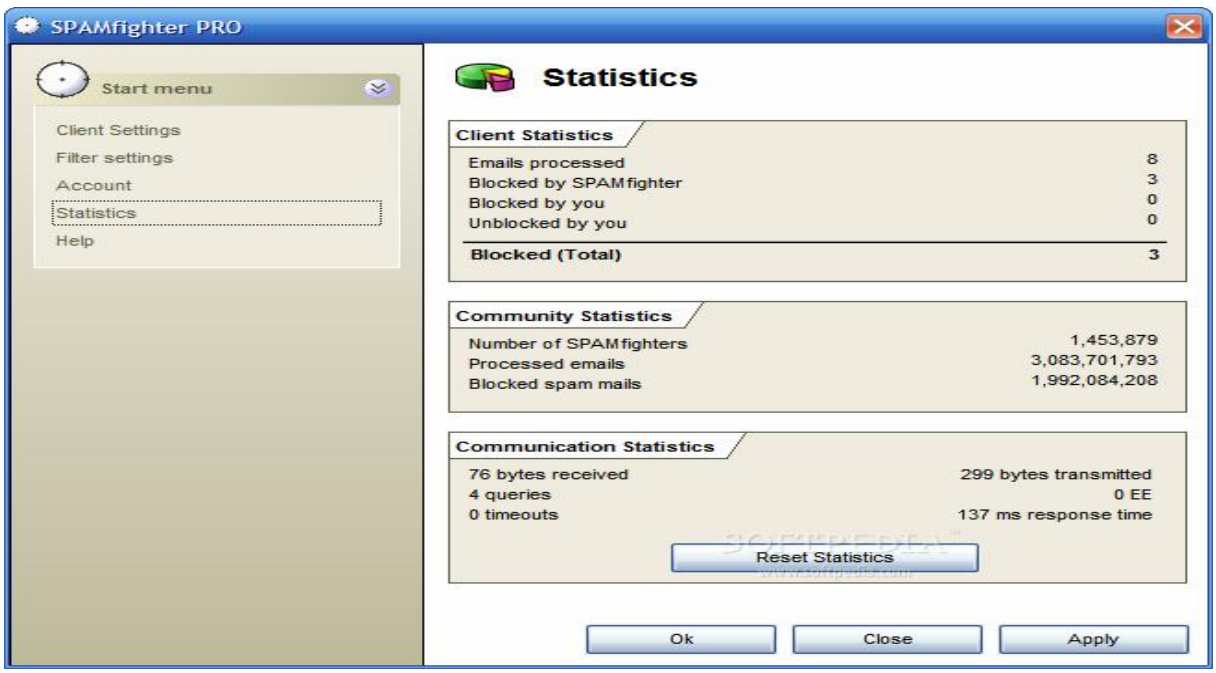






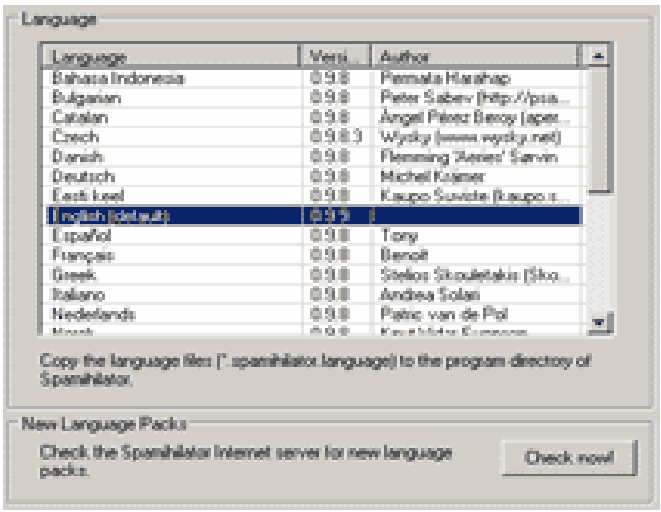
Επίσης, δίνεται η δυνατότητα στον χρήστη να επιλέξει ποια μηνύματα θα δέχεται με βάση την χώρα προέλευσης.

Τέλος, το πρόγραμμα παρέχει και στατιστική απεικόνιση των μηνυμάτων που έχει δεχθεί και δείχνει πόσα μηνύματα έχουν αντιμετωπιστεί από τον συγκεκριμένο χρήστη και πόσα από την κοινότητα του spamfighter.

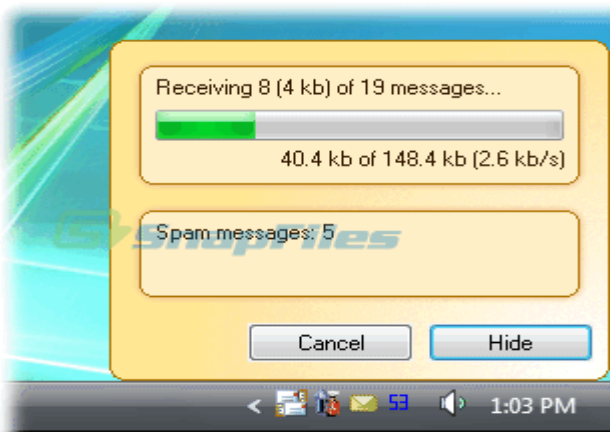


Spamhilator

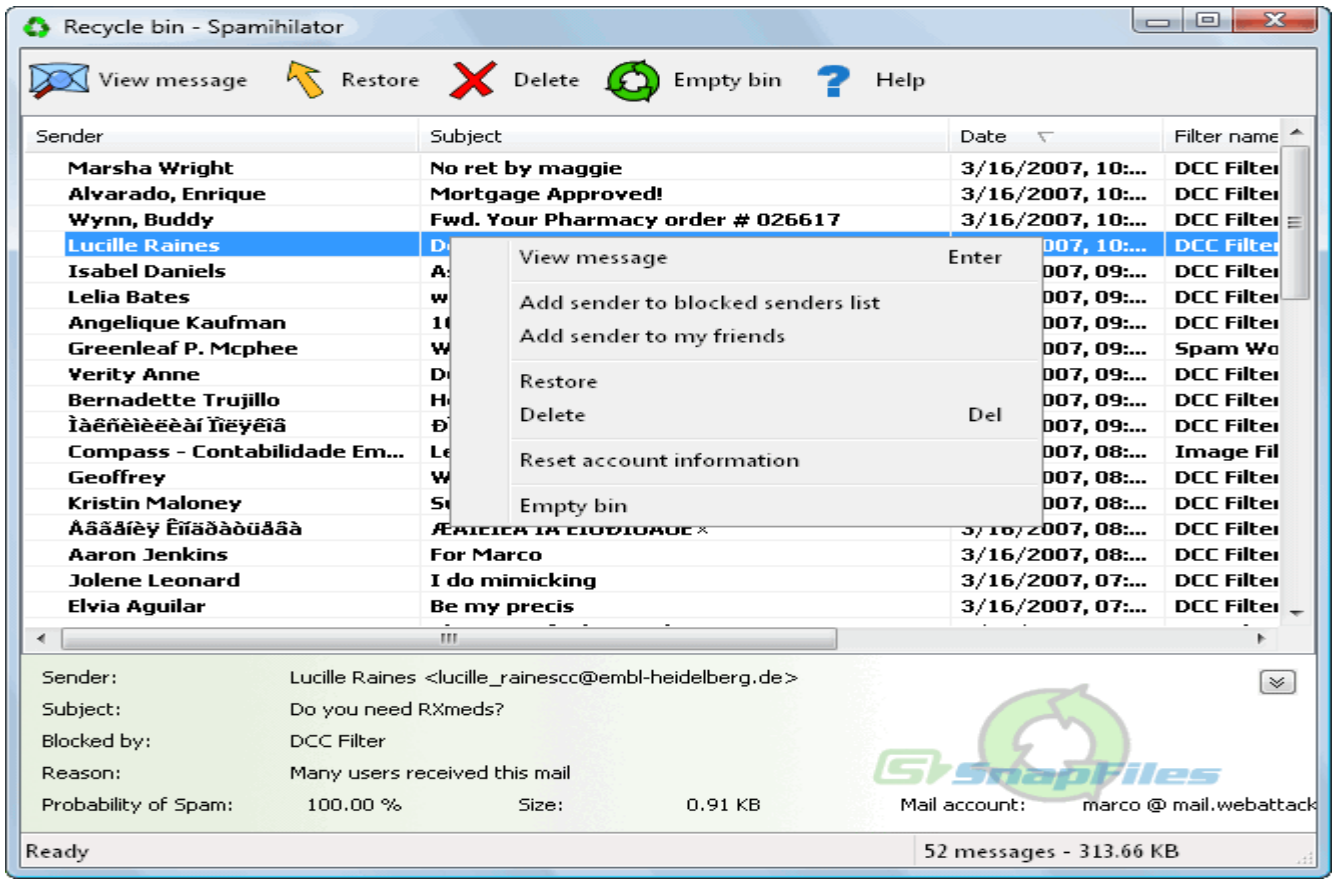
Το πρόγραμμα αυτό, ο κάθε χρήστης μπορεί να το βρει στον δικτυακό τόπο http://www.spamhilator.com και κλικάροντας download να κατεβάσει την τελευταία έκδοση του προγράμματος. Κατά την εμφάνιση του οδηγού εγκατάστασης επιλέγεται η γλώσσα στην οποία θα λειτουργήσει το πρόγραμμα.



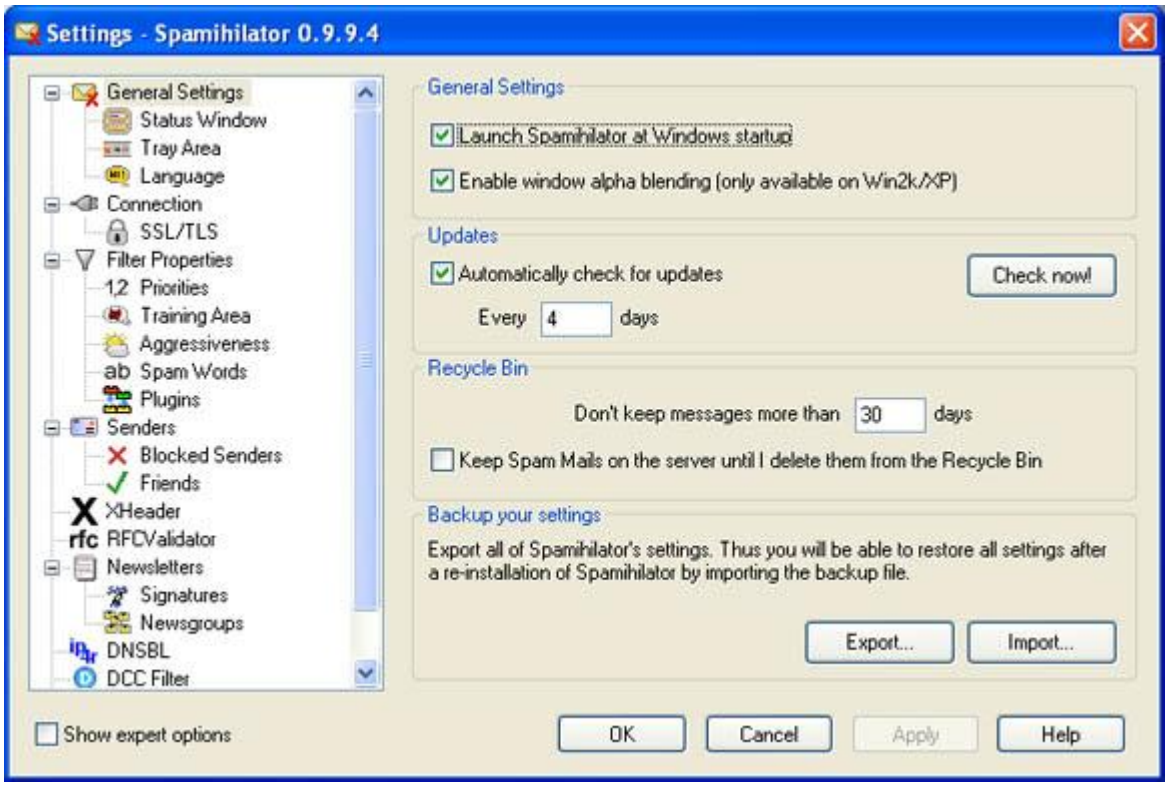
Το Spamihilator είναι ένα πλήρες anti-spam πρόγραμμα φιλτραρίσματος που λειτουργεί με οποιοδήποτε πελάτη ηλεκτρονικού ταχυδρομείου. Αυτό το πρόγραμμα, εγκαθίσταται μεταξύ του προγράμματος ηλεκτρονικού ταχυδρομείου και της ταχυδρομικής θυρίδας και ελέγχει τα email όταν ο χρήστης θελήσει να τα ανακτήσει.



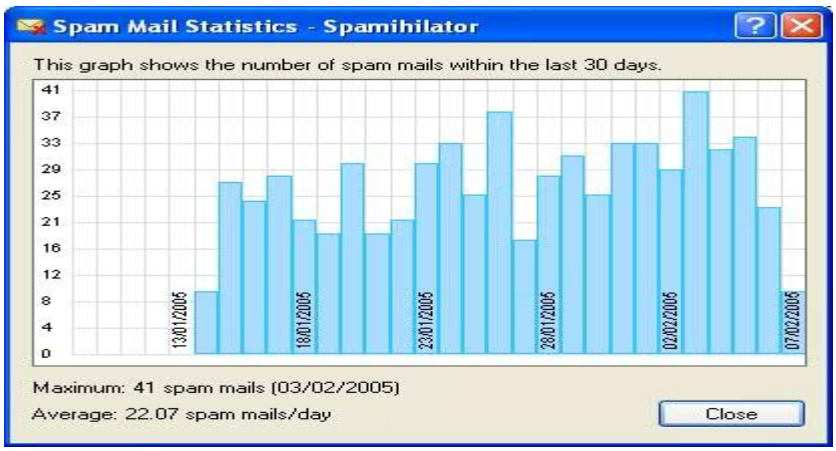
Το παρακάτω παράθυρο είναι η περιοχή ανακύκλωσης του προγράμματος, στην οποία εμφανίζονται όλα τα μηνύματα που υπάρχουν στο mailbox μας. Αυτόματα το πρόγραμμα αναγνωρίζει τα μηνύματα που χαρακτηρίζονται από spam με κάποια πιθανότητα και έτσι ο χρήστης έχει την δυνατότητα να τα διαγράψει.



Επιπλέον, το πρόγραμμα παρέχει ήδη φίλτρο διαχωρισμού των μηνυμάτων με βάση λέξεις κλειδιά, στο οποίο ο χρήστης μπορεί να προσθέσει και καινούργιες λέξεις ή φράσεις –κλειδιά. Επίσης, ο χρήστης σε αυτό το παράθυρο μπορεί να κάνει διάφορες επιλογές σχετικά με την ασφάλειά του απέναντι στα μηνύματα spam.

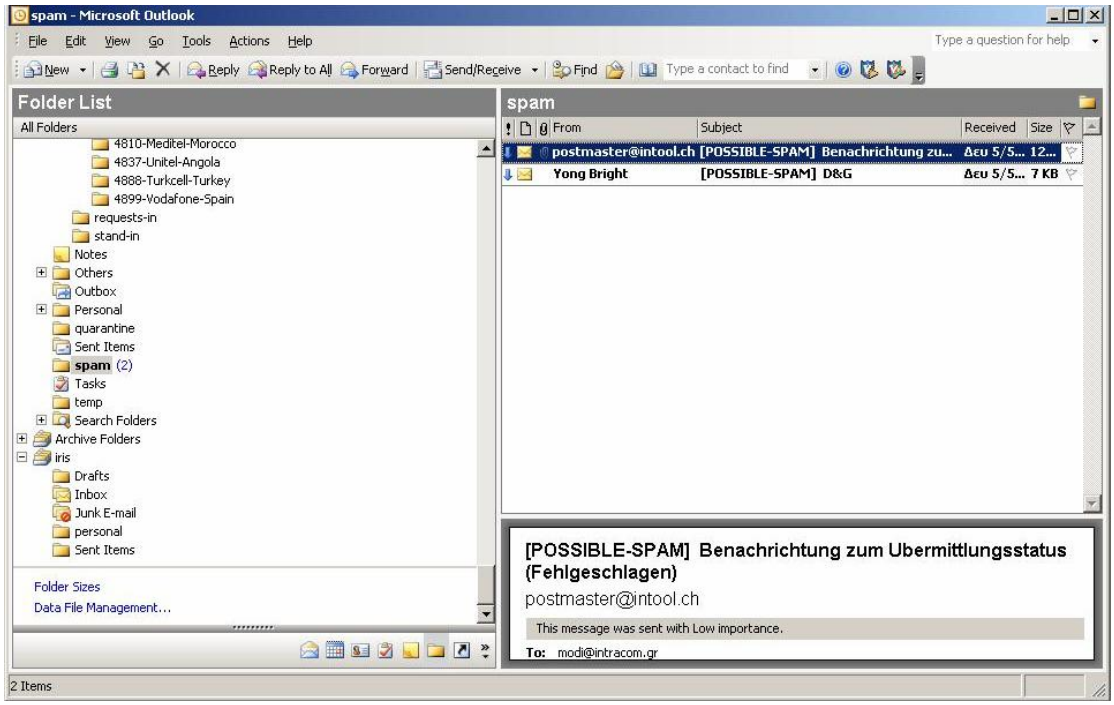


Τέλος, στο παρακάτω παράθυρο φαίνεται η στατιστική απεικόνιση των μηνυμάτων που έχει δεχθεί.

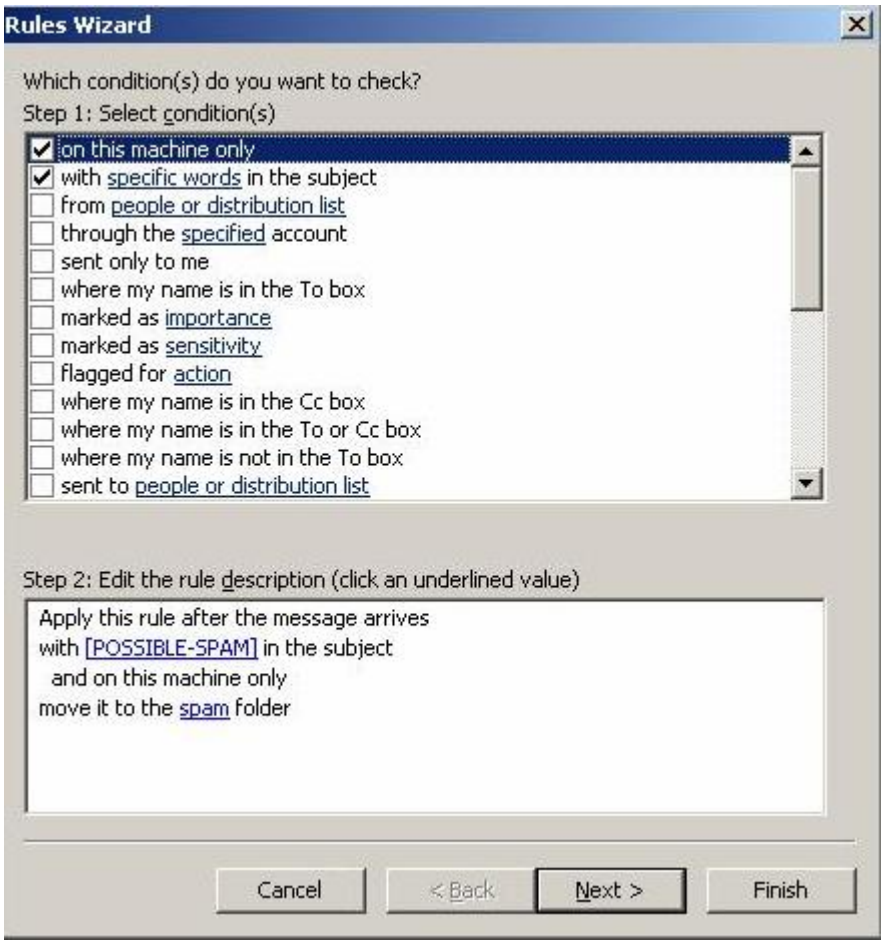


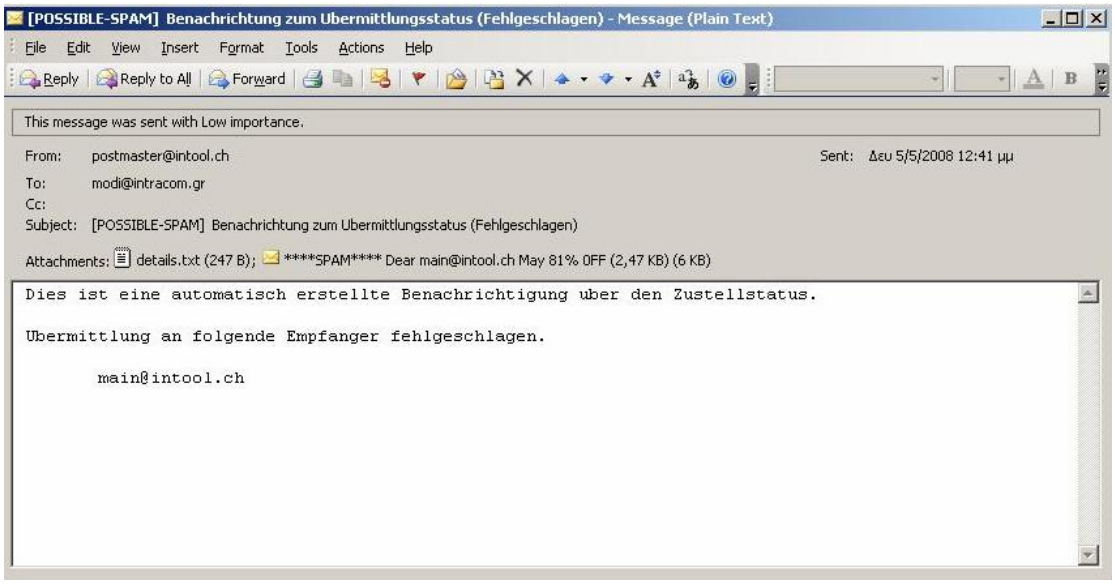
Τέλος, θα αναφερθούμε σε ένα φίλτρο το οποίο αναπτύχθηκε εσωτερικά για μεγάλη εταιρεία πληροφορικής.

Ο server της εταιρίας κατά την λήψη των νέων μηνυμάτων, τοποθετεί στο θέμα αυτών την ετικέτα [POSSIBLE-SPAM]. Έτσι όταν τα εισερχόμενα μηνύματα φτάνουν στο Outlook αποθηκεύονται κατευθείαν στον φάκελο spam.



Έπειτα ο χρήστης δημιουργεί ένα κανόνα σύμφωνα με τον οποίο αν κάποιο εισερχόμενο μήνυμα έχει στο θέμα του την συγκεκριμένη λέξη ή φράση, να αποθηκεύεται κατευθείαν στον φάκελο spam.


Rules Wizard
Which condition(s) do you want to check?
Step 1: Select condition(s)
on this machine only
with specific words in the subject
from people or distribution list
through the specified account
sent only to me
where my name is in the To box
marked as importance
marked as sensitivity
flagged for action
where my name is in the Cc box
where my name is in the To or Cc box
where my name is not in the To box
sent to people or distribution list
Step 2: Edit the rule description (click an underlined value)
Apply this rule after the message arrives
with [POSSIBLE-SPAM] in the subject
and on this machine only
move it to the spam folder
Cancel
< Back
Next >
Finish


[POSSIBLE-SPAM] Benachrichtung zum Ubermittlungsstatus (Fehlgeschlagen) - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
This message was sent with Low importance.
From: postmaster@intool.ch
Sent: Δευ 5/5/2008 12:41 μμ
To: modi@intracom.gr
Cc:
Subject: [POSSIBLE-SPAM] Benachrichtung zum Ubermittlungsstatus (Fehlgeschlagen)
Attachments: details.txt (247 B); ****SPAM**** Dear main@intool.ch May 81% OFF (2,47 KB) (6 KB)
Dies ist eine automatisch erstellte Benachrichtigung uber den Zustellstatus.
Ubermittlung an folgende Empfanger fehlgeschlagen.
main@intool.ch

Αναφορές

Internet:

http://www.saferinternet.gr/Default.aspx?tabid=178

http://www.no-spam.gr/mustknow.htm

http://www.no-spam.gr/index.php

http://www.no-spam.gr/moreonspam.htm

http://www.no-spam.gr/laws.htm

http://www.no-spam.gr/tools.htm

http://elawyer.blogspot.com/2005/10/spamming.html

http://en.wikipedia.org/wiki/Anti-spam_techniques#End-user_techniques

http://en.wikipedia.org/wiki/Anti-spam_techniques#Automated_techniques_for_e-mail_administrators

http://www.microsoft.com/protect/yourself/email/spam.mspx

http://www.cartoonstock.com/search.asp?

http://spam.abuse.net/overview/

http://www.private.org.il/harvest.html

http://www.noc.teithe.gr/html/electronic_mail.html

http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?_list

http://www.reason.comnews/show/28936.html

http://www.barracudanetworks.com/ns/products/spam_overview.php

http://www.firetrust.com/products/oss/mailwasher-server/?q=products/oss/mailwasher-server

http://www.webopedia.com/TERM/S/SPF.html

http://wiki.apache.org/spamassassin/SpamAssassin

http://www.mailscanner.biz/readme.html

http://metal.ntua.gr/modperl/index.pl?URLID=4_1

http://www.softpedia.com/progScreenshots/Spamihilator-Screenshot-5754.html

http://www.drmadcow.net/ViewArticle/ID/11/

http://www.snapfiles.com/screenshots/spami.htm

http://www.spambully.com

http://www.spamfighter.com/Lang_EL

http://www.spamhilator.com

Βιβλία

1. Διαφήμιση & Παρενόχληση: spam και τηλεόραση-
   Εκδόσεις Αντ. Ν. Σάκκουλα
2. e- Επιχειρηματικότητα: Από την ιδέα στην υλοποίηση-
   Εκδόσεις Ελληνικά Γράμματα
3. Νομικό περιοδικό ‘Αρμενόπουλος 2007/993’-
   Μελέτη «Διαδίκτυο και Αστικό Δίκαιο» του Παν. Κορνηλάκη

Περιοδικά/ Εφημερίδες

1. Έθνος της Κυριακής: Ειδική έκδοση «παιδί & INTERNET» 9/9/2007
2. PC Magazine: Τεύχος 3-Μάρτιος 2007