ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΣΧΟΛΗ:Σ.Δ.Ο.
ΤΜΗΜΑ:ΛΟΓΙΣΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

«ΑΝΕΠΙΘΥΜΙΤΗ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (SPAM): ΠΡΟΒΛΗΜΑΤΑ ΚΑΙ ΛΥΣΕΙΣ»

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΩΝ: Χονδρογιάννη Ειρήνη
Μακράκη Ειρήνη
Σπαντιδέας Γεώργιος

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: Κωνσταντίνος Σταμάτης

ΠΑΤΡΑ 2011

ΠΡΟΛΟΓΟΣ

Ο σκοπός αυτής της πτυχιακής εργασίας είναι να διευκρινίσει τι είναι το Spam όπως επίσης και τρόπους αποφυγής του. Η αυθαίρετη ηλεκτρονική αλληλογραφία ,Spam, είναι απλά το σύνολο των μηνυμάτων που στέλνονται σε ένα χρήστη χωρίς την συναίνεσή του ή την εκδήλωση της επιθυμίας του να τα λαμβάνει. Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση των προϊόντων ή των υπηρεσιών τους. Η μεγάλη διάδοση που γνωρίζει η αυθαίρετη ηλεκτρονική αλληλογραφία, θα κάνει το email προοδευτικά δυσκολότερο στη χρήση του, ίσως και ακόμη τελείως άχρηστο ως μέσο επικοινωνίας για καταναλωτές και επιχειρήσεις αν το πλήθος των μηνυμάτων συνεχίσει να αυξάνει αντί να μειωθεί δραστικά.

ΠΕΡΙΛΗΨΗ

Στις μέρες μας η λέξη SPAM χρησιμοποιείται από τους χρήστες του διαδικτύου για να χαρακτηρίσει την αυτόκλητη και αζήτητη αποστολή ηλεκτρονικών μηνυμάτων. Αποστολείς των μηνυμάτων αυτών είναι συνήθως εταιρίες που θέλουν ένα φτηνό τρόπο για να διαφημιστούν, ενώ παραλήπτες είναι λογαριασμοί ηλεκτρονικής αλληλογραφίας που έχουν γίνει γνωστοί στο διαδίκτυο, όπως για παράδειγμα ανοικτές λίστες αλληλογραφίας, διευθύνσεις καταγεγραμμένες σε δικτυακές σελίδες, είτε συνηθισμένα ονόματα χρήστη σε γνωστούς παρόχους ηλεκτρονικής αλληλογραφίας (π.χ.john@hotmail.com). Το SPAM ξεκίνησε ως κάτι άκακο και διασκεδαστικό, η ανάγνωση τέτοιων μηνυμάτων μπορούσε να θεωρηθεί και ως ευχάριστο διάλειμμα από τη δουλειά, αλλά κατέληξε να είναι μαζί με τους ιούς (worms & viruses) ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Η αυξανόμενη ποσότητα spam έχει όλο και μεγαλύτερο αντίκτυπο σε χρόνο και

χρήμα του τελικού χρήστη καθώς αυτός λαμβάνει περισσότερο όγκο δεδομένων από ότι χρειάζεται και θέλει. Παράλληλα αυξάνει την χρησιμοποίηση δικτυακών πόρων για τη διακίνηση ανάμεσα στους παρόχους Internet και επιβαρύνει τη διαχείρισή των ηλεκτρονικών μηνυμάτων στους κεντρικούς εξυπηρετητές καταναλώνοντας υπολογιστικούς και αποθηκευτικούς πόρους. Η ποσότητα των μηνυμάτων SPAM που λαμβάνει ο μέσος χρήστης αυξάνεται με όλο και μεγαλύτερο ρυθμό τα τελευταία χρόνια. Ο σκοπός αυτής της πτυχιακής εργασίας είναι να διευκρινίσει τι είναι το Spam όπως επίσης και τρόπους αποφυγής του. .

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το Spam είναι η χρήση των ηλεκτρονικών συστημάτων ανταλλαγής μηνυμάτων (συμπεριλαμβανομένων των περισσότερων ραδιοτηλεοπτικών μέσων, ψηφιακά συστήματα διανομής) για να στέλνουν αζήτητα μηνύματα, αδιακρίτως. Ενώ η πιο ευρέως αναγνωρισμένη μορφή spam είναι e-mail spam , εντούτοις ο όρος εφαρμόζονται σε παρόμοια καταχρήσεις σε άλλα μέσα ενημέρωσης όπως: instant messaging spam , Usenet newsgroup spam , spam Web μηχανή αναζήτησης , το spam στα blogs , wiki spam , online αγγελίες spam, κινητό τηλέφωνο μηνύματα spam , Internet spam φόρουμ , αποστολές φαξ σκουπίδια , την κοινωνική δικτύωση spam, τηλεοπτικές διαφημίσεις και την κοινή χρήση αρχείων spam δίκτυο. Το Spamming παραμένει οικονομικά βιώσιμο, επειδή οι διαφημιστές δεν έχουν κανένα κόστος λειτουργίας πέρα από τη διαχείριση στις λίστες τους, και είναι δύσκολο οι αποστολείς να λογοδοτήσουν για μαζική αλληλογραφία τους. Επειδή το εμπόδιο εισόδου στην αγορά είναι τόσο χαμηλό, οι spammers είναι πολλοί, και ο όγκος των ανεπίκλητων μηνυμάτων έχει γίνει πολύ υψηλός. Κατά το έτος 2011 η εκτίμηση για τα μηνύματα spam είναι περίπου επτά τρισ.. δαπάνες, όπως απώλεια παραγωγικότητας και της απάτης, οι οποίες βαρύνουν το δημόσιο και από τους παρόχους υπηρεσιών Διαδικτύου. Ο μονος τροπος που μπορούν να αντιμετωπιστούν είναι μέσω ειδικών φίλτρων (προγραμμάτων) και φυσικά μέσω κοινωνικής επαγρύπνησης του χρήστη.

ΚΕΦΑΛΑΙΟ 1^{ο} : ΕΝΝΟΙΟΛΟΓΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΜΕΛΕΤΗΣ

1.1 Τι είναι το Internet

Το Internet είναι το αποτέλεσμα της ταχείας ανάπτυξης των υπολογιστών και των τηλεπικοινωνιών. Αποτελείται από χιλιάδες διασυνδεόμενα δίκτυα υπολογιστών τα οποία είναι εγκατεστημένα στις περισσότερες χώρες του κόσμου. Στο Internet υπάρχουν εκατομμύρια sites (ιστοσελίδες) ανά τον κόσμο. Στα sites υπάρχουν οτιδήποτε μπορεί κανείς να σκεφτεί, από συνταγές μαγειρικής μέχρι εξειδικευμένα προγράμματα που αφορούν τον επιστημονικό χώρο. Μπορεί να φανταστεί κανείς το Internet σαν τη μεγαλύτερη αποθήκη προγραμμάτων σε όλο τον κόσμο.

Το Internet σήμερα είναι ένα πολλά υποσχόμενο μέσο άσκησης εμπορίου διεθνώς, μέσα από αυτό μπορούν να γίνονται συναλλαγές μεταξύ φορέων που βρίσκονται σε διαφορετικά μήκη και πλάτη της γης.

Επιταχύνει και διευκολύνει τις διαδικασίες τέλεσης των λειτουργιών του διεθνούς εμπορίου μιας και χαρίζει στις επιχειρήσεις μία γιγάντια βάση δεδομένων με προσφορά και ζήτηση εμπορευμάτων και υπηρεσιών. Η διαφήμιση στο Internet είναι ένας καταλυτικότατος παράγοντας, ίσως ο πλέον καταλυτικός, που προωθεί και οδηγεί στην τέλεση του διεθνούς εμπορίου αφού προωθεί την προσφορά και τη ζήτηση.

Το e-mail (ηλεκτρονικό ταχυδρομείο) αποτελεί ίσως το δημοφιλέστερο εργαλείο του ίντερνετ, ένα μέσω με το οποίο μπορούμε να επικοινωνούμε χωρίς οικονομική επιβάρυνση, γρήγορα, άμεσα αλλά και διακριτικά.

1.1.1 Η ιστορία του Internet

Κατά την περίοδο του ψυχρού πολέμου η συνεχής προσπάθεια για την εξασφάλιση τεχνολογικής και στρατιωτικής υπεροχής ανάμεσα στις δύο υπερδυνάμεις Η.Π.Α. και Ε.Σ.Σ.Δ., οδήγησαν το Υπουργείου Άμυνας των Η.Π.Α. να δημιουργήσει έναν επιστημονικό φορέα που θα είχε ως στόχο την σημαντική τεχνολογική ανάπτυξη του αμερικανικού αμυντικού μηχανισμού. Ο φορέας αυτός ήταν η Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων (Advance Research Projects Agency) ευρύτερα γνωστό ως A.R.P.A.. Στο A.R.P.A. συμμετείχαν εκατοντάδες κορυφαίοι επιστήμονες των οποίων η εργασία επικεντρωνόταν σε διαστημικές αποστολές και πυραυλικά συστήματα. Ένας από αυτούς ήταν ο Lawrence Roberts καθηγητής του Τεχνολογικού Ινστιτούτου Μασαχουσέτης (M.I.T).

Αποτέλεσμα αυτών των προσπαθειών ήταν η δημιουργία, το 1969, ενός πειραματικού δικτύου μη ιεραρχικής δομής που έγινε γνωστό ως ARPANET και αρχικά συνέδεσε 4 πανεπιστήμια των Η.Π.Α.. Εκείνη ήταν η στιγμή που άρχισαν να γίνονται τα πρώτα βήματα για τη δημιουργία ενός δικτύου απομακρυσμένων υπολογιστών, το οποίο μελλοντικά θα μας οδηγήσει στη δημιουργία του Διαδικτύου όπως το γνωρίζουμε σήμερα.

Το 1962 ο Leonard Klienrock, καθηγητής στο Πανεπιστήμιο UCLA σήμερα, μίλησε για την ιδέα διαμερισμού του μηνύματος σε πακέτα πριν τη μετάδοσή του και το 1965 έγινε πειραματικά η σύνδεση του Πανεπιστημίου του Berkeley, με το M.I.T.. Αυτό αποτέλεσε το πρώτο δίκτυο ευρείας απόστασης (WAN).

Το 1967 παρουσιάστηκε για πρώτη φορά δημόσια από τον L.Roberts, στο πλαίσιο διεθνούς συνεδρίου που πραγματοποιήθηκε στο Γκάτλινμπουργκ του Τεννεσί, το σχέδιο για την δημιουργία του ARPANET. Πολλοί ήταν οι οργανισμοί

και τα πανεπιστήμια που εργάσθηκαν πάνω σε αυτό το σχέδιο ώστε να δημιουργηθεί ένα πρωτόκολλο με το οποίο θα επικοινωνούσαν οι υπολογιστές και θα μετέφεραν δεδομένα.

Το 1972 το ARPANET, δόθηκε σε χρήση προς το κοινό και πολλά δίκτυα άρχισαν να συμμετέχουν σε αυτό. Αυτή είναι και η στιγμή που ξεκινάει η πραγματική ανάπτυξη του Διαδικτύου.

Την ίδια χρονιά δημιουργήθηκε από εκείνους που συμμετείχαν στο πρόγραμμα A.R.P.A.,και που τώρα πλέον είχαν ως στόχο τους να εξαπλώσουν τις δυνατότητες του Διαδικτύου, ένα πρόγραμμα που επέτρεπε την επικοινωνία δύο υπολογιστών μέσω δικτύου το οποίο είναι γνωστό ως ηλεκτρονικό ταχυδρομείο (e-mail).

Έτσι γεννήθηκε το πρώτο περιορισμένου βεληνεκούς δίκτυο,μπου ονομάστηκε ARPAnet. Στη συνέχεια καθιερώθηκε η χρήση του UNIX, ενός πρωτοποριακού συστήματος.

Στις αρχές της δεκαετίας του ’80, μετά από μελέτες του πανεπιστημίου του Berkeley στην ανάπτυξη ενός πρωτοκόλλου που έδωσε την οριστική λύση στα προβλήματα συμβατότητας μεταξύ του UNIX και του TCP/IP, τέθηκαν τα θεμέλια ενός σύγχρονου κολοσσού του παγκοσμίου υπερδίκτυου Internet. Μέχρι τα τέλη του 2000, το Internet κάλύπτε περισσότερες από 80 χώρες, συνέδέε μεταξύ τους περισσότερα από 18.000 δίκτυα, 40.000.000 υπολογιστές και φυσικά 40.000.000 άτομα σήμερα εκτιμάται ότι οι χρήστες ξεπερνούν τα 800.000.000 άτομα και είναι κάθε ηλικίας κι εθνικότητας.

1.1.2 Η κουλτούρα του Internet

Το Ίντερνετ ασκεί τρομερή επιρροή στην γνώση και την διαμόρφωση απόψεων . Μέσα από την αναζήτηση λέξεων-κλειδιών (key words) μέσω της χρήσης μηχανών αναζήτησης όπως τοGoogle, εκατομμύρια άνθρωποι έχουν εύκολη και άμεση πρόσβαση σε ένα τεράστιο, παγκόσμιο και ποικίλο όγκο πληροφοριών. Συγκρινόμενο με τις έντυπες εγκυκλοπαίδειες και τις παραδοσιακές βιβλιοθήκες, το Ίντερνετ αντιπροσωπεύει μία ξαφνική και απότομη αποκέντρωση των πληροφοριών και των δεδομένων.

Η γλώσσα που χρησιμοποιείται περισσότερο για την επικοινωνία στο Διαδίκτυο είναι η Αγγλική. Αυτό συμβαίνει κυρίως λόγω της Αμερικανικής καταγωγής του Ίντερνετ, της χρήσης της Αγγλικής στον προγραμματισμό και την δημιουργία λογισμικού και στην αδυναμία των πρώτων γενεών υπολογιστών να χρησιμοποιήσουν άλλους χαρακτήρες πέραν του λατινικού αλφάβητου.

Έχοντας αναπτυχθεί πάρα πολύ τα τελευταία χρόνια, το Διαδίκτυο περιλαμβάνει πλέον ποιοτικά και ποσοτικά ευρύ περιεχόμενο και στις υπόλοιπες γλώσσες των περισσότερο αναπτυγμένων χωρών. Ωστόσο, υπάρχουν ακόμα δυσλειτουργίες και τεχνικά προβλήματα.

1.1.3 Το Internet και η επιχειρηματικότητα

Βλέπουμε λοιπόν, μέσα σε λίγα χρόνια, το Internet γίνεται ευρύτερα γνωστό και όλο και περισσότεροι άνθρωποι γίνονται χρήστες του διαδικτύου. Η χρήση του διαδικτύου δεν περιορίζεται φυσικά μόνο σε προσωπικό επίπεδο αλλά απλώνεται και γίνεται μέρος της πολιτικής και στρατηγικής μικρών, μεσαίων και μεγάλων

επιχειρήσεων. Έτσι δραστηριότητες όπως η διαφήμιση, οι συναλλαγές, η προώθηση προϊόντων , το μάρκετινγκ, οι επιχειρησιακές επικοινωνίες, γενικότερα πλήθος επιχειρηματικών δραστηριοτήτων, βρίσκουν εφαρμογή και πρόσφορο έδαφος ανάπτυξής τους στο διαδικτυακό χώρο ή κυβερνοχώρο.

Το internet έχει μπει για τα καλά στη ζωή μας και δεν μας προσφέρει απλώς ψυχαγωγία ή επικοινωνία.

1.1.4 Βασικά χαρακτηριστικά του internet

Μερικά αξιοσημείωτα χαρακτηριστικά του Διαδικτύου είναι:

- Η ιδιαιτερότητα που διέπει το ιδιοκτησιακό καθεστώς του. Ανήκει σε όλους και ταυτόχρονα δεν είναι ιδιοκτησία κανενός.

- Η ελεύθερη διακίνηση ιδεών και η ανταλλαγή πληροφοριών μεταξύ των χρηστών, ανεξάρτητα από τη γεωγραφική απόσταση και την πολιτική, ιδεολογική ή θρησκευτική κατάσταση της χώρας τους.

- Οι μεγάλες οικονομικές δυνατότητες που προσφέρει και η άμεση εμφάνιση διαδικτυακών εταιρειών.

1.1.5 Νομικά και ηθικά ζητήματα του internet

Μια γενική ανησυχία αναφορικά με το Διαδίκτυο πηγάζει από μέρος του περιεχομένου του που είναι αρκετά (έως πολύ) αμφισβητήσιμο. Η παραβίαση πνευματικών δικαιωμάτων, η πορνογραφία, η ψευδοπροσωπία και η προσφορά παράνομων προϊόντων είναι φαινόμενα υπαρκτά στο Ίντερνετ και ο περιορισμός τους είναι ιδιαίτερα δύσκολος.

Το Διαδίκτυο έχει κατηγορηθεί ως παράγοντας που έπαιξε ρόλο σε θανάτους, σε περιπτώσεις παιδεραστίας, σε ιστοσελίδες σατανιστών κ.ά. Επιπλέον, το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη, αντίστοιχη, αρχή, η οποία να ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί - σύμφωνα με πολλούς χρήστες αυτό θα αποτελούσε λογοκρισία.

Όπως χαρακτηριστικά λέγεται "το Διαδίκτυο ελέγχεται από τους χρήστες του". Βεβαίως, οι κρατικές υπηρεσίες και αστυνομίες σε κάθε χώρα, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου. Στην Ελλάδα υπάρχει η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος. Σε ορισμένες χώρες (όπως π.χ. στις Κίνα, Ιράν, Βόρεια Κορέα) ο κρατικός μηχανισμός παρεμβαίνει στους παρόχους υπηρεσιών Διαδικτύου, υποχρεώνοντάς τους να βάλουν φραγή σε ορισμένους, επιλεγμένους Διαδικτυακούς χώρους.

1.2 Διαδικτυακοί κίνδυνοι

Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.

1.2.1 Πρόκληση ζημιών στο υπολογιστικό σύστημα

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανύποπτου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο αρχείο, φαινομενικά αθώο, όπως ένα κείμενο ή μια φωτογραφία και, όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα και μπορεί να καταστρέψει αρχεία ή το σκληρό δίσκο του συστήματος.

Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη (φυλλομετρητή ή Λειτουργικό Σύστημα).

Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm (κατά λέξη μετάφραση σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth).

Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

1.2.2 Πρόκληση ζημιών σε προσωπικά δεδομένα

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνον είναι δυνατό να υφαρπαγούν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών Τραπέζης κτλ.

Ανάλογη μέθοδος ακολουθείται και από ορισμένους ιστότοπους, στους οποίους ο ανύποπτος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλνοντας ένα προϊόν, το οποίο όχι μόνο δε θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστότοπου για να πραγματοποιήσουν οι ίδιοι αγορές, χρεώνοντας τον "πελάτη" τους.

Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται "Phishing" (παραφθορά της λέξης fishing = ψάρεμα). Αρκετά προγράμματα περιήγησης (browsers) αναγνωρίζουν τους ιστότοπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα, ωστόσο αυτό δεν συμβαίνει σε ποσοστό 100%.

Οι χρήστες είναι καλό να γνωρίζουν ότι κανείς χρηματοπιστωτικός φορέας δεν χρησιμοποιεί το Διαδίκτυο για να ανανεώσει προσωπικές πληροφορίες, ενώ ένας προστατευμένος ιστότοπος αρχίζει πάντα με το πρόθεμα https (secure, ασφαλής).

1.2.3 Παραπλάνηση

Αρκετές φορές οι χρήστες του Διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι

εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε για αποκομιδή ιδίου οφέλους είτε, απλά, η χαρά της παραπλάνησης των (αγνώστων) χρηστών. Ο όρος που περιγράφει αυτού του τύπου την παραπλάνηση είναι "Hoax".

1.2.4 Προστασία

Υπάρχουν τρεις τρόποι προστασίας, οι οποίοι θα πρέπει να χρησιμοποιούνται σε συνδυασμό:

- Χρήση τείχους προστασίας (firewall)
- Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (spyware).
- Χρήση λογισμικού προστασίας ενάντια σε spamming (ανεπιθύμητης αλληλογραφίας).

1.3 Ο ορισμός ηλεκτρονικού ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο αποτελεί σήμερα τη βασικότερη μορφή επικοινωνίας στο Διαδίκτυο. Υποστηρίζει την ανταλλαγή μηνυμάτων μεταξύ χρηστών χάρη στην προσωπική ηλεκτρονική διεύθυνση του καθενός η οποία μπορεί να παρομοιαστεί με μια πλήρη ταχυδρομική διεύθυνση.

Το περιεχόμενο του μηνύματος, μπορεί να είναι κείμενο, ήχος, εικόνα, βίντεο ή δεδομένα. Κάθε χρήστης έχει τη δική του μοναδική διεύθυνση η οποία

χρησιμοποιεί αποκλειστικά λατινικούς χαρακτήρες και έχει την παρακάτω μορφή: onoma@paroxeasypiresiwn.kataliksi.

Την μοναδική και προσωπική αυτή διεύθυνση του ηλεκτρονικού ταχυδρομείου την προμηθεύει ο πάροχος υπηρεσιών διαδικτύου που έχει επιλεγεί (ενίοτε και δωρεάν), ενώ απαιτείται και ένας προσωπικός κωδικός πρόσβασης (password), ο οποίος παρέχει ασφαλή χρήση της ηλεκτρονικής αλληλογραφίας.

Ουσιαστικά το Ηλεκτρονικό ταχυδρομείο μπορεί να οριστεί ως τον ακρογωνιαίο λίθο σε ότι συμβαίνει στο Internet, είναι μια απλή υπηρεσία που επιτρέπει σε δύο ή σε περισσότερους ανθρώπους να στέλνουν μηνύματα ο ένας στον άλλον, σε σχεδόν πραγματικό χρόνο.

Πολλοί θεωρούν το ηλεκτρονικό ταχυδρομείο ως την πιο διαδεδομένη υπηρεσία του Internet. Σύμφωνα με αυτούς είναι «ένα εργαλείο μεταβίβασης και ανταλλαγής μηνυμάτων. Τα περισσότερα μηνύματα περιέχουν απλό κείμενο, άλλα μπορεί κανείς να στείλει και εικόνες, σχέδια ή φωτογραφίες».

Πέραν της χρήσης του e-mail για κοινωνικούς ή απλά ψυχαγωγικούς σκοπούς, θεωρείται ως το πλέον δημοφιλές μέσο επικοινωνίας στις εταιρείες και γενικότερα για τους επαγγελματίες. Είναι τόσο εύχρηστο και αποτελεσματικό όπου πλέον ακόμα και οι δημόσιες υπηρεσίες ενός κράτους επιβάλουν στους υπαλλήλους τους τη χρήση του e-mail για λόγους αποτελεσματικότητας και επιτάχυνσης των διαδικασιών.

1.3.1 Ιστορική αναδρομή του ηλεκτρονικού ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο έχει ήδη συμπληρώσει τέσσερις δεκαετίες ζωής. Ουσιαστικά έκανε την εμφάνισή του από τη λειτουργία των πρώτων κιόλας ηλεκτρονικών συστημάτων, υπήρχε ακόμη και πριν από το ARPANET. Τότε

κάλυπτε την επικοινωνία κάποιων χειριστών που εργαζόντουσαν στα ίδια υπολογιστικά συστήματα διαφορετικές ώρες της ημέρας.

Ήδη από τη δεκαετία του 1960 αρκετά μέλη της Αμερικάνικης Πανεπιστημιακής Κοινότητας έστειλαν μηνύματα ο ένας στον άλλο. Δεν υπήρχε όμως η δυνατότητα επικοινωνίας μεταξύ διαφορετικών υπολογιστικών συστημάτων.

Θεμελιωτής της σύγχρονης μορφής ηλεκτρονικού ταχυδρομείου θεωρείται ο Ray Tomilnson, μηχανικός ηλεκτρονικών υπολογιστών, επικεφαλής ομάδας ερευνών στην επιχείρηση μηχανολογικού εξοπλισμού BBN με έδρα το Cambridge της Μασαχουσέτης. Ήταν εκείνος που κατά τη διετία 1971-1972 κατάφερε να δημιουργήσει ένα μικρό και απλό πρόγραμμα ανταλλαγής ηλεκτρονικών μηνυμάτων μεταξύ δύο υπολογιστών.

Κατάφερε να στείλει μήνυμα σε περισσότερο από ένα δίκτυο της επιχείρησης στην οποία εργαζόταν, ενώ ως τότε η ανταλλαγή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου ήταν εφικτή μόνο μέσω μεμονωμένων δικτύων. Ήταν επίσης εκείνος που επέλεξε το σύμβολο @ για να ξεχωρίσει την ονομασία του “χρήστη” από εκείνου του “οικοδεσπότη” του.

Σήμερα υπολογίζεται σύμφωνα με την εταιρεία ερευνών IDC, ότι περίπου 300

εκατομμύρια χρήστες παγκοσμίως ανταλλάσσουν κάτι λιγότερο από 10 δισεκατομμύρια emails καθημερινά. Πολλοί άνθρωποι χρησιμοποιούν το Διαδίκτυο αποκλειστικά για να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο χωρίς να ενδιαφέρονται για τις άλλες υπηρεσίες. Αυτός είναι άλλωστε και ο λόγος που πολλές εταιρείες εκτός βέβαια από τους πάροχους σύνδεσης, προσφέρουν δωρεάν ηλεκτρονικό ταχυδρομείο σε χρήστες από όλον τον κόσμο. Π.χ. yahoo, google, msn κ.τ.λ.

1.4 Σύγκριση ηλεκτρονικού ταχυδρομείου - φαξ – τηλεφώνου

Είδαμε πως η τεχνολογική εξέλιξη μας οδήγησε στην δημιουργία και χρήση του ηλεκτρονικού ταχυδρομείου. Πριν όμως από την εκτεταμένη χρήση του προ υπήρχαν το τηλέφωνο και το fax (τηλομοιότυπο). Παρακάτω θα μελετήσουμε τα πλεονεκτήματα και τα μειονεκτήματά του σε σχέση με αυτά.

1.4.1 Πλεονεκτήματα

Το σημαντικότερο από τα πλεονεκτήματα που παρουσιάζει το ηλεκτρονικό ταχυδρομείο, είναι το γεγονός ότι είναι οικονομικότερο εφόσον κατά κανόνα προσφέρεται δωρεάν ή διαφορετικά η τιμή αποστολής ενός μηνύματος είναι σταθερή και ελάχιστη ανεξάρτητα από τον τόπο του αποστολέα και του δέκτη. Ένα ηλεκτρονικό μήνυμα κοστίζει το ίδιο είτε αποστολέας και δέκτης βρίσκονται

στην ίδια γειτονιά, στην ίδια πόλη, στην ίδια χώρα ή ακόμα και αν βρίσκονται σε διαφορετικές ηπείρους.

Αντίθετα τα κόστη του fax (τηλομοιότυπο) και του τηλεφώνου εξαρτώνται από την απόσταση. Όσο μεγαλύτερη η απόσταση τόσο μεγαλύτερο το κόστος. Όσον αφορά το τηλέφωνο , ο χρόνος χρήσης του το επιβαρύνει κατά πολύ. Βέβαια το internet προσφέρει τελευταία και μια νέα λύση όσον αφορά τις κλήσεις φωνής. Το skipe είναι ένα άλλο επαναστατικό λογισμικό το οποίο μας επιτρέπει να κάνουμε τηλεφωνικές κλήσεις από τον υπολογιστή μας με μηδενικό κόστος. Ακόμα και βιντεοκλήσεις ή και κλήσεις συνδιασκέψεις με πολλούς συνομιλητές ταυτοχρόνως.

Παρόλα αυτά είναι σημαντικό το γεγονός πως με το ηλεκτρονικό ταχυδρομείο μπορεί να σταλεί ένας μεγάλος όγκος πληροφοριών και αρχείων σε πολλαπλούς δέκτες ταυτόχρονα. Αυτό είναι απαγορευτικό για τα άλλα δύο μέσα επικοινωνίας. Οι δέκτες αυτοί μπορεί να έχουν καταχωρηθεί στο ηλεκτρονικό ταχυδρομείο του αποστολέα ανά ομάδες ανάλογα με διάφορα κοινά χαρακτηριστικά, π.χ. συνεργάτες, φίλοι, συνάδελφοι κ.τ.λ. διευκολύνοντας έτσι τη διεκπεραίωση των εργασιών τους.

Όταν κάποιος χρησιμοποιεί το τηλέφωνο ή το fax είναι υποχρεωμένος να πραγματοποιεί μία και μόνο κλήση ανά δέκτη. Αυτό δυσχεραίνει την εργασία και αποτελεί σπατάλη χρόνου.

Στα πλεονεκτήματα πρέπει να προστεθεί και η δυνατότητα που παρέχεται στο χρήστη του ηλεκτρονικού ταχυδρομείου να αποστέλλει αρχεία με πολλές μορφές σε αντιδιαστολή με το τηλέφωνο που είναι εφικτό να υπάρξει επικοινωνία μονάχα βάση ήχου (ομιλία, μουσική) ή του fax που μπορεί να γίνει μόνο αποστολή κειμένου και εικόνας. Το ηλεκτρονικό ταχυδρομείο όχι μόνο προσφέρει και καλύπτει τις δύο παραπάνω μορφές επικοινωνίας αλλά μπορεί και να τις συνδυάσει. Είναι φανερό λοιπόν πως είναι δυνατή η αποστολή οποιουδήποτε

αρχείου, όποια μορφή κι αν αυτό έχει. Έτσι είναι εφικτή η οποιαδήποτε αποστολή αρχείου, είτε αυτή είναι εικόνα, ήχος, ακόμα και σε μορφή video.

Δεν πρέπει επιπρόσθετα να παραμελήσουμε το γεγονός πως η χρήση του ηλεκτρονικού ταχυδρομείου μας επιτρέπει να αποστέλλουμε μηνύματα οποιαδήποτε ώρα της ημέρας επιθυμούμε χωρίς να ενοχλούμε εφόσον ο δέκτης μπορεί να έχει πρόσβαση σε αυτό οποτεδήποτε κάνει χρήση του ηλεκτρονικού ταχυδρομείου του. Υπάρχει διακριτικότητα, ο παραλήπτης δεν ενοχλείτε όταν φτάνει το μήνυμα. Είναι αυτονόητο πως η χρήση του τηλεφώνου στις τρεις η ώρα τα ξημερώματα για ένα μη επείγον ζήτημα είναι τουλάχιστον ενοχλητική.

Μεγάλης σημασίας είναι επιπλέον η δυνατότητα που παρέχουν πολλές διαδικτυακές υπηρεσίες για διάθεση δωρεάν ηλεκτρονικού ταχυδρομείου. Όπως ισχύει για το τηλέφωνο και το fax, έτσι και για το ηλεκτρονικό ταχυδρομείο προαπαιτείται μια τηλεφωνική γραμμή , χωρίς να απαιτείται κάποιο επιπρόσθετο κόστος.

Τέλος η δυνατότητα να αποστέλλονται μεγάλα σε όγκο αρχεία ταυτόχρονα σε πολλούς αποδέκτες, σε ελάχιστο χρόνο, καθιστά το ηλεκτρονικό ταχυδρομείο ένα οικολογικό μέσο επικοινωνίας. Απαιτεί πολύ μικρή κατανάλωση ενέργειας που άμεσα οδηγεί σε εξοικονόμηση ενέργειας, ενώ τεράστιες είναι και οι ποσότητες χαρτιού που εξοικονομούνται από τη μη χρήση των φαξ.

1.4.2 Μειονεκτήματα

Το βασικότερο μειονέκτημα που παρουσιάζει το ηλεκτρονικό ταχυδρομείο σε σχέση με το τηλέφωνο και το fax, είναι οι κίνδυνοι που υπάρχουν κατά την παραλαβή αρχείων. Στη σύγχρονη εποχή με τις διαστάσεις που έχει πάρει η χρήση του INTERNET ολοένα και πληθαίνουν εκείνοι οι χρήστες που δημιουργούν διαφόρους ιούς και με μεγάλη ευκολία τους αποστέλλουν με e-mails. Οι ιοί αυτοί

εισχωρούν στο σύστημα του ηλεκτρονικού υπολογιστή προκαλώντας από μικρές βλάβες που μπορούν να επιδιορθωθούν έως και καθολική καταστροφή του λογισμικού με αποτέλεσμα την αχρήστευση του ηλεκτρονικού υπολογιστή.

Πολλές είναι οι εταιρείες βέβαια που στην προσπάθειά τους να εξαλείψουν ή να περιορίσουν το κίνδυνο αυτό δημιουργούν προληπτικά και κατασταλτικά προγράμματα, τα γνωστά Antivirus. Τα προγράμματα αυτά όμως είναι αποτελεσματικά μόνο σε γνωστούς ιούς, οπότε η δημιουργία και η μετάδοση οποιουδήποτε νέου ιού, δεν μπορεί να προστατεύσει τον υπολογιστή. Είναι σαφές πως οι ιοί δεν μπορούν να δράσουν και να επηρεάσουν το τηλέφωνο ή το fax εφόσον απαιτείται η ύπαρξη και η χρήση λογισμικού.

Ένα σημαντικό πρόβλημα που παρουσιάζει το ηλεκτρονικό ταχυδρομείο είναι η ευκολία με την οποία μπορεί να παραβιαστεί η ιδιωτικότητά του. Έχει παρατηρηθεί και αναφερθεί πολλές φορές πως διάφοροι χρήστες του Internet, έχουν καταφέρει να εισχωρήσουν στο ηλεκτρονικό ταχυδρομείο άλλων χρηστών, είτε υποκλέπτοντας στοιχεία και αρχεία, είτε για περιπαικτικούς λόγους. Παρόλο που για την εισαγωγή στο προσωπικό e-mail απαιτείται ως δικλείδα ασφαλείας η εισαγωγή ενός προσωπικού κωδικού, αυτό απλά αποτελεί κίνητρο για πολλούς χρήστες να εισβάλλουν σε ξένα e-mails. Ένα παράδειγμα αυτών των χρηστών είναι οι Hackers. Hacker χαρακτηρίζεται αυτός που διεισδύει ή παραβιάζει την ακεραιότητα συστημάτων (σπάει κωδικούς ασφαλείας κλπ.) με πρόθεση τη διάπραξη κακόβουλων πράξεων, όπως καταστροφή δεδομένων, στρέβλωση συστημάτων και παρεμπόδιση λειτουργιών. Επιπλέον, λόγω του μη συγχρονισμού μεταξύ του αποστολέα και του δέκτη δεν είναι δυνατόν ο αποστολέας να γνωρίζει πως το μήνυμα έχει αποσταλεί με επιτυχία και πως ο δέκτης έχει ενημερωθεί γι' αυτό. Κινήσεις βέβαια για την αναβάθμιση τη υπηρεσίας αυτής πραγματοποιούνται συνεχώς με την παραχώρηση δυνατότητας αναφοράς παράδοσης από πολλές εταιρείες. Είναι όμως γεγονός πως οι περισσότεροι χρήστες

ηλεκτρονικού ταχυδρομείου παγκοσμίως είτε δε γνωρίζουν την ύπαρξη της υπηρεσίας είτε δεν τη θέτουν σε εφαρμογή. Βέβαια πέραν της ραγδαίας αύξησης των χρηστών, θεαματική αύξηση σημειώνεται επίσης και στο χρόνο που περνάει κάποιος μπροστά στον υπολογιστή. Συνεπώς αυξάνονται οι πιθανότητες να συγχρονισθούμε ή εάν όχι, να διαβαστεί το μήνυμα σχετικά σύντομα.

Το fax παρέχει αναφορά παράδοσης ενώ με το τηλέφωνο η συνομιλία αποτελεί αποδεικτικό της επικοινωνίας. Επίσης τελευταία χρησιμοποιούνται και συστήματα instant messaging (στιγμιαίο ταχυδρομείο, msn messenger κ.α.) που μας επιτρέπει να επικοινωνούμε με μηνύματα σε πραγματικό χρόνο.

Άλλη εξέλιξη είναι ο συγχρονισμός που μπορούμε να κάνουμε του λογαριασμού μας με το προσωπικό κινητό μας τηλέφωνο ώστε να λαμβάνουμε άμεσα τα μηνύματά μας.

Είναι επίσης δεδομένο πως το ηλεκτρονικό ταχυδρομείο, δεν αποτελεί πρώτη επιλογή μεταφοράς επειγόντων και άκρως σημαντικών θεμάτων. Ακριβώς τα

παραπάνω μειονεκτήματα καθώς και ο μη συγχρονισμός αποστολέα – δέκτη, προτρέπουν το χρήστη να χρησιμοποιήσει το τηλέφωνο για να μεταφέρει μια πληροφορία με ασφάλεια και ακρίβεια. Είναι χαρακτηριστικό παράδειγμα πως σε ένα ατύχημα, ή σε θέματα που αφορούν προβλήματα υγείας που χρίζουν άμεσης αντιμετώπισης η συνειρμική και η αυτόματη κίνηση θα είναι η χρήση του τηλεφώνου.

Άλλο κύριο μειονέκτημα το οποίο είναι και το κυρίως θέμα της παρούσας εργασίας είναι η ανεπιθύμητη αλληλογραφία (spamming). Ακριβώς λόγω του ότι ένα e-mail δεν κοστίζει, μπορούν κάποιοι να στέλνουν αναρίθμητα μηνύματα αδιακρίτως κυρίως για διαφημιστικούς σκοπούς, κάτι που θα κόστιζε πολύ χρήμα και χρόνο με οποιοδήποτε άλλο μέσο. Έχει τέλος κατηγορηθεί – και ίσως όχι άδικα – για την ανθρώπινη απομόνωση και την έλλειψη άμεσης επικοινωνίας όπως

αυτή φανερώνεται με την ανθρώπινη επαφή και χαρακτηριστικά προσφέρεται από το τηλέφωνο. Με τη χρήση του τηλεφώνου ο χρήστης γνωρίζει ακριβώς με ποιον ομιλεί, ενώ η προσωπική επαφή επιτυγχάνεται με την αλλοίωση της χροιάς και του τόνου της φωνής ανάλογα με το θέμα συζήτησης και τη σημαντικότητά του. Με τη χρήση του ηλεκτρονικού ταχυδρομείου ο χρήστης επικοινωνεί με τρόπο ψυχρό και απρόσωπο ενώ η ταυτότητα του ατόμου με το οποίο επικοινωνεί δηλώνεται χωρίς να μπορεί να ελεγχθεί.

Υπάρχουν βέβαια και κάποια θετικά ή αρνητικά χαρακτηριστικά που διέπουν τα μέσα αυτά και τα οποία εμφανίζονται με τέτοια συχνότητα τόσο στο fax, στο τηλέφωνο και στο ηλεκτρονικό ταχυδρομείο που δεν μπορούν να πιστωθούν ή να χρεωθούν σε κανένα από αυτά. Αυτά είναι η ταχύτητα με την οποία πραγματοποιείται μία κλήση ή που αποστέλλεται ένα μήνυμα, όπου ο χρόνος στη χρήση οποιουδήποτε από αυτά τα μέσα είναι ελάχιστος (αποστολή fax, e-mail, χρόνος κλήσης) και η λήψη διαφημιστικών ή άχρηστων πληροφοριών που πραγματοποιείται καθημερινά και είναι συνήθως αναπόφευκτη(spamming) . Όλοι μας βιώνουμε καθημερινά βομβαρδισμό διαφημιστικού υλικού ή προϊόντα ερευνών ή απλά ενημερώσεων είτε στα e-mail μας είτε κυρίως μέσω τηλεφώνου.

Η ανάπτυξη των νέων ηλεκτρονικών υπηρεσιών του Διαδικτύου (Internet) είναι μια πραγματικότητα που κερδίζει καθημερινά μεγαλύτερο έδαφος. Οι υπηρεσίες πλοήγησης στον παγκόσμιο ιστό (web-surfing), ηλεκτρονικής αλληλογραφίας (e-mail), μεταφοράς αρχείων (ftp), ηλεκτρονικού εμπορίου (e-Commerce) και άλλες, αποκτούν ολοένα και περισσότερους χρήστες με ποσοστά που σε κάποιες χώρες ξεπερνούν το 70% του πληθυσμού (ΗΠΑ, Σουηδία κα). Στη χώρα μας, οι χρήστες του Διαδικτύου εκτιμάται ότι έχουν υπερβεί το 15% του πληθυσμού και αυξάνονται με υψηλό ρυθμό.

Οι νέες υπηρεσίες αξιοποιούνται για ποικίλους λόγους. Είναι πιθανόν να χρησιμοποιηθούν στην αρχή για παιχνίδι ή ψυχαγωγία, κι αυτό ανεξάρτητα από

την ηλικία του χρήστη. Σύντομα όμως, μπορεί να διαπιστώσει κάποιος την δυνατότητα του Διαδικτύου να παρέχει πρόσβαση σε ενημέρωση, πληροφόρηση, γνώση και να αποτελέσει ένα εξελιγμένο εργαλείο που μπορεί να υποστηρίξει τις επαγγελματικές και επιχειρηματικές δραστηριότητες.

Η ηλεκτρονική αλληλογραφία είναι από τις πιο δημοφιλείς νέες υπηρεσίες που παρέχονται μέσω του Διαδικτύου. Με πολύ χαμηλό κόστος και σε ελάχιστα δευτερόλεπτα ή έστω μερικά λεπτά, μικρά ή εκτενή κείμενα, φωτογραφίες, video, ακόμα και ηχογραφημένα (ψηφιοποιημένα) μηνύματα μπορούν να φτάσουν στον παραλήπτη αυτής της νέας μορφής αλληλογραφίας, σε όποια γωνιά της γης και αν βρίσκεται.

Η αυθαίρετη ηλεκτρονική αλληλογραφία είναι απλά το σύνολο των μηνυμάτων που στέλνονται σε ένα χρήστη χωρίς την συναίνεσή του ή την εκδήλωση της επιθυμίας του να τα λαμβάνει. Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση των προϊόντων ή των υπηρεσιών τους. Συχνά, αυτά τα ηλεκτρονικά μηνύματα περιλαμβάνουν προτάσεις για προγράμματα, προσφορές για γραμμές τηλεφωνικού ή δικτυακού σεξ, προσκλήσεις σε δικτυακό τζόγο που προκαλούν σύγχυση, είναι πολλές φορές προσβλητικά και κοστίζουν ακριβά για να τα «κατεβάσει» κανείς, να τα διαβάσει και να τα διαγράψει.

Η μεγάλη διάδοση που γνωρίζει η αυθαίρετη ηλεκτρονική αλληλογραφία, θα κάνει το ηλεκτρονικό ταχυδρομείο όλο και πιο δύσκολο στη χρήση του, ίσως και ακόμη τελείως άχρηστο ως μέσο επικοινωνίας για καταναλωτές και επιχειρήσεις αν το πλήθος των μηνυμάτων συνεχίσει να αυξάνει αντί να μειωθεί δραστικά.

ΚΕΦΑΛΑΙΟ 2ο:ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΓΥΡΟ ΑΠΟ ΤΟ SPAM

2.1 Ορισμός και κατηγοριοποίηση της έννοιας SPAM

Spam ή αλλιώς Junk Mail αποκαλείται η ανεπιθύμητη αλληλογραφία. Για την ιστορία, το καθ' αυτού Spam ήταν το πρώτο κονσερβοποιημένο κρέας που κατασκεύασε μια εταιρεία ονόματι Hormel στις αρχές του 20ου αιώνα. Το Spam έγινε ευρύτερα γνωστό κατά τη διάρκεια του 2ου Παγκοσμίου Πολέμου με απίστευτα νούμερα από κονσέρβες να έχουν διατεθεί κατά τη διάρκεια του. Λέγεται ότι αν όλες οι κονσέρβες Spam που έχουν καταναλωθεί έως και σήμερα έμπαιναν στη σειρά, θα έκαναν το γύρο του πλανήτη 10 φορές! Ίσως λόγο αυτού του όγκου και μαζικότητας επελέγη το όνομα Spam ως όρος για την ανεπιθύμητη αλληλογραφία

Υπάρχουν δύο κύριοι τύποι Spam οι οποίοι έχουν διαφορετικά χαρακτηριστικά, αλλά το ίδιο αποτέλεσμα στους χρήστες του Διαδικτύου. Το USENET Spam και το EMAIL Spam

USENET SPAM

Το USENET Spam είναι ένα ενιαίο μήνυμα που στέλνεται σε 20 ή περισσότερες ομάδες πληροφόρησης (Newsgroups) του USENET. (Το USENET είναι ένα παγκόσμια κατανεμημένο σύστημα συζητήσεων. Αποτελείται από ένα σύνολο "ομάδων πληροφόρησης" (newsgroups) όπου τα ονόματα των ομάδων ταξινομούνται ιεραρχικά).Το USENET Spam στοχεύει ακόμα και χρήστες που ενώ διαβάζουν τις ομάδες πληροφόρησης, σπάνια ή ποτέ δεν δίνουν την ηλεκτρονική

διεύθυνσή τους. Το USENET Spam λοιπόν ληστεύει το ηλεκτρονικό ταχυδρομείο αυτών των χρηστών χρησιμοποιώντας ένα «μπαράζ» διαφημίσεων ή άλλων άσχετων θεμάτων. Επιπλέον, το USENET Spam προβληματίζει τους administrators και τους ιδιοκτήτες συστημάτων να διαχειριστούν τα θέματα των newsgroups που δέχονται στα συστήματά τους, οπότε και τα θέματα που περιέχουν Spam δεν μπορούν να φιλτραριστούν.

EMAIL SPAM

Το EMAIL Spam στοχεύει σε μεμονωμένους χρήστες του ηλεκτρονικού ταχυδρομείου, στέλνοντάς τους μηνύματα άμεσα στο ηλεκτρονικό τους γραμματοκιβώτιο. Οι κατάλογοι με διευθύνσεις για αποστολή Spam αλληλογραφίας δημιουργούνται συχνά είτε με τυχαίες ταχυδρομήσεις, είτε μέσω ανίχνευσης του USENET, είτε κλέβοντας καταλόγους διευθύνσεων του Διαδικτύου, ή με στοχευμένη έρευνα στο Internet αναζητώντας διευθύνσεις χρηστών του. Το Spam κοστίζει στους χρήστες για την λήψη του. Εύκολα καταλαβαίνουμε ότι κάποιος χρήστης με μια dial-up σύνδεση χαμηλής ταχύτητας ξοδεύει χρόνο και χρήμα καθώς μένει περισσότερη ώρα συνδεδεμένος στο Internet περιμένοντας να κατεβάσει την αλληλογραφία του, και παράλληλα κατεβαίνει και η Spam αλληλογραφία.

2.1.1.Οι πηγές του SPAM

Ο όρος spam χρησιμοποιήθηκε αρχικά σε ομάδες συζήτησης του Usenet για να περιγράψει πανομοιότυπες διαφημίσεις ή εκτός θέματος επιστολές που απευθύνονταν ταυτόχρονα σε περισσότερες ομάδες συζήτησης. Από τότε ο όρος έχει επεκταθεί ώστε να συμπεριλαμβάνει και τα USE (ανεπιθύμητα διαφημιστικά ηλεκτρονικά μηνύματα) και τα UBE (ανεπιθύμητα ογκώδη ηλεκτρονικά μηνύματα). Η χρήση του ονόματος ενός κονσερβοποιημένου χοιρινού γεύματος για αυτές τις επιστολές και τα μηνύματα εμπνεύστηκε από μια μικρή κωμωδία του Monty Python στην οποία μια ομάδα Vikings τραγουδούσε στο βάθος “Spam, spam, spam,……”, επισκιάζοντας κάθε άλλη συζήτηση. Το spam δρα παρομοίως, αν και οι περισσότεροι νέοι χρήστες για να μην ενοχλούνται από αυτά, χρησιμοποιούν προγράμματα που τα αναγνωρίζουν και τα διαγράφουν.

2.1.2 Τα πρώτα SPAM

Ο Einar Stefferud, ένας μακροχρόνιος χειριστής του δικτύου, αναφέρει ότι η DEC το 1978, ανακοίνωσε ένα νέο DEC-20 μηχάνημα στέλνοντας μια πρόσκληση σε όλες τις ARPANET διευθύνσεις στη δυτική ακτή, αφού χρησιμοποίησε τον κατάλογο διευθύνσεων του δικτύου ARPANET, προσκαλώντας άτομα σε μια δεξίωση στη Καλιφόρνια. Η εταιρεία τιμωρήθηκε διότι παραβίασε την πολιτική χρήσης της ARPANET και ένα μήνυμα στάλθηκε σ’ αυτήν για να υπενθυμίσει τους κανόνες. Φυσικά κανείς τότε δεν ήξερε ότι αυτό θα ονομαζόταν αργότερα spam. Ακόμα νωρίτερα μία άλλη περίπτωση ενός spam πραγματοποιήθηκε το 1971. Κάποιος ονόματι Peter Bos χρησιμοποίησε το CTSS MAIL για να στείλει σε όλους το εξής αντιπολεμικό μήνυμα : “THERE IS NO WAY TO PEACE. PEACE IS THE WAY.” Αναφέρεται ότι ο spammer υποστήριζε το spam του λέγοντας, «μα αυτό είναι σημαντικό»!!!.

2.1.3 Είδη SPAMMING

Οι περιγραφές που ακολουθούν ερμηνεύουν κάποιους απ' τους όρους που χρησιμοποιούνται στις συζητήσεις σχετικά με το Spamming. Αυτές οι ερμηνείες επίσης θα διευκρινίσουν κάποιους όρους που συχνά χρησιμοποιούνται λανθασμένα όταν περιγράφονται προβλήματα με τα ηλεκτρονικά μηνύματα.

- **Spamming:** Είναι η διαδικασία της αποστολής ηλεκτρονικού μηνύματος σε ένα μεγάλο αριθμό ηλεκτρονικών διευθύνσεων και συχνά συγκρίνεται με τον όρο "junk mail" που χρησιμοποιείται για να περιγράψει παρόμοιες δραστηριότητες που πραγματοποιούνται μέσω ταχυδρομικών υπηρεσιών. Εντούτοις,, υπάρχει άλλη μια δραστηριότητα που ονομάζεται Spamming. Αυτή είναι όταν ένας μονός υπολογιστής κατακλύζεται με ηλεκτρονικά μηνύματα σε μια προσπάθεια να προκαλέσει ενόχληση και έξοδα.

- **Spam:** Χρησιμοποιείται όταν αναφέρεται σε ένα ή πολλαπλά κομμάτια ηλεκτρονικών μηνυμάτων τα οποία αντιλαμβάνονται από τον παραλήπτη ως ανεπιθύμητα και ως αποτελέσματα του Spamming.

- **Spoofing:** Είναι η διαδικασία σύνδεσης με έναν πράκτορα μεταφορών ηλεκτρονικών μηνυμάτων, και νόθευσης της πληροφορίας που απαιτείται να παρέχει, έτσι ώστε να προκαλέσεις το μήνυμα να φαίνεται ότι προέρχεται από κάποιον άλλον και όχι από εσένα.

- **Mail Forwarding:** Η διαδικασία της λήψης και αποστολής μηνύματος το οποίο κατευθύνεται σε ένα mail server αλλά στην ουσία κατευθύνεται ολοκληρωτικά κάπου αλλού παρά σε εκείνη την ιστοσελίδα.

- **Host:** Ένας υπολογιστής συνδεδεμένος στο δίκτυο, ο οποίος παρέχει δυνατότητα πρόσβασης στο δίκτυο.
- **Postmaster:** Το άτομο ή τα άτομα που είναι υπεύθυνα και εξασφαλίζουν ότι το σύστημα μηνυμάτων στην ιστοσελίδα δουλεύει κανονικά. Postmaster μπορεί να είναι το άτομο που εγκαθιστά το προϊόν που χειρίζεται το μήνυμα, ή κάποιος ο οποίος έχει πολύ μικρή εμπειρία στους υπολογιστές και στα ηλεκτρονικά μηνύματα. Η εμπειρία έχει δείξει ότι postmaster μπορεί να είναι ο καθένας.

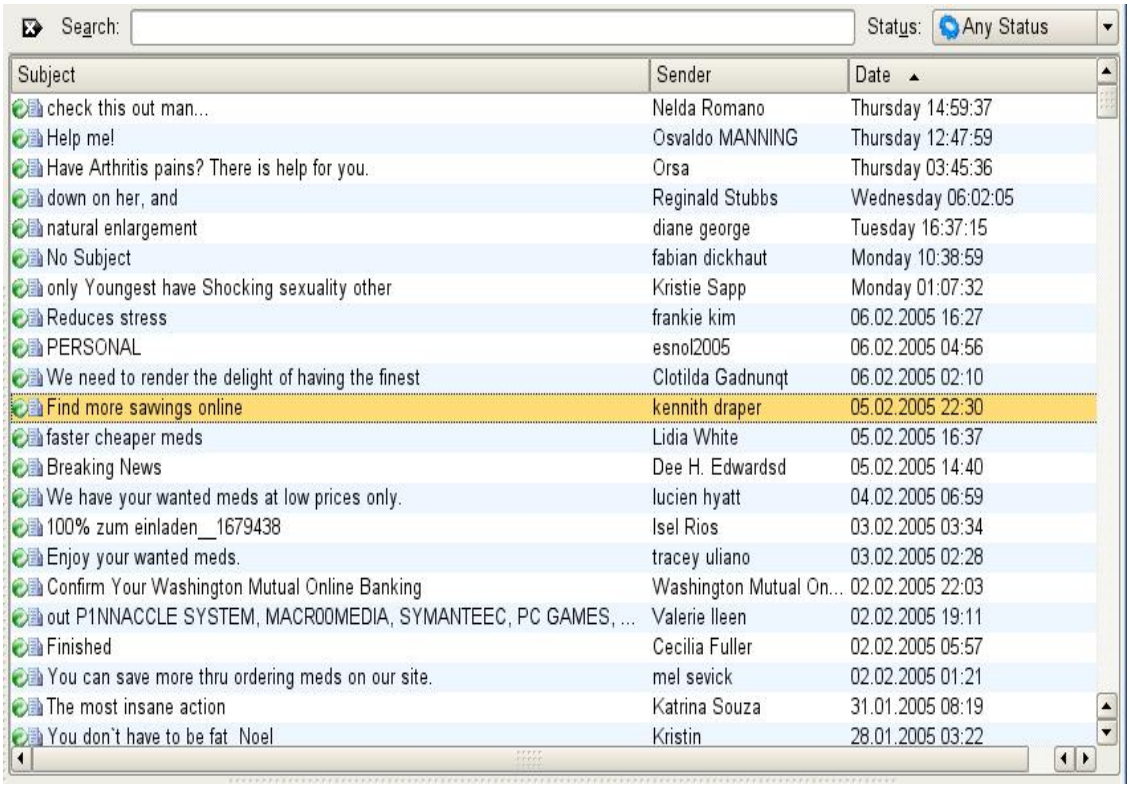
2.1.4 SPAM (Ηλεκτρονικό)

Ο πιο κοινός τύπος Spam είναι αυτός που μεταφέρεται μέσω της υπηρεσίας του ηλεκτρονικού ταχυδρομείου στην μορφή μιας εμπορικής διαφήμισης. Εντούτοις, οι άνθρωποι έχουν κάνει πράγματα συγκρινόμενα (ανάλογα) του Spamming και για πολλούς άλλους λόγους εκτός από τους διαφημιστικούς, και σε άλλα μέσα εκτός του ηλεκτρονικού ταχυδρομείου. Μια απ’ τις δυνατότητες των ηλεκτρονικών μέσων είναι ότι πραγματικά δεν κοστίζει τίποτα να σταλθεί ένα μήνυμα. Αφού αυτά τα έξοδα πληρωθούν, το κόστος να μεταβιβάσεις ένα μήνυμα σε έναν μονό δέκτη είναι μηδαμινό, όταν συγκριθεί με παλαιότερα μέσα όπως το ταχυδρομικό μήνυμα. Η ηλεκτρονική ανταλλαγή μηνυμάτων είναι φτηνή, γρήγορη και εύκολη να αυτοματοποιηθεί. Τα προγράμματα των υπολογιστών μπορούν να στείλουν εκατομμύρια μηνύματα μέσα σε λεπτά ή ώρες με σχεδόν καθόλου κόστος. Παραδοσιακές μέθοδοι διαφήμισης, όπως πίνακες αγγελιών, διαφημίσεις

τηλεόρασης και εφημερίδων είναι παρόμοιες με το spam στο ότι είναι συνήθως ανεπιθύμητα και στέλνονται σε μεγάλες ποσότητες. Η μόλυνση του δημόσιου χώρου από την διαφήμιση είναι επίσης αρκετά παρόμοια με το πρόβλημα του spam. Το Spamming έχει θεωρηθεί από διάφορους διαφημιστικούς, κυβερνητικούς και ανεξάρτητους τομείς ότι είναι ένα από τα πρωτεύοντα κοινωνικά προβλήματα που αντιμετωπίζουν τα ηλεκτρονικά μέσα σήμερα. Πολλές προσπάθειες έχουν γίνει για να αμβλυνθεί το πρόβλημα: τεχνικά μέσα, φιλτράρισμα των ηλεκτρονικών μηνυμάτων, αυτοματοποιημένη ακύρωση των Netnews spams, νόμοι όπως ο Can Spam Act 2003 και μέτρα της αγοράς όπως μποϊκοτάζ σε εκείνους που χρησιμοποιούν ή υποστηρίζουν τα spam.

2.1.5.Το SPAM στην καθημερινή ηλεκτρονική αλληλογραφία

Το Spam πλημμυρίζει το Διαδίκτυο και κατ’ επέκταση το κουτί μηνυμάτων μας με πολλά αντίγραφα του ίδιου μηνύματος, σε μια προσπάθεια να αναγκάσει τη λήψη ενός μηνύματος στους παραλήπτες, που σε καμία περίπτωση δεν θα επέλεγαν να το λάβουν. Η περισσότερη Spam αλληλογραφία είναι εμπορική διαφήμιση, συχνά για αμφίβολα προϊόντα. Το Spam κοστίζει στον αποστολέα πολύ λίγα, μιας και οι περισσότερες από τις δαπάνες για την αποστολή ενός τέτοιου μηνύματος πληρώνονται από τον παραλήπτη ή τους πάροχους Internet (ISPs).



Εικ. Ένας λογαριασμός ηλεκτρονικού ταχυδρομείου γεμάτος από Spam.

2.1.6 Γιατί το SPAM είναι τόσο μεγάλο πρόβλημα.

- **Κόστος:** Η αποστολή μαζικών ηλεκτρονικών μηνυμάτων είναι απίστευτα φτηνή. Παρ' αυτά όμως, κάθε άτομο που λαμβάνει το spam πρέπει να μπορεί να

πληρώσει το κόστος του. Και το κόστος για τους παραλήπτες είναι πολύ μεγαλύτερο από το κόστος του αποστολέα.

- **Απάτη:** Οι spammers γνωρίζουν μετά από πολλές έρευνες, ότι η πλειοψηφία (που συχνά φτάνει το 95%) των παραληπτών δεν θέλουν να λαμβάνουν τα μηνύματά τους. Ως αποτέλεσμα, πολλοί junk emailers χρησιμοποιούν τεχνικές για να σε κάνουν να ανοίξεις τα μηνύματά τους. Για παράδειγμα, κάνουν το θέμα του μηνύματος να μοιάζει σαν να είναι οτιδήποτε άλλο παρά διαφήμιση.
- **Απώλεια άλλων πόρων:** Όταν οι spammers στέλνουν ένα ηλεκτρονικό μήνυμα σε εκατομμύρια ανθρώπους, αυτό μεταφέρεται από άλλα συστήματα που βρίσκονται καθ' οδόν προς τον προορισμό τους, μετακινώντας το για άλλη μια φορά μακριά απ' την πηγή του. Οι μεταφορείς ανάμεσά τους ξαφνικά κουβαλούν τεράστιο φορτίο διαφημίσεων για τον spammer. Ο αριθμός των spam που στέλνονται κάθε μέρα είναι πραγματικά απεριόριστος και κάθε ένα ξεχωριστά πρέπει να διαχειρίζεται από άλλα συστήματα.
- **Εκτόπισμα του κανονικού ηλεκτρονικού μηνύματος:** Το ηλεκτρονικό μήνυμα γίνεται όλο ένα και περισσότερο, σημαντικό εργασιακό εργαλείο. Στα τέλη του 1980, αφού όλο και περισσότερες επιχειρήσεις άρχισαν να χρησιμοποιούν μηχανήματα fax, οι πωλητές αποφάσισαν ότι μπορούσαν στείλουν με fax τις διαφημίσεις τους στο κοινό.
- **Ενοχλητικός παράγοντας:** Η διεύθυνση του ηλεκτρονικού μηνύματος δεν είναι δημόσιος χώρος. Είναι προσωπική, πληρώνεται κάποιο χρηματικό ποσό και θα πρέπει να υπάρχει ο πλήρης έλεγχος για οτιδήποτε χρησιμοποιείται, από τον νόμιμο κάτοχο. Εάν επιθυμούμε να λαμβάνουμε τόνους ανεπιθύμητων διαφημίσεων, θα πρέπει να μπορούμε. Αλλά δεν θα πρέπει να αναγκαζόμαστε να υποφέρουμε αυτή τη πληθώρα μηνυμάτων εκτός και μέχρι εμείς πραγματικά να το ζητήσουμε.

- **Ηθικολογία:** Το spam είναι βασισμένο στην κλοπή υπηρεσίας, στην απάτη και παραπλάνηση όπως συμβαίνει με τη μετακίνηση κόστους προς τον παραλήπτη. Η μεγάλη υπερίσχυση των προϊόντων και των υπηρεσιών που πωλούνται από την UCE είναι αμφίβολης νομιμότητας. Κάθε επιχείρηση που εξαρτάται από το κλέψιμο των πελατών της, που στήνει ενέδρες στον αθώο και υβρίζει τα γνωστά πρότυπα του Internet είναι - και θα πρέπει να είναι - καταδικασμένη στην αποτυχία..

ΠΙΝΑΚΕΣ

Πίνακας 1

1) Θα λέγατε ότι το spamming είναι πολύ ενοχλητικό, κάπως ενοχλητικό, όχι πολύ ενοχλητικό ή καθόλου ενοχλητικό;

		Ενοχλητικό	Πολύ ενοχλητικό	Κάπως ενοχλητικό	Όχι ενοχλητικό	Όχι πολύ ενοχλητικό	Καθόλου ενοχλητικό
Το spamming ή το να λαμβάνεις ανεπιθύμητα μηνύματα από αγνώστους	%	96	80	16	4	3	1
Πληροφορίες που παίρνεις απ'το Web που δεν είναι ακριβείς ή αξιόπιστες	%	72	32	40	29	21	6
Πόση ώρα πρέπει να περιμένεις μέχρι να εμφανιστούν οι πληροφορίες που θες στην οθόνη σου	%	52	17	35	48	30	18

Πόση ώρα σου παίρνει να βρεις τα websites που ψάχνεις ή χρειάζεσαι	%	43	10	33	57	39	18
Φορές που χρειάζεσαι βοήθεια από κάποιον εκτός σπιτιού για να φτιάξει το σύστημα να δουλέψει κατάλληλα	%	50	21	30	50	27	22

Πίνακας 2

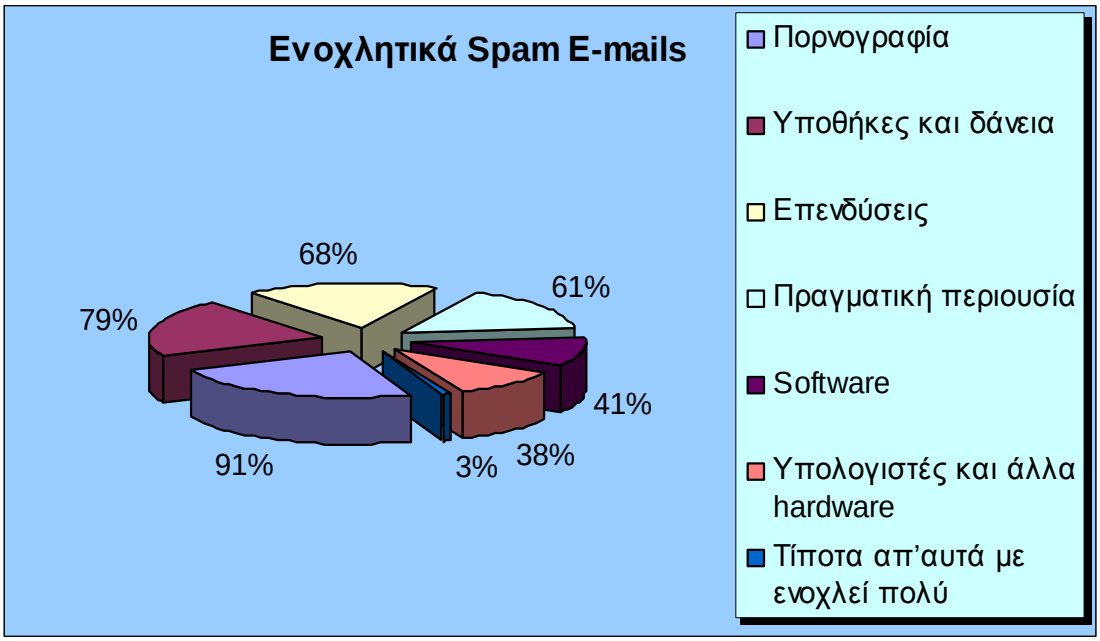
2) Αλλαγές στο τι είναι πολύ ενοχλητικό 2000-2002

	2000	2002
	%	%
Spam - το να παίρνεις	49	80

ανεπιθύμητα μηνύματα από αγνώστους		
Πληροφορίες που παίρνεις από το web που δεν είναι ακριβείς ή αξιόπιστες	35	32
Φορές που χρειάστηκες βοήθεια από κάποιον εκτός σπιτιού για να φτιάξει το σύστημα του υπολογιστή να δουλέψει κατάλληλα	18	21
Πόση ώρα πρέπει να περιμένεις τις πληροφορίες που θες να εμφανιστούν στην οθόνη σου	25	17
Πόσο περιμένεις για να βρεις τα websites που ψάχνεις ή χρειάζεσαι	20	10

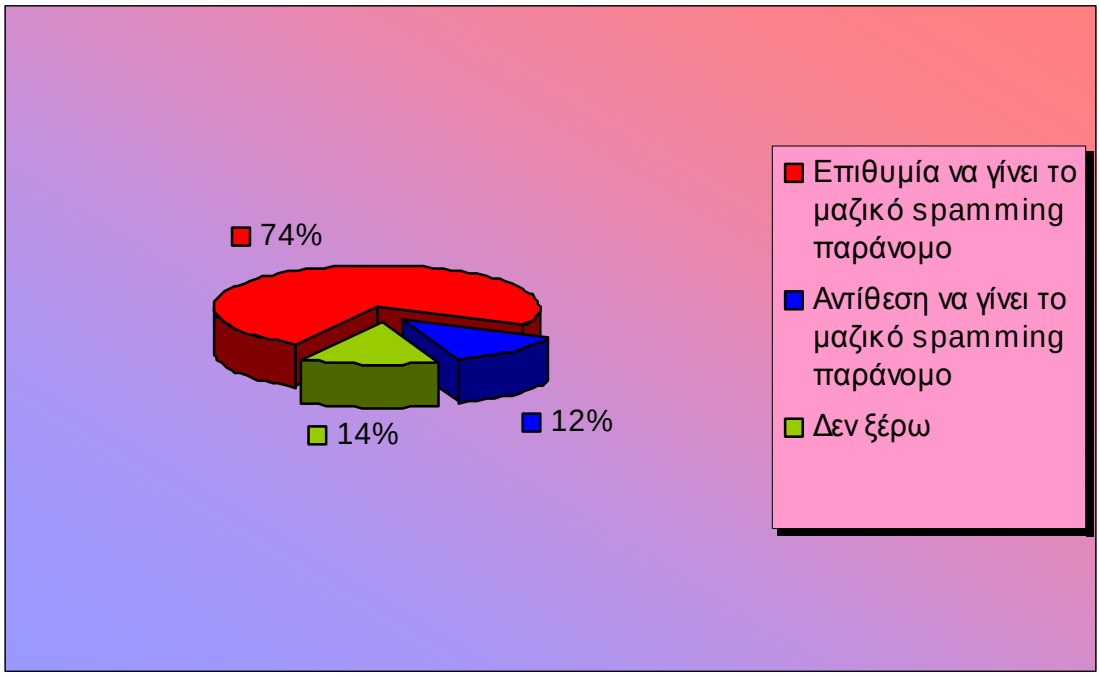
Πίνακας 3

3) Ποιο, εάν κάποιο, απ΄ τα παρακάτω spam emails σας ενοχλεί περισσότερο, αυτά που πουλάνε…;



Πίνακας 4

4) Θα επιθυμούσατε έναν νόμο που θα καθιστούσε το μαζικό spamming παράνομο ή θα ήσασταν αντίθετοι σε αυτόν;



Σημείωση: Οι πίνακες προέρχονται από στατιστική έρευνα που έχει γίνει μέσω του Internet.

Σημείωση: Μεταξύ του 70% και 80% όλων των ηλικιών, ομάδων εισοδήματος, και των δύο φύλων, λευκών και έγχρωμων, Δημοκρατών και Ρεπουμπλικάνων επιθυμούν να τιμωρείται το μαζικό spamming στην Η.Π.Α. Τα στοιχεία αυτά αφορούν τις Η.Π.Α μόνο και έχουν προέλθει μέσα από την ανάλογη έρευνα.

2.1.7 Άλλες μορφές ηλεκτρονικών διαφημιστικών απορριμμάτων

- **Spamdexing:** Το Spamdexing (ένας συνδυασμός spamming και indexing) αναφέρεται στην πρακτική στο World Wide Web των HTML σελίδων για να αυξήσει την πιθανότητα να τοποθετηθούν ψηλά στις σχετικές λίστες των μηχανών αναζήτησης. Οι άνθρωποι που το κάνουν αυτό λέγονται search engine spammers.

- **Blog spam:** Στο Blog spam οι στόχοι είναι τα weblogs. Τοποθετεί σχόλια σε διάφορα blog posts που δεν παρέχουν τίποτα περισσότερο από μια σύνδεση με το διαφημιστικό website του spammer.
- **Wiki spam:** Τα Wikis είναι επίσης ένας στόχος των search engine spam, αρκετά όμοια με το blog spam
- **Junk mail:** Οι πιο γνωστοί τύποι junk mail:
  - Chain letters
  - Pyramids schemes (πυραμοειδή σχήματα, επιχειρήσεις πυραμίδες)
  - Άλλα "Get Rich Quick" ή "Make Money Fast" σχήματα
  - Προσφορές τηλεφωνικών γραμμών σεξ και διαφημίσεις πορνογραφικών websites
  - Προσφορές λογισμικού για συλλογή ηλεκτρονικών διευθύνσεων και αποστολής UCE
  - Προσφορές υπηρεσιών αποστολής μεγάλου όγκου ηλεκτρονικών μηνυμάτων για αποστολή στο UCE
  - Συνεισφορές για ίδρυση άγνωστων σωματείων
  - Γρήγορες θεραπείες και υγιεινά προϊόντα
  - Παράνομα πειρατικά software

2.2 Λόγοι αποστολής ανεπιθύμητων μαζικών μηνυμάτων

Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση των προϊόντων ή των υπηρεσιών τους. Συχνά, αυτά τα ηλεκτρονικά μηνύματα περιλαμβάνουν προτάσεις για πυραμοειδή – προγράμματα, προσφορές για γραμμές τηλεφωνικού ή δικτυακού σεξ, προσκλήσεις σε δικτυακό τζόγο και

άλλα που προκαλούν σύγχυση, είναι πολλές φορές προσβλητικά και κοστίζουν ακριβά για να τα «κατεβάσει» κανείς, να τα διαβάσει και να τα διαγράψει.

2.2.1 Πλεονεκτήματα του ηλεκτρονικού μηνύματος σαν εμπορικού μέσου επικοινωνίας

Εκτός από τις εταιρείες παροχής υπηρεσιών Internet, οι οποίες παρέχουν υπηρεσία ηλεκτρονικού ταχυδρομείου με την έναρξη της συνδρομής, υπάρχουν διάφορες εταιρείες που προσφέρουν δωρεάν ηλεκτρονική αλληλογραφία μέσω Διαδικτύου (υπηρεσιών web). Οι εταιρείες αυτές επιτρέπουν να στέλνονται και να λαμβάνονται ηλεκτρονικό ταχυδρομείο, χρησιμοποιώντας απλώς το πρόγραμμα περιήγησης, χωρίς να απαιτείται η χρήση ειδικού προγράμματος ταχυδρομείου. Επισκέπτεται κανείς την ιστοσελίδα της εταιρείας και ακολουθώντας δεσμούς (επιλογές), στέλνονται και λαμβάνονται μηνύματα. Αφού ένας φυλλομετρητής όπως ο Internet Explorer, για παράδειγμα, δεν έχει σχεδιαστεί για να χειρίζεται ηλεκτρονικό ταχυδρομείο, όλη τη διαδικασία αναλαμβάνει ο διακομιστής που βρίσκεται πίσω από την εταιρεία. Αυτό που κάνει ο διακομιστής είναι να εμφανίζει πληροφορίες και να επιτρέπει να γίνονται επιλογές. Εμφανίζει, για παράδειγμα, ένα μενού με επιλογές όπως αποστολή μηνύματος, λήψη, έλεγχο για νέα μηνύματα κ.λ.π. Χρησιμοποιώντας τον φυλλομετρητή όπως θα γινόταν σε μια κοινή ιστοσελίδα, γίνεται κλικ στην επιθυμητή επιλογή. Ακολουθούν τα μενού ή τις επιλογές στη νέα σελίδα που θα εμφανιστούν, και συνεχίζεται κατ’ αυτό τον τρόπο μέχρι να ολοκληρωθεί η διαδικασία.

Πλεονεκτήματα

Είναι πολλά τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζει αυτό το σύστημα ηλεκτρονικής αλληλογραφίας. Τα βασικότερα πλεονεκτήματα είναι ότι παρέχουν τη δυνατότητα ηλεκτρονικής αλληλογραφίας δωρεάν (με το αντίτιμο ίσως των πολλών διαφημίσεων που εμφανίζονται) και δεν απαιτούν ειδικό πρόγραμμα ταχυδρομείου. Ιδιαίτερα το γεγονός ότι με τη χρήση ενός απλού browser μπορεί να στέλνει και να λαμβάνει μηνύματα, απαλλάσσει από πολλά προβλήματα και ρυθμίσεις. Το μόνο που χρειάζεται είναι ένας υπολογιστής με πρόσβαση στο Internet. Από οποιοδήποτε μέρος του κόσμου και με έναν άλλο υπολογιστή ή ενός Internet Cafe, μπορεί να στέλνει και να λαμβάνετε μηνύματα κάποιος. Αν αντίθετα, διατηρείτο λογαριασμός ταχυδρομείου με συνδρομή σε κάποιον ISP, θα έπρεπε να διαθέτει και πρόγραμμα ταχυδρομείου, αλλά και να το ρυθμιστεί για να λαμβάνει τα μηνύματα από τη διεύθυνσή (κάτι ιδιαίτερα δύσκολο όταν υπάρχει συνεχής μετακίνηση ή διαμονή στο εξωτερικό).

Ένα ακόμα μεγάλο πλεονέκτημα αυτών των υπηρεσιών είναι η ανωνυμία που προσφέρουν. Πρόκειται για ένα ιδιαίτερα βολικό χαρακτηριστικό, όταν, για παράδειγμα, η μόνη πρόσβαση που υπάρχει στο Διαδίκτυο είναι από το γραφείο και δεν χρησιμοποιείτε η διεύθυνση του ηλεκτρονικού ταχυδρομείου της εργασίας για την προσωπική αλληλογραφία. Οι περισσότερες βέβαια εταιρείες που προσφέρουν τέτοιες υπηρεσίες, υποχρεώνουν τη συμπλήρωση στοιχείων όπως το ονοματεπώνυμό, τη διεύθυνσή, τη χώρα κλπ. Δεν είναι όμως υποχρεωμένοι να δηλώνουν τα ακριβή στοιχεία, αφού δεν υπάρχει και τρόπος να ελεγχθούν ή να επιβεβαιωθούν. Προσοχή πρέπει γιατί το όνομα που θα δηλωθεί θα φαίνεται σε όλα τα μηνύματα που στέλνονται. Όταν γράφεται κανείς σε αυτές τις υπηρεσίες, δηλώνει όποιο όνομα (αρκεί να μην το χρησιμοποιεί άλλος χρήστης) και κωδικό πρόσβασης θέλει.

2.3 Πως δρουν οι SPAMMERS;

Μπορεί να είδαμε τις «βλαβερές» συνέπειες του spamming τόσο σε επίπεδο χρηστών όσο και σε επίπεδο εταιρειών αλλά σίγουρα δεν αναφέρθηκε στο πώς οι spammers βοηθιούνται από την τεχνολογία για να επιτύχουν τους στόχους τους. Εύκολα μπορεί να αναλογιστεί κανείς πως για να μπορέσει ένας spammer να στείλει ένα τόσο μεγάλο όγκο ηλεκτρονικών μηνυμάτων θα πρέπει η ίδια η τεχνολογία του internet και του ηλεκτρονικού μηνύματος να του το επιτρέπει.

Πράγματι, όπως προκύπτει από διάφορες μελέτες ο αρωγός των spammers στη προσπάθειά τους να διανείμουν όλο αυτό το spamming είναι κυρίως η τεχνολογία που χρησιμοποιείται για την μεταφορά των ηλεκτρονικών μηνυμάτων. Ειδικότερα τώρα, το Simple Mail Transfer Protocol, που είναι το κύριο πρωτόκολλο του Internet για τη μεταφορά και λήψη ηλεκτρονικού μηνύματος, επιτρέπει σε ένα ηλεκτρονικό μήνυμα να αποσταλεί σε ένα αόριστο-«άπειρο» αριθμό παραληπτών. Παράλληλα το πρωτόκολλο δεν απαιτεί μια έγκυρη διεύθυνση προκειμένου να αυθεντικοποιήσει τον χρήστη-αποστολέα, αυτό σημαίνει πως αν ένας spammer δεν φοβάται μήπως αναγνωριστεί, αφού κατοικεί σε μια χώρα όπου δεν υπάρχει νομική κάλυψη για τέτοιου είδους θέματα, μπορεί απλά να χρησιμοποιήσει τον e-mail server του provider του προκειμένου να στείλει τα spam ηλεκτρονικά μηνύματά του.

Έτσι λοιπόν λόγω της απουσία της αυθεντικοποίησης κατά τη χρήση του SMTP, ο spammer μπορεί να στείλει τα spam ηλεκτρονικά μηνύματά του σε μια τρίτη μερίδα e-mail server(ένα ανοιχτό SMTP-Relay) χωρίς φυσικά να γνωρίζει τίποτε ο provider του e-mail server. Αναλογιζόμενοι τα παραπάνω ορισμένοι Internet Service Providers(ISPs) θέλοντας να προστατεύσουν κατά κάποιο τρόπο τους servers τους από την κακομεταχείρισή τους από τους spammers άρχισαν να

χρησιμοποιούν ένα καινούργιο πρωτόκολλο που καλείται “SMTP-Auth”. Με το SMTP-Auth ο αποστολέας πρέπει να αυθεντικοποιήσει τον εαυτό του με ένα password στον Mail Transfer Agent(MTA) που δεν είναι τίποτε άλλο από ένα λογισμικό που υπάρχει στον e-mail server. Θα πρέπει να τονιστεί σε αυτό το σημείο πως το προαναφερθέν πρωτόκολλο δεν αποτρέπει το spamming αλλά κάνει ευκολότερη την αναγνώριση του spammer (με τη βοήθεια εννοείται του ISP).

Παρόλα αυτά είναι πολύ εύκολο για τους αποστολείς μηνυμάτων να στέλνουν spam με ανώνυμο τρόπο σε ένα ακαθόριστο αριθμό από αποδέκτες. Ανακεφαλαιώνοντας λοιπόν τα παραπάνω αντιλαμβάνεστε πως το spam «ταξιδεύει» μέσα στο internet χρησιμοποιώντας Simple Mail Transfer Protocol (SMTP). Αυτό το πρωτόκολλο δουλεύει καλά για να σταλεί ένα ηλεκτρονικό μήνυμα, όμως η φυσική αδυναμία του πρωτοκόλλου αυτού έγκειται στην έλλειψη μηχανισμών αυθεντικοποίησης που θα «λάμβαναν υπ’ όψιν τους» την εμφάνιση μηνυμάτων τα οποία δεν είχαν «ζητηθεί». Έτσι είναι πολύ εύκολο για τον οποιοδήποτε να στείλει ένα υπερβολικά μεγάλο όγκο δεδομένων-μηνυμάτων σε όποια διεύθυνση επιθυμεί χωρίς να φοβάται μήπως γίνει εύκολα αντιληπτός.

Μέχρις στιγμής λοιπόν είδαμε πως οι spammers καταφέρνουν να διοχετεύσουν τα ηλεκτρονικά μηνύματά τους στο διαδίκτυο και αυτά να φτάσουν στον προορισμό τους. Το μεγάλο ερώτημα που γεννάται είναι ποιος είναι ο προορισμός των ηλεκτρονικών μηνυμάτων spam και πως τον βρίσκουν οι spammers. Με άλλα λόγια, ένα ενδιαφέρον ζήτημα είναι το πώς οι spammers καταφέρνουν να βρουν τις διευθύνσεις των «θυμάτων» χωρίς αυτοί να γίνουν αντιληπτοί. Όπως είναι γνωστό οι spammers είναι άτομα ή ομάδες ατόμων ή εταιρείες που σκοπό έχουν να παρουσιάσουν το ηλεκτρονικό μήνυμα τους μπροστά μας.

2.3.1 Από που παίρνουν τις διευθύνσεις

Σύμφωνα λοιπόν με μελέτες και έρευνες που κατά καιρούς έχουν γίνει, έχει διαπιστωθεί ότι οι spammers βρίσκουν τις διευθύνσεις με τους εξής τρόπους:

- Συνήθως οι spammers εκμεταλλεύονται το γεγονός ότι πολλοί χρήστες «δημοσιοποιούν» τις ηλεκτρονικές διευθύνσεις τους όταν επισκέπτονται μια ιστοσελίδα ή μια ομάδα συζητήσεων στο Internet. Έτσι οι spammers βρίσκουν πρόσφορο έδαφος και συλλέγουν τις διευθύνσεις που τους χρειάζονται. Αυτή είναι η πιο ευρέως διαδεδομένη μέθοδος και ονομάζεται «σόδιασμα» (“Harvesting”). Είναι αντιληπτό ότι κάποιος που επισκέπτεται μια ιστοσελίδα ή μια ομάδα συζητήσεων(newsgroup) στο internet αναζητά κάποια πληροφορία ή κάποια ενημέρωση αντίστοιχα. Για το λόγο αυτό άλλωστε «δέχεται» να διαθέσει και την ηλεκτρονική διεύθυνσή του. Όμως όπως οι περισσότερες έρευνες έχουν δείξει, μια τέτοια ενέργεια συχνά καταλήγει στο να γίνονται οι ανωτέρω διευθύνσεις αντικείμενο εκμετάλλευσης από τους spammers.
- Ένας άλλος τρόπος που οι spammers χρησιμοποιούν προκείμενου να εκμαιεύσουν κάποιες ηλεκτρονικές διευθύνσεις είναι να αγοράζουν κάποιο έτοιμο cd που να τις περιέχει. Φυσικά όμως κάτι τέτοιο περιέχει αρκετό ρίσκο για τους ίδιους τους spammers αφού οι διευθύνσεις που περιέχει το cd μπορεί να είναι «απαρχαιωμένες» και να μην χρησιμοποιούνται πια. Ακόμα μπορεί ούτε καν να υπάρχουν. Άλλώστε όπως πολύ σωστά λέει και ο σοφός λαός «πόση ειλικρίνεια μπορεί να υπάρχει μεταξύ κλεφτών…;!»
- Επιπρόσθετα δεν είναι λίγες οι φορές που οι spammers προσπαθούν να μαντέψουν οι ίδιοι τις διευθύνσεις των εν δυνάμει παραληπτών τους. Παραδείγματος χάριν μια ηλεκτρονική διεύθυνση όπως η ακόλουθη: nick@gmail.com είναι πολύ πιθανό να υπάρχει παρόλο που δεν είναι σε θέση

να γνωρίζουν σε ποιόν αντιστοιχεί. Αν καλοεξεταστεί αυτή η τεχνική που ακολουθούν αρκετοί spammers θα παρατηρηθεί ότι τις περισσότερες φορές την «εστιάζουν» σε κάποιο domain, γι' αυτό άλλωστε και πολλές φορές καλείται: «Dictionary Attack».

- Δυστυχώς το πιο άσχημο στη όλη υπόθεση είναι ότι κάποιες φορές οι ίδιοι οι ISPs πουλάνε τις ηλεκτρονικές διευθύνσεις στους spammers. Αν και κάτι τέτοιο είναι πολύ σπάνιο στις μέρες μας αφού μια τέτοια κίνηση θα οδηγούσε έμμεσα πολλούς χρήστες να εγκαταλείψουν τον συγκεκριμένο ISP αφού θα ήταν δυσαρεστημένοι από τις υπηρεσίες που θα τους προσφέρονταν.
- Όπως αναφέραμε στην αρχή τις περισσότερες φορές οι ίδιοι οι χρήστες είναι που δίνουν τις διευθύνσεις τους στους spammers. Έτσι για την αποφυγή κάτι τέτοιου, θα πρέπει να διαβαστεί προσεκτικά το ιδιωτικό έγγραφο σύμβασης ασφάλειας όταν πρόκειται ή ζητούν να δοθεί η ηλεκτρονική διεύθυνση κατά την περιήγησή σε κάποια ιστοσελίδα. Διότι πολλές φορές τα ηλεκτρονικά μηνύματα που δίνονται χρησιμοποιούνται για σκοπούς άλλους από αυτούς για τους οποίους αρχικά δόθηκαν.
- Ένας άλλος αρκετά δημοφιλής τρόπος για να μπορούν οι spammers να εκμαιεύουν ηλεκτρονικές διευθύνσεις είναι με το να δημιουργούν ένα ή περισσότερα websites τα οποία προσπαθούν να ξεγελάσουν τους επισκέπτες τους και να τους αποκαλύψουν τις ηλεκτρονικές διευθύνσεις τους.
- Παράλληλα μέσα από την ιστοσελίδα που δημιουργούν για κάλυψη οι επίδοξοι spammers, πολλές φορές μοιράζουν διάφορα «ύποπτα» προγράμματα (ιούς ή δούρειους ίππους) τα οποία εγκαθίστανται στα PC των χρηστών και σαρώνουν το δίσκο τους προκειμένου να βρουν ηλεκτρονικές διευθύνσεις.

- Τέλος οι spammers προκειμένου να αποκτήσουν τις πολυπόθητες γι' αυτούς διευθύνσεις, προσπαθούν να «πάρουν στα χέρια τους» τη λίστα με τις διευθύνσεις των αποδεκτών ενός μηνύματος.

Συνοψίζοντας όλα όσα προαναφερθήκαν, επικεντρώνονται στο πιο διαδεδομένο τρόπο με τον οποίο οι spammers εκμαιεύουν τις διευθύνσεις που αναζητούν και που δεν είναι άλλος από το να τις ψάχνουν μόνοι τους.

2.3.2 Εξάπλωση μαζικών μηνυμάτων στο Internet

Το spam κατακλύζει το Internet με πολλά αντίγραφα του ίδιου μηνύματος, σε μια προσπάθεια να επιβάλλει το μήνυμα σε ανθρώπους που ούτως ή άλλως δε θα επέλεγαν να το παραλάβουν. Τα περισσότερα spam αφορούν την εμπορική διαφήμιση, συχνά για αμφιλεγόμενα προϊόντα, για get-rich-quick σχήματα ή για σχεδόν νόμιμες υπηρεσίες. Το spam κοστίζει στον αποστολέα ελάχιστα για να το στείλει - τα περισσότερα έξοδα πληρώνονται από τον παραλήπτη ή τους μεταφορείς παρά απ’ τον αποστολέα.

Υπάρχουν 2 κύριοι τύποι spam και έχουν διαφορετικές επιδράσεις στους χρήστες του Internet. Το Cancellable Usenet spam είναι ένα μονό μήνυμα σταλμένο σε 20 ή περισσότερες Usenet ομάδες συζήτησης. Το Usenet spam στοχεύει στους «ενεδρευτές» (“lurkers”), ανθρώπους που διαβάζουν ομάδες συζήτησης αλλά σπάνια ή ποτέ ταχυδρομούν και δίνουν τις διευθύνσεις τους. Το Usenet spam κλέβει απ’ τους χρήστες τη χρησιμότητα των ομάδων συζήτησης κατακλύζοντας τους με ένα σωρό από διαφημιστικές ή άλλες άσχετες επιστολές. Το ηλεκτρονικό μήνυμα spam στοχεύει ατομικούς χρήστες με απευθείας ηλεκτρονικά μηνύματα. Οι ηλεκτρονικές spam λίστες συχνά δημιουργούνται

σκανάροντας Usenet αφίσες, κλέβοντας ταχυδρομικές λίστες διαδικτύου ή αναζητώντας διευθύνσεις στο Web.

Τα ηλεκτρονικά μηνύματα spams τυπικά κοστίζουν στο χρήστη χρήματα, που δε δίνει, για να τα παραλάβει. Πολλοί άνθρωποι - καθένας με μετρημένη τηλεφωνική υπηρεσία - διαβάζουν ή λαμβάνουν τα μηνύματά τους ενώ ο μετρητής τρέχει. Το spam κοστίζει σ' αυτούς επιπλέον χρήματα. Κοστίζει χρήματα για ISPs και online υπηρεσίες που μεταβιβάζουν spam, και αυτά τα έξοδα μεταβιβάζονται απευθείας στους συνδρομητές. Μια συγκεκριμένα ρυπαρή παραλλαγή του ηλεκτρονικού spam στέλνει spam σε ταχυδρομικές λίστες. Επειδή πολλές ταχυδρομικές λίστες περιορίζουν δραστηριότητα στους συνδρομητές τους, οι spammers χρησιμοποιούν αυτοματοποιημένα εργαλεία για να εγγραφούν σε όσες περισσότερες λίστες είναι δυνατόν, για να μπορούν να αρπάζουν τις λίστες των διευθύνσεων, ή για να χρησιμοποιούν τη ταχυδρομική λίστα ως έναν άμεσο στόχο για τις επιθέσεις τους.

ΚΕΦΑΛΑΙΟ 3ο:ΠΡΟΒΛΗΜΑΤΙΣΜΟΣ ΓΥΡΟ ΑΠΟ ΤΟ SPAM

3.1 Η ζημιά από την οπτική γωνία του ιδιώτη/τελικού χρήστη του ηλεκτρονικού ταχυδρομείου.

Θα πρέπει να αναφερθεί πως το spamming δεν είναι κάτι το ανέξοδο. Αντιθέτως κοστίζει, και μάλιστα πολύ. Με άλλα λόγια μπορεί η διαδικασία λήψης και αποστολής ενός ηλεκτρονικού μηνύματος να φαίνεται ανέξοδη, κανείς όμως δεν εγγυάται τα αποτελέσματα που μπορεί να έχει ένα μήνυμα spam σε ένα χρήστη. Ειδικότερα τώρα, και σύμφωνα με το Internet Fraud Complaint Center, ένα πρόγραμμα επιδοτούμενο από το Federal Bureau of Investigation και από το National White Collar Crime Center, το συνολικό ποσό δολαρίων που χάνονται από απάτες μέσω του ηλεκτρονικού ταχυδρομείου και που έχουν αναφερθεί, έφτασαν το 2001 τα 17,81 εκατομμύρια δολάρια με μέση ζημιά, από κάθε παράπονο που έγινε, της τάξης των 435 δολαρίων. Βέβαια η ζημιά αυτή δεν οφείλεται στο ίδιο το spamming αλλά στο περιεχόμενο που είχαν αυτά τα μηνύματα και που προφανώς δεν είναι αντικείμενο της παρούσης εργασίας.

Παράλληλα στην ίδια έρευνα αναφέρεται ότι η μέση ημερησία κίνηση των ηλεκτρονικών μηνυμάτων φτάνει τα 27 δισεκατομμύρια και από τα οποία περισσότερα από το 44% είναι spam. Έτσι, όπως είναι φυσικό, ένα τόσο μεγάλο ποσοστό ημερησίας κίνησης της ηλεκτρονικής αλληλογραφίας, το οποίο οφείλεται κατά κύριο λόγο στους spammers, έχει σαν αποτέλεσμα πολλές συνέπειες που μεταφράζονται σε κόστος και ενόχληση σε διάφορα επίπεδα.

- Οι αποδέκτες έχουν να αντιμετωπίσουν κόστος «κατεβάσματος», κόστη λόγω έλλειψης αποθηκευτικού χώρου, ενώ πολλοί από αυτούς λόγω έλλειψης αποθηκευτικού χώρου στο λογαριασμό τους δεν μπορούν να λάβουν κάποια ηλεκτρονικά μηνύματα που όντως τους ενδιαφέρουν. Έτσι αναγκάζονται να ξοδεύουν υπερβολικές ώρες με το να διαβάζουν και να διαγράφουν μηνύματα που είναι spam.
- ISP (Internet Service Provider) του παραλήπτη έχει να επωμιστεί το «κόστος» της αποθήκευσης του μηνύματος μέχρι αυτό να διαγραφεί από το server, καθώς και το κόστος της κίνηση των μηνυμάτων ενώ παράλληλα θα πρέπει να ξοδέψει σημαντικό χρόνο στο να χειριστεί τα παράπονα των συνδρομητών του και να αποφύγει την απομάκρυνση τυχών ενοχλημένων πελατών.
- Οι ISPs που είναι επιφορτισμένοι με την μεταφορά των μηνυμάτων μέσα από το δίκτυο είναι υποχρεωμένοι να επωμιστούν τα ανάλογα έξοδα.
- Η κοινότητα των χρηστών είναι ενοχλημένη καθώς έχει να αντιμετωπίσει αρκετές «ζημιές» ενώ η αποδοτικότητα και η ταχύτητα του internet απειλείται.

Στο σημείο αυτό, θα πρέπει να αναφερθεί πως πολλοί servers κρασσάρουν λόγω των ηλεκτρονικών μηνυμάτων spam. Ειδικότερα τόσο οι servers από τους οποίους στέλνονται τα spam μηνύματα όσο και οι servers από τους οποίους περνάνε τα μηνύματα αυτά μπορεί να αντιμετωπίσουν πρόβλημα κρασσαρίσματος. Αυτό αποδίδεται τόσο στις ποσότητες των μηνυμάτων που στέλνονται και μεταφέρονται καθώς επίσης και στα μηνύματα που επιστρέφονται σε αυτούς αφού στάλθηκαν σε ανύπαρκτους αποδέκτες.

Όμως παρόλα αυτά το μεγαλύτερο πρόβλημα παραμένει η ενόχληση των χρηστών, που ναι μεν μπορεί να μην είναι και τόσο εξεζητημένο θέμα σε επίπεδο

χρηστών, αλλά σίγουρα προβληματίζει έντονα τις αντίστοιχες εταιρείες που βλέπουν να χάνουν την αξιοπιστία των πελατών τους.

Τέλος οι ISPs λόγω του μεγάλου όγκου των δεδομένων που μετακινούνται αναγκάζονται να δαπανούν μεγάλα ποσά για να αγοράζουν υπερβολικό εύρος ζώνης(bandwidth), να προσφέρουν 24ωρη υποστήριξη καθώς και επιπλέον αποθηκευτικό χώρο ως δείγμα προληπτικής πολιτικής. Φυσικό επακόλουθο είναι κάποιος να αναρωτηθεί αν τα χρήματα που δαπανώνται για όλες αυτές τις προαναφερθείσες υπηρεσίες είναι περισσότερα από το κόστος που υπάρχει αν κάποιος server δυσλειτουργεί. Κι όμως!!! Ενδεικτικά αναφέρουμε πως κάποια στιγμή σε μια ορισμένη περιοχή στις Ηνωμένες Πολιτείες της Αμερικής το spam επηρέασε τόσο πολύ τον server που τα μηνύματα που ήταν να μεταφερθούν(στον προορισμό τους) σε διάστημα ενός λεπτού χρειάστηκαν τρεις μέρες. Αναλογίζεστε λοιπόν πόσο τεράστιο ήταν το κόστος της επαναληπτικής αυτής διαδικασίας. Ανακεφαλαιώνοντας λοιπόν όλα τα παραπάνω μπορούμε να πούμε πως το spamming είναι πράγματι επιζήμιο, και μάλιστα όχι μόνο όσο αναφορά τους χρήστες αλλά και τις ίδιες τις εταιρίες που προσφέρουν τις υπηρεσίες τους στους συνδρομητές αφού υποχρεώνονται σε μεγάλα έξοδα προκειμένου να διασφαλίσουν την ποιότητα των υπηρεσιών τους.

3.2 Κόστος και προβλήματα των επιχειρήσεων

Ο λόγος για τον οποίο η Ευρωπαϊκή Ένωση, οι ΗΠΑ και μεμονωμένες ευρωπαϊκές χώρες έχουν αρχίσει να ευαισθητοποιούνται απέναντι στο πρόβλημα της ανεπιθύμητης διαφημιστικής αλληλογραφίας είναι απλό: χάνεται χρήμα.

Το 2001 η διακίνηση Spam μηνυμάτων αντιστοιχούσε στο 8% του συνόλου της ηλεκτρονικής αλληλογραφίας μέσω Internet. Το αντίστοιχο ποσοστό του 2002 έφθασε το 40%! Η απώλεια παραγωγικότητας των επιχειρήσεων της Ε.Ε υπολογίζεται σε 2,5 δις ευρώ για το 2002 (περισσότερα από 10δις ευρώ συνυπολογίζοντας και το κόστος στους ιδιώτες). Ειδικά για τις ΜΜΕ, οι οποίες συχνά αμελούν να επενδύσουν σε ειδικά συστήματα φιλτραρίσματος αλληλογραφίας και εξακολουθούν να δέχονται ανεξέλεγκτα μεγάλες ποσότητες Spam μηνυμάτων, το κόστος υπολογίζεται μεγάλο (χωρίς προς το παρόν να υπάρχουν συγκεκριμένα στοιχεία).

Πρόσφατη έρευνα της αμερικανικής Ferris Research επιβεβαιώνει την απώλεια 2,5δις ευρώ στις επιχειρήσεις της Ε.Ε αλλά δίνει και επιπλέον στοιχεία: περίπου 8,9δις δολάρια απώλειες για τις αμερικανικές επιχειρήσεις, και από περίπου 500 εκατ. δολάρια για εταιρείες παροχής υπηρεσιών Internet και στις δυο πλευρές του Ατλαντικού. Τα ποσά αυτά αντιστοιχούν κυρίως σε χαμένο χρόνο. Στην έρευνα της Ferris υπολογίζεται ότι, μολονότι συνήθως τα αυτόκλητα μηνύματα διαγράφονται από τον εργαζόμενο σε μια επιχείρηση μέσα σε λίγα δευτερόλεπτα, πολλοί υπάλληλοι ρίχνουν μια γρήγορη έστω ματιά σε κάποια από αυτά. Ο περισσότερος χαμένος χρόνος υπολογίζεται ότι αφιερώνεται στο διαχωρισμό των χρήσιμων μηνυμάτων από τα άχρηστα και στη εξακρίβωση των πραγματικά άχρηστων: δεν είναι σπάνιο το φαινόμενο να χαρακτηρίζεται ως Spam ένα χρήσιμο μήνυμα, λόγω σφάλματος στο φιλτράρισμα της αλληλογραφίας από το σύστημα.

Ακόμη πιο πρόσφατη έρευνα (Ιούνιος-Ιούλιος 2003) της αμερικανικής Nucleus Research δείχνει ότι τα μηνύματα Spam κοστίζουν στις επιχειρήσεις των ΗΠΑ 874 δολάρια ετησίως ανά εργαζόμενο, κάτι που αντιστοιχεί σε μείωση της παραγωγικότητας κατά 1,4% σε ετήσια βάση. Το ποσό των 874 δολαρίων βασίζεται σε ωριαίες απολαβές 30 δολαρίων σε μια χρονιά 2080 ωρών. Στην

έρευνα της Nucleus καταδεικνύεται ότι ο μέσος εργαζόμενος λαμβάνει 13,3 προσωπικά μηνύματα την ημέρα. Οι εργαζόμενοι αφιερώνουν 6,5 λεπτά την ημέρα, ελέγχοντας, διαγράφοντας ή διαβάζοντας spam μηνύματα.
Τέλος, η επίσης αμερικανική Network Associates δημοσίευσε έρευνά της, που διεξήχθη on-line με 1500 συμμετέχοντες, και έδειξε ότι οι εργαζόμενοι σπαταλούν περίπου 40 λεπτά την εβδομάδα ασχολούμενοι με μηνύματα spam.

3.3 Κόστος και προβλήματα για τους ISPs

Ο ISP (internet Service Provider) του παραλήπτη έχει να επωμιστεί το «κόστος» της αποθήκευσης του μηνύματος μέχρι αυτό να διαγραφεί από το server, καθώς και το κόστος διακίνησης των μηνυμάτων ενώ παράλληλα θα πρέπει να ξοδέψει σημαντικό χρόνο στο να χειριστεί τα παράπονα των συνδρομητών του και να αποφύγει την απομάκρυνση τυχών ενοχλημένων πελατών,

Οι ISPs του είναι επιφορτισμένοι με την μεταφορά των μηνυμάτων μέσα από το δίκτυο και είναί υποχρεωμένοι να επωμιστούν τα ανάλογα έξοδα.

Δυστυχώς το πιο άσχημο στη όλη υπόθεση είναι ότι κάποιες φορές οι ίδιοι οι ISPs πουλάνε τις ηλεκτρονικές διευθύνσεις στους spammers. Αν και κάτι τέτοιο είναι πολύ σπάνιο στις μέρες μας, αφού μια τέτοια κίνηση θα οδηγούσε έμμεσα πολλούς χρήστες να εγκαταλείψουν τον συγκεκριμένο ISP αφού θα ήταν δυσαρεστημένοι από τις υπηρεσίες που θα τους προσφέρονταν.

Όπως αναφέρθηκε στην αρχή τις περισσότερες φορές οι ίδιοι οι χρήστες είναι που δίνουν τις διευθύνσεις τους στους spammers. Έτσι για την αποφευχθεί κάτι τέτοιο θα πρέπει να διαβαστεί προσεκτικά το ιδιωτικό έγγραφο σύμβασης ασφάλειας όταν πρόκειται ή ζητηθεί να δοθεί η ηλεκτρονική διεύθυνση κατά την περιήγηση σε κάποια ιστοσελίδα. Διότι πολλές φορές τα μηνύματα που δίνονται

χρησιμοποιούνται για σκοπούς άλλους από αυτούς για τους οποίους αρχικά δόθηκαν.

Ένας άλλος αρκετά δημοφιλής τρόπος για να μπορούν οι spammers να εκμαιεύουν ηλεκτρονικές διευθύνσεις είναι με το να δημιουργούν ένα ή περισσότερα websites τα οποία προσπαθούν να ξεγελάσουν τους επισκέπτες τους και αποκαλύπτουν τις ηλεκτρονικές διευθύνσεις τους. Παράλληλα μέσα από τις ιστοσελίδες που δημιουργούν για κάλυψη οι επίδοξοι spammers, πολλές φορές μοιράζουν διάφορα «ύποπτα» προγράμματα (ιούς ή δούρειους ίππους) τα οποία εγκαθίστανται στα PC των χρηστών και σαρώνουν το δίσκο τους προκειμένου να βρουν ηλεκτρονικές διευθύνσεις.

Τέλος οι spammers προκειμένου να αποκτήσουν τις πολυπόθητες γι' αυτούς διευθύνσεις, προσπαθούν να «πάρουν στα χέρια τους» τη λίστα με τις διευθύνσεις των αποδεκτών ενός μηνύματος.

Συνοψίζοντας όλα όσα προαναφέραμε, επικεντρωνόμαστε στο πιο διαδεδομένο τρόπο με τον οποίο οι spammers εκμαιεύουν τις διευθύνσεις που αναζητούν και που δεν είναι άλλος από το να τις ψάχνουν μόνοι τους. Όμως παρόλα αυτά το μεγαλύτερο πρόβλημα παραμένει η ενόχληση των χρηστών, που ναι μεν μπορεί να μην είναι και τόσο εξεζητημένο θέμα σε επίπεδο χρηστών, αλλά σίγουρα προβληματίζει έντονα τις αντίστοιχες εταιρείες που βλέπουν να χάνουν την αξιοπιστία των «πελατών» τους. Τέλος οι ISPs λόγω του μεγάλου όγκου των δεδομένων που μετακινούνται αναγκάζονται να δαπανούν μεγάλα ποσά για να αγοράζουν υπερβολικό εύρος ζώνης. Επιπρόσθετα, θα πρέπει να αναφερθεί πως το spamming δεν είναι κάτι το ανέξοδο. Αντιθέτως κοστίζει και μάλιστα πολύ. Με άλλα λόγια μπορεί η διαδικασία λήψης και αποστολής ενός ηλεκτρονικού μηνύματος να είναι ανέξοδη, κανείς όμως δεν εγγυάται τα αποτελέσματα που μπορεί να έχει ένα spam μήνυμα σε ένα χρήστη. Ειδικότερα τώρα σύμφωνα με το internet Fraud Complaint Center, ένα πρόγραμμα επιδοτούμενο από το Federal

Bureau of Investigation και από το National White Collar Crime Center, το συνολικό ποσό δολαρίων που χάνονται από απάτες μέσω ηλεκτρονικών μηνυμάτων και που έχουν αναφερθεί έφτασαν το 2001 τα 17,81 εκατομμύρια δολάρια με ένα μέσο χάσιμο, από κάθε παράπονο που έγινε, της τάξης των 435 δολαρίων. Βέβαια το χάσιμο αυτών των χρημάτων δεν έγκειται στο ίδιο το spamming αλλά στο περιεχόμενο που είχαν αυτά τα μηνύματα και που προφανώς δεν είναι αντικείμενο της παρούσης εργασίας. Παράλληλα στην ίδια έρευνα αναφέρεται ότι η μέση ημερησία κίνηση των ηλεκτρονικών μηνυμάτων φτάνει τα 27 δισεκατομμύρια και από τα οποία πάνω από το 44% είναι spam. Έτσι όπως είναι φυσικό, ένα τόσο μεγάλο ποσοστό ημερησίας κίνησης των ηλεκτρονικών μηνυμάτων, το οποίο οφείλεται κατά κύριο λόγο στους spammers, έχει σαν αποτέλεσμα πολλές συνέπειες που μεταφράζονται σε κόστος και ενόχληση σε διαφορετικά επίπεδα.

ΚΕΦΑΛΑΙΟ 4ο :ΛΗΨΗ ΤΕΧΝΙΚΩΝ ΜΕΤΡΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ SPAM

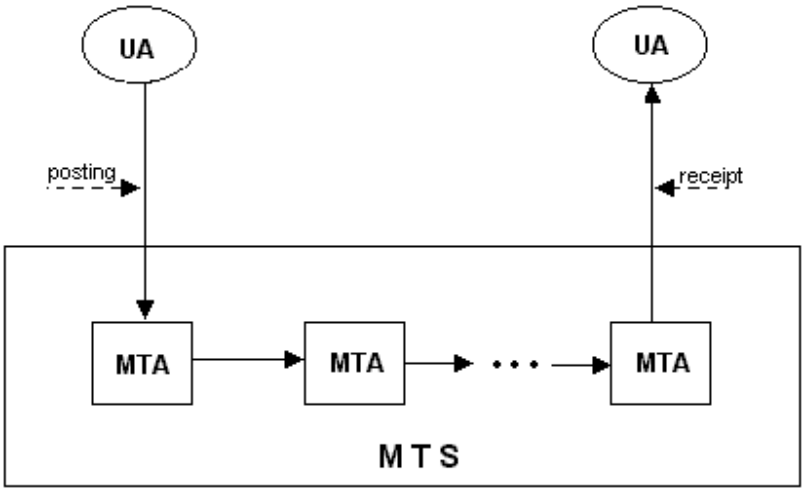
4.1 Οι Mail Servers

- Θα πρέπει να έχουν κατάλληλο DNS όνομα και διεύθυνση IP
- Το Λογισμικό του e-mail server θα πρέπει να είναι ασφαλές, εκπληρώνοντας τα διεθνή standards και σωστά ρυθμισμένο.
- Συχνή παρακολούθηση μηνυμάτων καταγραφής στον mail server, για να δει κάποιος ποιος τον χρησιμοποιεί για την αποστολή μηνυμάτων και ελέχθη η πιθανότητα να χρησιμοποιηθεί από χρήστες εκτός του δικτύου (π.χ. το δίκτυο της σχολικής ή διοικητικής μονάδας) για την αποστολή μηνυμάτων. (περίπτωση Open Relay Server)

4.1.1 Λειτουργιά MTA

- Ηλεκτρονικό Ταχυδρομείο (E-mail)

Το ηλεκτρονικό ταχυδρομείο επιτρέπει την αποστολή μηνυμάτων μεταξύ των χρηστών του Διαδικτύου. Οι διευθύνσεις του ηλεκτρονικού ταχυδρομείου βασίζονται στις διευθύνσεις του Internet και έχουν την μορφή "user@domain", όπου user το όνομα του χρήστη και domain το όνομα του υπολογιστή.



Παρακάτω φαίνεται πως μεταφέρονται τα ηλεκτρονικά μηνύματα. Ο User Agent (UA) είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο Mail Transfer Agent (MTA) παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται Message Transfer System (MTS).

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων POP (Post Office Protocol) και IMAP (Internet Message Access Protocol). Τα ίδια τα μηνύματα συντάσσονται με βάσει το πρωτόκολλο MIME (Multipurpose Internet Mail Extensions) ή με το RFC822.

Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server

και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστής του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA).

4.1.2 POP-before-SMTP

Το Pop-before-smtp Home είναι ένα απλό daemon που γράφεται σε Perl, για να επιτρέψει τον έλεγχο ηλεκτρονικού ταχυδρομείου βασισμένο επιτυχές σε POP ή IMAP logins. Αυτό είναι η ακριβής εργασία που εκτελείται από DRAC. Αυτό το daemon διαφέρει από το DRAC ως προς το στόχο για το οποίο σχεδιάστηκε. Το DRAC είναι ένα σχέδιο πελατών εξυπηρετηθούν, και απαιτεί Pop ή imap daemon. Το Pop-before-smtp Home δεν απαιτεί κανένα mods στα άλλα daemons, και δεν χρησιμοποιεί καμία επικοινωνία πελατών εξυπηρετητών. Έτσι είναι πολύ απλούστερο να εγκατασταθούν και να διατηρηθούν. Παρόλα αυτά αποτυγχάνει να καλύψει τις ανάγκες των ανθρώπων με χωριστούς pop/imap και smtp στους κεντρικούς υπολογιστές. Ένα άλλο σύστημα με μερικές ομοιότητες σε DRAC είναι το WHOSQN.

4.1.3 SMTP-Auth

SMTP AUTH είναι μια επέκταση υπηρεσιών SMTP [ESMTP] με το οποίο ένας πελάτης SMTP μπορεί να δείξει έναν μηχανισμό επικύρωσης στον κεντρικό

υπολογιστή, και να εκτελεστεί μια ανταλλαγή πρωτοκόλλου επικύρωσης, και διαπραγματεύεται προαιρετικά ένα στρώμα ασφάλειας για τις επόμενες αλληλεπιδράσεις πρωτοκόλλου. Αυτή η επέκταση είναι ένα σχεδιάγραμμα του [SASL].

4.2 Βασικές αρχές φιλτραρίσματος

Είναι γεγονός ότι οι περισσότεροι χρήστες που λαμβάνουν spam απλά το αγνοούν. Αυτό συμβαίνει είτε επειδή δεν έχουν τον απαραίτητο χρόνο να ασχοληθούν μαζί του είτε επειδή δεν έχουν τις απαραίτητες γνώσεις. Η στάση τους αυτή είναι κατανοητή όμως και πλήρης απραξία δεν είναι λύση. Μια τέτοια συμπεριφορά οδηγεί τους spammers να βασίζονται σε διάφορα στατιστικά στοιχεία και να χρησιμοποιούν επιχειρήματα του τύπου «Έστειλα το spam μου σε 7 εκατομμύρια λογαριασμούς και μόνο 190 διαμαρτυρήθηκαν, άρα οι υπόλοιποι το βρήκαν χρήσιμο και δεν καταλαβαίνω το λόγω που το δικό μου spamming είναι ενοχλητικό.»

Εναλλακτικά, κάποια θύματα του spam ίσως προσπαθήσουν να χρησιμοποιήσουν κάποια “remove address” κάποιου spam για να επικοινωνήσουν με τον spammer. Η κύρια ιδέα μιας τέτοιας πράξης είναι να ενημερώσουν τον spammer ότι δεν τους ενδιαφέρει το μήνυμά τους και κατ’ επέκταση να τους εξαιρέσουν από την λίστα τους (mailing list). Σίγουρα όμως μια τέτοια ενέργεια δεν πρόκειται να έχει τα επιθυμητά αποτελέσματα και είναι καταδικασμένη να αποτύχει (όπως άλλωστε και έγινε παγκοσμίως). Αντιθέτως, με αυτό τον τρόπο δείχνει στον spammer να καταλάβει ότι όντως ο λογαριασμός αυτός υπάρχει και ότι το spam του έφτασε στο στόχο του. Φυσικά και δεν πρόκειται ποτέ να εξαιρεθεί από τη λίστα του αλλά απεναντίας θα στέλνει περισσότερα spam

μηνύματα. Έτσι το καλύτερο πράγμα που έχει να κάνει κανείς είναι να διαμαρτυρηθεί!!!!!!.

Είναι γεγονός πως σήμερα οι περισσότεροι ISPs, για τους λόγους που προαναφέραμε, έχουν ορίσει σαν όρους «συνεργασίας» στους πελάτες τους ότι απαγορεύεται το spamming. Έτσι λοιπόν αν καταφέρει ο χρήστης που βομβαρδίζεται από ηλεκτρονικά μηνύματα spam να εντοπίσει τον ISP του spammer και τον ενημερώσει ότι ο πελάτης του έσπασε τη συμφωνία ή τους κανονισμούς και στέλνει spam τότε αυτομάτως θα ακυρωθεί ο λογαριασμός του. Μια τέτοια λοιπόν πρακτική θα λειτουργήσει ως αποθαρρυντικό για τους περισσότερους επίδοξους spammers, οι οποίοι θα το σκεφθούν καλά πριν κάνουν οτιδήποτε άλλο. Βέβαια πρέπει να τονιστεί σε αυτό το σημείο πως ένας ISP θα κινηθεί σύμφωνα με τα παραπάνω αφού πρώτα έχει λάβει αρκετά παράπονα για τον συγκεκριμένο πελάτη του και αφού έχει προσπαθήσει, άκαρπα, να τον συνετίσει.

Το ερώτημα που εύλογα γεννάται τώρα είναι το πώς θα μπορέσει ο χρήστης να ανακαλύψει τον ISP του spammer. Οι περισσότεροι spammer ξέρουν το κίνδυνο που διατρέχουν (κλείσιμο του λογαριασμού τους) με το spam που στέλνουν γι' αυτό και φροντίζουν να μην φαίνεται η σωστή διεύθυνση στο τμήμα «From:» του μηνύματος. Έτσι οι χρήστες πρέπει να είναι προσεκτικοί σε ποιόν ISP θα διαμαρτυρηθούν γιατί πολλές φορές το περιεχόμενο του τμήματος «From:» μπορεί να ανήκει σε κάποιον τρίτο που πραγματικά δε φταίει σε τίποτα. Με άλλα λόγια θα πρέπει ο χρήστης να μάθει να διαβάζει το «full message headers» το οποίο μοιάζει σαν ένας «κορμός» ενός μηνύματος που ταξιδεύει μέσα στο internet. Ίσως ορισμένοι spammers να έχουν «παραχαράξει» και το «full message headers» αλλά κάτι τέτοιο συμβαίνει σπάνια. Αν υποτεθεί λοιπόν ότι συμβαίνουν όλα τα παραπάνω με επιτυχία και καταλάβει ένας ISP ότι κάτι δεν πάει καλά με κάποιον πελάτη του, τότε εύλογα θα αποφασίσει να του κλείσει τον λογαριασμό.

Φυσικά όμως και οι spammers δεν είναι χαζοί και έχουν καταλάβει ότι ένας τέτοιος κίνδυνος ελλοχεύει. Έτσι λοιπόν οι λογαριασμοί των spammers σπάνια διατηρούνται για πολύ καιρό μετά την εκπλήρωση του στόχου τους (τη διανομή του spam). Συνήθως οι spammers ανοίγουν κάποιο λογαριασμό προκειμένου να στείλουν το spam τους που αφορά κάποιο site που βρίσκεται σε κάποια άλλη τοποθεσία. Μόλις το spam σταλθεί τότε ο λογαριασμός κλείνει ενώ το site παραμένει στην θέση του ανέπαφο και το spam εκπληρώνει το στόχο του. Για το λόγω αυτό οι περισσότερες εταιρίες web-hosting περιέχουν όρους στα συμβόλαιά τους που απαγορεύουν να χρησιμοποιούν spam για να «διαφημίσουν» κάποια υπηρεσία που βρίσκεται σε κάποια φιλοξενούμενη ιστοσελίδα.

Το θέμα βέβαια είναι πώς μπορεί κάποιος να εντοπίσει την εταιρεία που φιλοξενεί μια ιστοσελίδα που προβάλλεται μέσα από spam μηνύματα;! Είναι πιθανό ότι οι επίδοξοι spammers θα θέλουν κάπως να το κρύψουν όμως στόχος τους είναι και να ενημερώσουν τους παραλήπτες για την ύπαρξη της ιστοσελίδας που περιέχει την υπηρεσία που διαφημίζουν. Έτσι, αν και με λίγη δυσκολία αρχικά, μπορεί κάποιος να εντοπίσει την ιστοσελίδα και στην συνέχεια με εργαλεία όπως τα “traceroute” και τα “whois” να εντοπίσει την εταιρεία που κάνει hosting, να διαμαρτυρηθεί σε αυτή και κατ’ επέκταση να κλείσει την συγκεκριμένη ιστοσελίδα. Ειδικότερα τώρα το “traceroute” είναι ένα εργαλείο που παρέχει μια λίστα με μηχανές στο internet από τις οποίες ένα μήνυμα πέρασε από τη στιγμή που στάλθηκε μέχρι τη στιγμή που έφτασε στον προορισμό της.

Όσο αναφορά τώρα τα εργαλεία “whois”, αυτά ψάχνουν για να βρουν τους ιδιοκτήτες ενός domain ή ενός IP address. Τέλος πρέπει να αναφερθεί ότι αυτά τα εργαλεία λογισμικού μπορούν να τα τρέξουν τόσο από ένα desktop όσο και από το ίδιο το internet. Συνοψίζοντας όλα τα παραπάνω εύκολα συμπεραίνει κανείς ότι όλες οι λειτουργίες που περιγράφηκαν, προκειμένου να διαμαρτυρηθεί κάποιος για το spam συνιστούν μια όχι και τόσο εύκολη διαδικασία. Έχοντας λοιπόν

καταλάβει οι ειδικοί τη δυσκολία αυτή, έχουν κατασκευάσει κατά καιρούς διάφορα εργαλεία για να την αυτοματοποιήσουν. Το spamcop είναι μια υπηρεσία η οποία σκοπεύει να αντιμετωπίσει με αυτοματοποιημένο τρόπο την παραπάνω διαδικασία. Ειδικότερα, δίνεις το spam, γράφει και ταχυδρομεί τα παράπονα. Το spamcop έχει την φήμη του πιο ασφαλούς λογισμικού αφού πολύ λίγες φορές στέλνει τα παράπονα σε λάθος τοποθεσίες. Πάντως συνιστάται να παρατηρεί ο χρήστης την λειτουργία ενός εργαλείου.

Advanced Spam fighting

Μια τακτική που χρησιμοποιείται πάρα πολύ από αρκετούς ISPs είναι η τεχνική του φιλτραρίσματος. Ο ISP σαρώνει τα εισερχόμενα ηλεκτρονικά μηνύματα και γενικά οποιαδήποτε μηνύματα τα οποία ταιριάζουνε με ένα συγκεκριμένο μοτίβο (pattern) το οποίο έχει χαρακτηριστεί ως spam. Ειδικότερα πάντα υπήρχαν άτομα τα οποία φιλτράρανε το spam χρησιμοποιώντας απλούς κανόνες μέσα από το ηλεκτρονικό μήνυμά τους. Για παράδειγμα ανάλογα με τις προτιμήσεις του κάθε χρήστη, ένα μήνυμα που θα περιλάμβανε την έκφραση “free live sex” στην γραμμή του θέματος θα μπορούσε να χαρακτηριστεί ως spam, και είτε να διαγραφεί, είτε να περάσει σε ένα φάκελο όπως λόγου χάριν ενοχλητική αλληλογραφία.

Παρόλα΄ αυτά όπως είναι φυσικό τέτοια συστήματα μπορεί να έχουν και ένα ποσοστό απωλειών. Άρα γίνεται εύκολα αντιληπτό ότι ο μεγάλος κίνδυνος που εγκυμονούν συστήματα σαν και αυτά είναι ότι ο χρήστης μπορεί να χάσει ορισμένα για αυτόν σημαντικά μηνύματα αφού αυτά θα έχουν χαρακτηριστεί ως spam. Πρόσφατα αρκετά προσωπικά spam φίλτρα έχουν παρουσιαστεί στο

προσκήνιο. Αυτά τοποθετούνται μεταξύ του mail προγράμματος και του mail box χρησιμοποιώντας πιο υψηλού επιπέδου μεθόδους και τεχνικές για να φιλτράρει ή να χαρακτηρίσει spam μηνύματα. Τα περισσότερα από αυτά δουλεύουν με διαφορετικούς τρόπους, ενώ παρουσιάζουν διαφορετικές ικανότητες και αδυναμίες.

Commercial/Shareware spam-filters for Windows users:

- **Cloudmark SpamNet (needs Outlook)**
- **Disruptor OL (needs Outlook)**
- **McAfee SpamKiller**
- **MiserMail (email reader with spam-filtering features)**
- **PostArmor**
- **Spam Buster**
- **Spam Butcher**
- **Spam CounterStrike**
- **SpamEater Pro**
- **Spam Inspector**
- **SpamNix (for Eudora users)**
- **SpamX**

Spam-filters for Unix users:

- **PostArmor**
- **SpamAssassin**

- **SpamX**
- **The Spam Bouncer**
- **Vipul's Razor**

Spam-filters for Macs users:

- **PostArmor**
- **Spamfire**
- **SpamX**

Free spam-filters for Windows users:

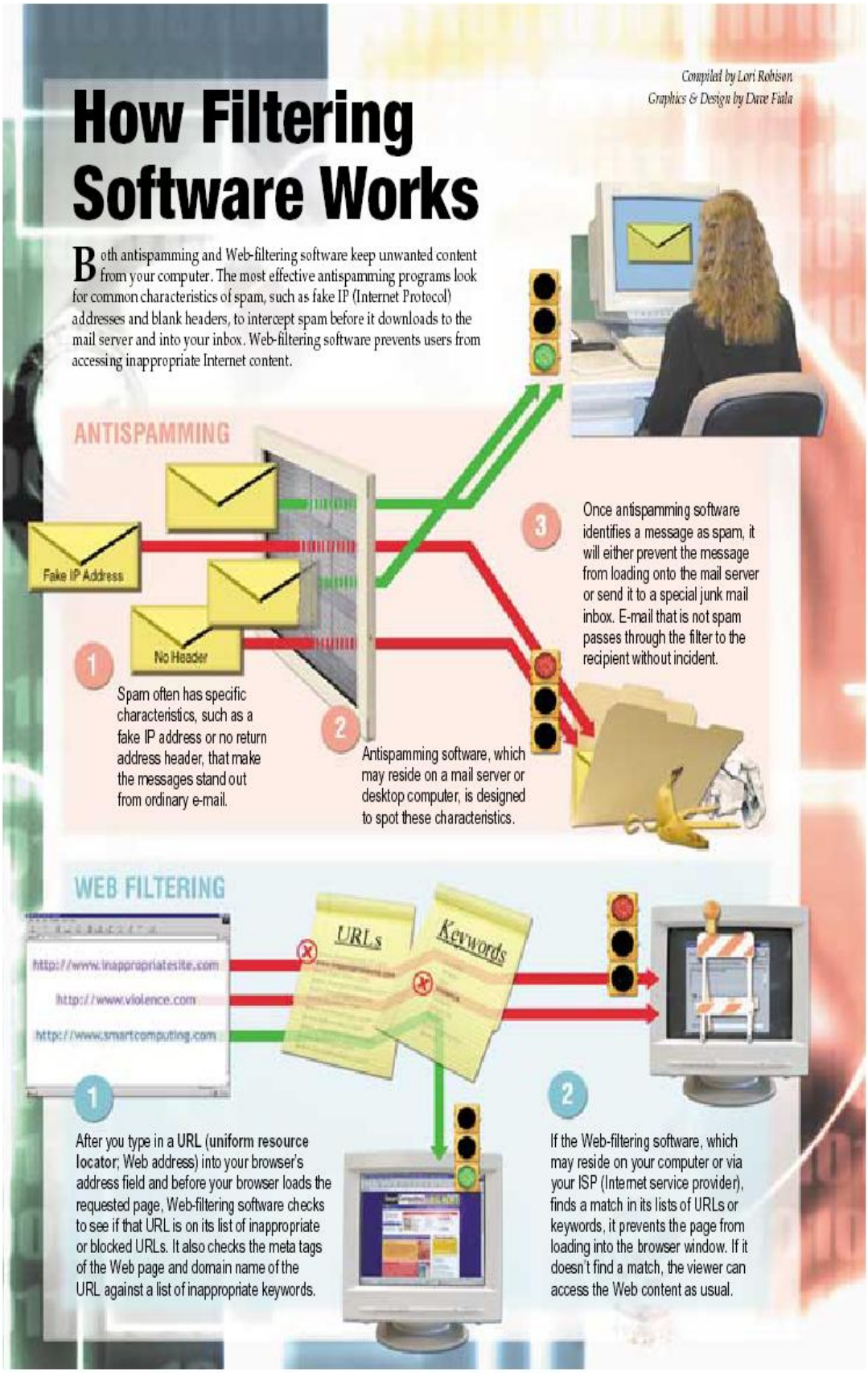
- **K9 (trainable spam-filter)**
- **MailWasher**
- **POP3 Catcher (cut-down free version)**
- **PostArmor (free for personal use)**
- **SAProxy (SpamAssassin)**
- **SpamFighter (needs Outlook or Outlook Express)**
- **SpamPal**

Bayesian filtering

Το πιθανοθεωρητικό φίλτρο του Bayes είναι μια ιδιαίτερα δημοφιλής μέθοδος φιλτραρίσματος, η οποία ενσωματώνεται σε δημοφιλή προγράμματα, όπως το mozilla thunderbird. Η ιδέα είναι ότι εκπαιδεύει κάποιος το φίλτρο του

στο να αναγνωρίζει το spam από το μη spam, με το να του υποδεικνύει πότε έκανε λάθος. Αυτό μπορεί να είναι μια ιδιαίτερα επιτυχημένη τεχνική αφού για τον καθένα, το τι είναι spam και τι όχι είναι κάτι διαφορετικό.

Για παράδειγμα, για κάποιον που λαμβάνει το μήνυμα που περιέχει την λέξη “Viagra” μπορεί να είναι spam ενώ για κάποιον άλλο μπορεί να μην είναι για ευνόητους λόγους. Το μειονέκτημα του συγκεκριμένου φίλτρου είναι ότι χρειάζεται μεγάλη προσπάθεια και χρόνο για να εκπαιδευτεί, ενώ τα a priori εκπαιδευμένα φίλτρα δεν είναι τόσο πρακτικά. Στην συνέχεια υπάρχη ένα ένθετο το οποίο περιγράφει τον τρόπο λειτουργίας ενός φίλτρου:



4.3 Realtime Blackhole List

Είναι ένας κατάλογος διευθύνσεων IP, των οποίων οι ιδιοκτήτες αρνούνται να σταματήσο

υν τον πολλαπλασιασμό του spam. Το RBL απαριθμεί συνήθως τις διευθύνσεις κεντρικών υπολογιστών IP από ISPs του οποίου πελάτες είναι αρμόδιοι για το spam και από ISPs του οποίου οι κεντρικοί υπολογιστές πειρατεύονται για τον ηλεκτρονόμο spam.

4.4 Αντιμετωπίζοντας το SPAM

Το να αντιμετωπίσει κανείς το Spam δεν είναι κάτι εύκολο. Ο χρήστης όμως έχει στην διάθεση του μερικούς τρόπους αντιμετώπισης πχ. Antispam Software. Όμως κατά κύριο λόγο θα πρέπει ο ίδιος να προσέχει και να εφαρμόζει μερικές τεχνικές.

4.4.1 Απόψεις σχετικά με το spam και την αντιμετώπισή του

Τρεις απόψεις επικρατούν στην δικτυακή κοινότητα σε σχέση με το spam και την αντιμετώπιση του.

- **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.

- Οι χρήστες αυτής της άποψης πιστεύουν ότι δεν θα χάσουν ποτέ χρήσιμα μηνύματα και προτιμούν να λαμβάνουν όλη την αλληλογραφία που απευθύνεται σε αυτούς.

- **Η αντιμετώπιση του spam είναι ευθύνη των τελικών χρηστών:** Η τακτοποίηση του spam είναι πολύ δύσκολη. Η αντιμετώπιση του γίνεται από τις

προσωπικές επιλογές του τελικού χρήστη. Οι τελικοί χρήστες επιλέγουν και διαμορφώνουν τα φίλτρα με βάση τα επιλεγμένα μηνύματα που θα περνάνε ή θα αποκλείονται από το γραμματοκιβώτιο τους. Η άποψη αυτή ενισχύεται και από την αρχή ότι η απόρριψη μηνυμάτων χωρίς την εξουσιοδότηση του κάθε τελικού χρήστη είναι παραβίαση της ιδιωτικότητας (μυστικότητας) της επικοινωνίας.

- Οι χρήστες αυτής της άποψης πιστεύουν ότι η απώλεια χρήσιμων μηνυμάτων σε σχέση με τα απορριπτόμενα spam μηνύματα αφήνεται στην προσωπική επιλογή και ευθύνη του τελικού χρήστη.

- **Η αντιμετώπιση του spam είναι ευθύνη των διαχειριστών στους mail servers:** Η άποψη αυτή ενισχύεται από την παρουσία εργαλείων για την απόρριψη μηνυμάτων σε επίπεδο κεντρικών συστημάτων. Η καταπολέμηση του spam πρέπει να γίνεται στα κεντρικά συστήματα διακίνησης της αλληλογραφίας (mail servers) στο όνομα της εξασφάλισης των πόρων των κεντρικών συστημάτων και του δικτύου. Επίσης πολλές φορές οι υπεύθυνοι των δικτύων θεωρούν απαράδεκτο να φθάνει μέσω του δικτύου τους απαράδεκτη εμπορική ή επικίνδυνη αλληλογραφία.

- Οι χρήστες αυτής της άποψης πιστεύουν ότι η απώλεια χρήσιμων μηνυμάτων σε σχέση με τα απορριπτόμενα spam μηνύματα μπορεί να κρατηθεί σε αποδεκτά χαμηλά επίπεδα. Η άποψη αυτή ενισχύεται και από το γεγονός ότι τα χρήσιμα μηνύματα που απορρίπτονται οφείλονται στην ελλιπή ή κακή διαμόρφωση κάποιου άλλου διαχειριστή από το σύστημα από το οποίο προέρχεται η αλληλογραφία.

Πάνω στις 3 πιο πάνω απόψεις υπάρχουν δύο βασικές παραλλαγές.

- Τα μηνύματα που προέρχονται από διάφορους αποστολείς οι οποίοι βρίσκονται σε διάφορες λίστες τύπου RBL (Real Time Black Hole Lists) πρέπει να απορρίπτονται χωρίς εξαίρεση. Άλλοι πιστεύουν ότι αυτές οι λίστες δεν είναι πάντα δίκαιες με την έννοια της καταγραφής ή όχι των διαφόρων αποστολέων, ενώ τα κριτήρια ποικίλουν από λίστα σε λίστα. Αυτό οδηγεί πολλές φορές στη απόρριψη αποδεκτών μηνυμάτων και τα παράπονα των χρηστών των οποίων τα μηνύματα απορρίπτονται.

- Μια άλλη άποψη που υπάρχει είναι ότι τα μηνύματα που δεν ικανοποιούν τα γνωστά standards, πρέπει να απορρίπτονται ή να χαρακτηρίζονται ως πιθανόν μηνύματα spam. Ο έλεγχος αυτός περιλαμβάνει τις επικεφαλίδες From ή τον φάκελο «envelope» του μηνύματος. Για διάφορους λόγους πολλά μηνύματα τύπου spam δεν έχουν έγκυρες επικεφαλίδες (mail Headers). Στο σημείο αυτό άλλοι πιστεύουν ότι τα μηνύματα αυτά πρέπει να απορρίπτονται και άλλοι ότι δεν πρέπει, γιατί τέτοια λάθη μπορεί να συναντήσει κανείς και σε αποδεκτά όσο αφορά το περιεχόμενο μηνύματα.

4.4.2 Τι μπορεί να γίνει για την αποφυγή του SPAM

- **Μη δημοσίευση των διευθύνσεων ηλεκτρονικού ταχυδρομείου.** Βάζοντας κάποιος την διεύθυνση ηλεκτρονικού ταχυδρομείου του σε μια

ιστοσελίδα είναι σχεδόν σίγουρο ότι σύντομα θα υπάρχουν μηνύματα spam στο γραμματοκιβώτιο του.

- **Αποφυγή κοινοποίησης την διεύθυνσης ηλεκτρονικού ταχυδρομείου σε μη έμπιστους οργανισμούς:** Πρέπει να είναι κάποιος προσεκτικός όταν επισκέπτεται διάφορους δικτυακούς τόπους όπου ζητείται η συμπλήρωση προσωπικών στοιχείων και στοιχείων επικοινωνίας. Όταν είναι αναγκασμένος να κάνει κάτι τέτοιο, πρέπει να διαβάσει προσεκτικά τους όρους χρήσης και τη πολιτική εχεμύθειας για την οποία δεσμεύεται ο συγκεκριμένος οργανισμός.
- **Ποτέ απάντηση στο spam:** Ποτέ δεν απαντάει κάποιος στους spammers ακόμα και στην ένδειξη για διαγραφή από τις ηλεκτρονικές λίστες τους. Αυτό έχει ως τελικό αποτέλεσμα:
- Να διαπιστωθεί η εγκυρότητα της ηλεκτρονικής διεύθυνσης και επομένως να γίνει στόχος αποστολής επιπλέον μηνυμάτων.
- Χάσιμο χρόνου και σπατάλης πόρων χωρίς λόγο, ενώ δεν υπάρχει αποτέλεσμα.
- **Αναφορά κάθε μηνύματος spam που λαμβάνονται**: Υπάρχουν σχετικές υπηρεσίες του διαδικτύου η οποίες συντηρούν λίστες spammers. Τις λίστες αυτές αξιοποιούν πολλοί εξυπηρετητές ηλεκτρονικού ταχυδρομείου για τον περιορισμό του spam που φθάνει στους χρήστες. Στις υπηρεσίες αυτές μπορεί να αναφερθούν τα μηνύματα τύπου spam που φθάνουν στον παραλήπτη.
- **Διάδοση της γνώσης και της εμπειρίας σχετικά με το spam.** Επικοινωνία με τους χρήστες του διαδυκτίου, μαθητές, εκπαιδευτικούς, διοικητικό προσωπικό, στην οικογένεια και τους φίλους για το θέμα του spam και την αντιμετώπιση του. Είναι αρκετά συνηθισμένο οι spammers να συγκεντρώνουν ηλεκτρονικές διευθύνσεις από τις απαντήσεις χρηστών του διαδικτύου.
- **Έλεγχος των συστημάτων ώστε αυτά να είναι σωστά διαμορφωμένα και ασφαλή.** Ένα μεγάλο ποσοστό του spam διαδίδεται από mail servers που δεν

είναι σωστά διαμορφωμένοι (Open Relay), αλλά ακόμα και από συστήματα χρηστών.

4.4.3 Το έργο Lumos

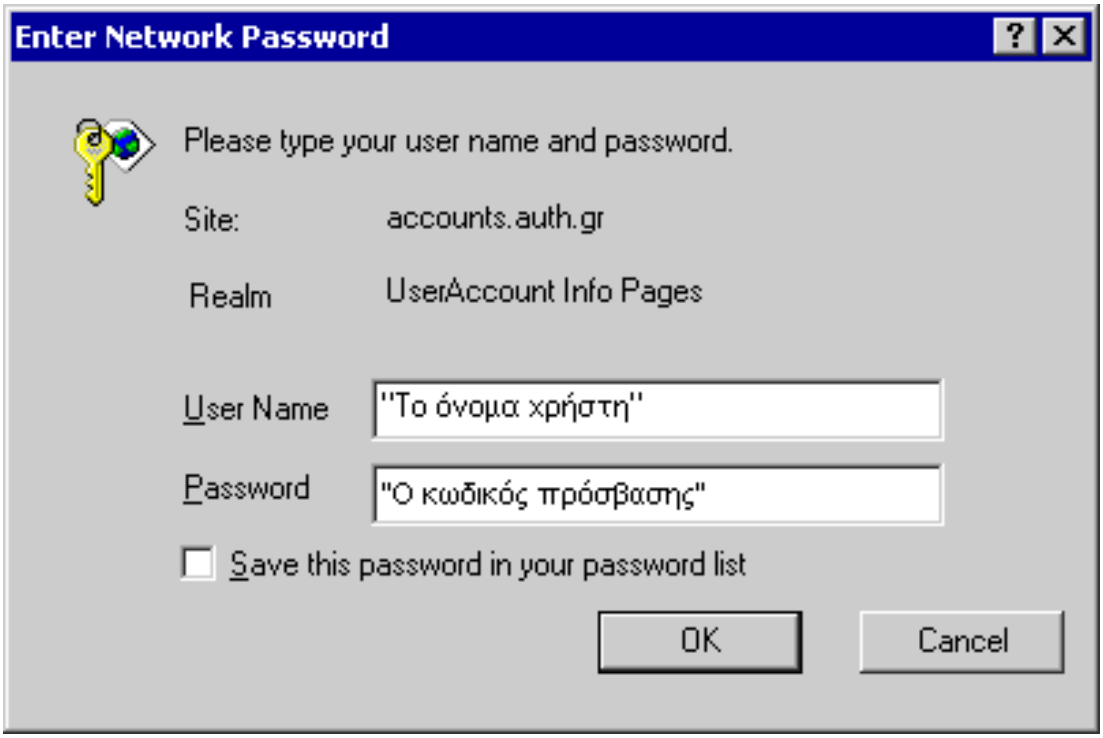
Το πρόγραμμα Lumos είναι η προσπάθεια να εξεταστεί το πρόβλημα spam μέσω ενός ληξιαρχείου για τα μαζικά ηλεκτρονικά μηνύματα. Απελευθέρωσε ένα λεπτομερές σχέδιο για το πώς το ληξιαρχείο θα λειτουργούσε. Παρά την πρόοδο εντούτοις, η προσπάθεια πρέπει να κερδίσει ακόμα την υποστήριξη των φορέων παροχής υπηρεσιών Διαδικτύου. Το πρόγραμμα Lumos έδωσε ελπίδες να αντιμετωπιστεί το spam με την επίλυση ενός βασικού προβλήματος του ηλεκτρονικού ταχυδρομείου: την έλλειψη ταυτότητας και υπευθυνότητας. Μέσω του ληξιαρχείου αυτοί που στέλνουν μηνύματα θα υπέγραφαν on-line και θα συμφωνούσαν να παραμείνουν υπεύθυνοι όσο αφορά στις αποστολές μηνυμάτων τους. Οι ISPs θα τους αξιολογούσαν σε μια κλίμακα από το 1 έως το 100 τοποθετώντας τους σε μια σειρά που θα μπορούσε να χρησιμοποιηθεί από ISPs για να απορρίψει ορισμένους από αυτούς.

Εντούτοις οι ISPs δεν έχουν πει ότι θα εφάρμοζαν ένα τέτοιο σύστημα, σύμφωνα με τον Trevor Hughes (ο εκτελεστικός διευθυντής του δικτύου που διαφημίζει τον συνασπισμό φορέων παροχής υπηρεσιών ηλεκτρονικού ταχυδρομείου και διευθύνει τα προγράμματα lumos). Οι φορείς παροχής υπηρεσιών ηλεκτρονικού ταχυδρομείου έχουν παραπονεθεί πικρά που οι ISPs εμποδίζουν τις αποστολές τους. Εντούτοις σε μια πρόσφατη antispam συνεδρίαση έγινε σαφές ότι η No.1 προτεραιότητα ήταν να προστατεύσουν τους χρήστες από το ανεπιθύμητο ηλεκτρονικό ταχυδρομείο.

Πέρα από το κορυφαίο πρόγραμμα lumos οι ISPs πρέπει να δημιουργήσουν ένα σύστημα που είναι εύκαμπτο και αρκετά φτηνό που θα μπορούν να το υιοθετήσουν χιλιάδες μικροί ISPs.

4.5 Anti-SPAM Software

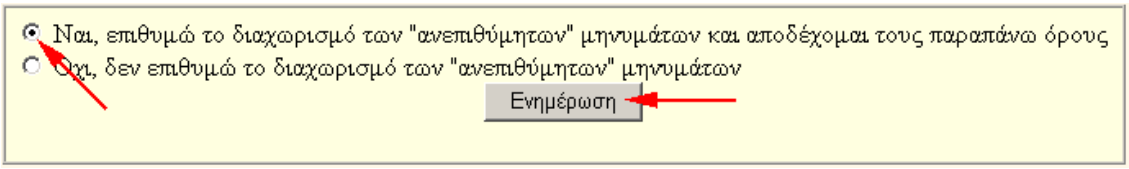
Μια δυνατότητα ενεργοποίησης μηχανισμού anti - spam παρέχεται και μέσα από τη σελίδα διαχείρισης του λογαριασμού https://accounts.auth.gr. Η παραπάνω σελίδα απαιτεί πιστοποίηση ταυτότητας και γι' αυτό θα πρέπει να συμπληρωθεί το όνομα χρήστη (User Name) και τον κωδικό πρόσβασης (Password) του λογαριασμού στο παρακάτω παράθυρο με το κλικ του OK



Στην επιλογή Ανεπιθύμητα μηνύματα του https://accounts.auth.gr μπορούν να δουν την τρέχουσα επιλογή δίπλα στην Μηχανισμός Διαχωρισμού, η οποία αρχικά είναι ρυθμισμένη στην ένδειξη **ΑΠΕΝΕΡΓΟΠΟΙΗΜΕΝΟΣ**:

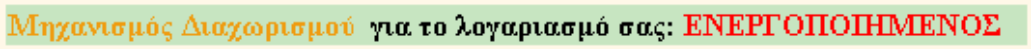
Ενεργοποίηση

Στην σελίδα με τίτλο Ανεπιθύμητα μηνύματα του https://accounts.auth.gr, πρέπει να επιλεγεί Ναι, επιθυμώ το διαχωρισμό των "ανεπιθύμητων" μηνυμάτων και αποδέχομαι τους παραπάνω όρους και να πατηθεί το κουμπί Ενημέρωση:

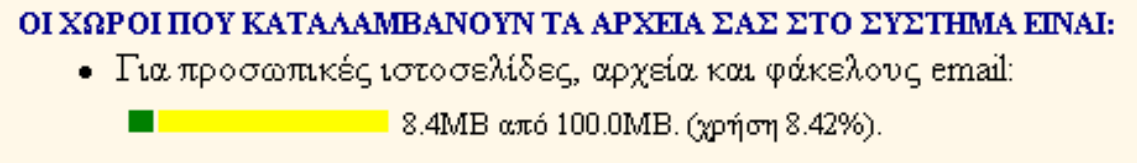


Μόλις ενεργοποιηθεί ο μηχανισμός, θα αλλάξει η ένδειξη στην σελίδα Μηχανισμός Διαχωρισμού από **ΑΠΕΝΕΡΓΟΠΟΙΗΜΕΝΟΣ** σε θα ενεργοποιηθεί σε 10 λεπτά:

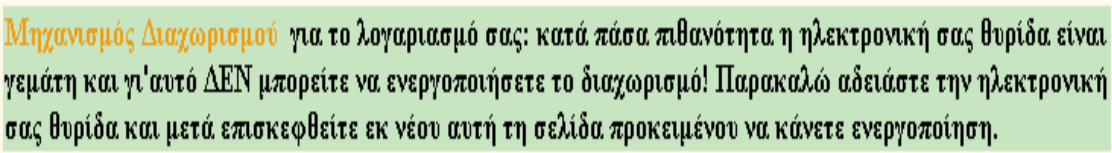
Οι χρήστες καλούνται να επιβεβαιώσουν αργότερα την ενεργοποίηση του μηχανισμού επισκεπτόμενος την σελίδα ενεργοποίησης: μετά από 10 λεπτά η ένδειξη για τον χρήστη μεταβάλλεται σε **ΕΝΕΡΓΟΠΟΙΗΜΕΝΟΣ***



*Σε περίπτωση που ο προσωπικός χώρος δίσκου που έχει διατεθεί στο χρήστη είναι ήδη κατειλημμένος με άλλα αρχεία του χρήστη, ο μηχανισμός δεν θα μπορέσει να ενεργοποιηθεί (ακόμη και μετά από 10'). Οι χρήστες μπορούν να ελέγξουν τον διαθέσιμο προσωπικό χώρο στην διεύθυνση https://accounts.auth.gr/ στην επιλογή **Ο λογαριασμός μου:**



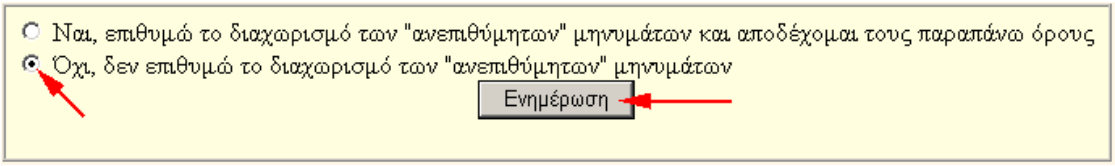
Το μήνυμα που εμφανίζεται μετά από 10 λεπτά είναι: **κατά πάσα πιθανότητα η ηλεκτρονική σας θυρίδα είναι γεμάτη και γι' αυτό ΔΕΝ μπορείτε να ενεργοποιήσετε το διαχωρισμό! Παρακαλώ αδειάστε την ηλεκτρονική σας θυρίδα και μετά επισκεφθείτε εκ νέου αυτή τη σελίδα προκειμένου να κάνετε ενεργοποίηση:**



Αφού ο χρήστης μειώσει το μέγεθος του λογαριασμού του μέσα στα επιτρεπτά, από το Α.Π.Θ. όρια, θα πρέπει να επισκεφθεί εκ νέου την σελίδα https://accounts.auth.gr, συγκεκριμένα την σελίδα **Ανεπιθύμητα μηνύματα, και να επαναλάβει την διαδικασία ενεργοποίησης του μηχανισμού anti-spam.**

Απενεργοποίηση

Στην σελίδα με τίτλο **Ανεπιθύμητα μηνύματα** του https://accounts.auth.gr, πρέπει να κάνει την επιλογή **Όχι, δεν επιθυμώ το διαχωρισμό των "ανεπιθύμητων" μηνυμάτων:**



Μόλις απενεργοποιηθεί ο μηχανισμός, θα αλλάξει η ένδειξη στην σελίδα **Ανεπιθύμητα Μηνύματα** από **ΕΝΕΡΓΟΠΟΙΗΜΕΝΟΣ** σε **ΑΠΕΝΕΡΓΟΠΟΙΗΜΕΝΟΣ**, ώστε να αντικατοπτρίζει την νέα κατάσταση αναφορικά με τον μηχανισμό anti-spam

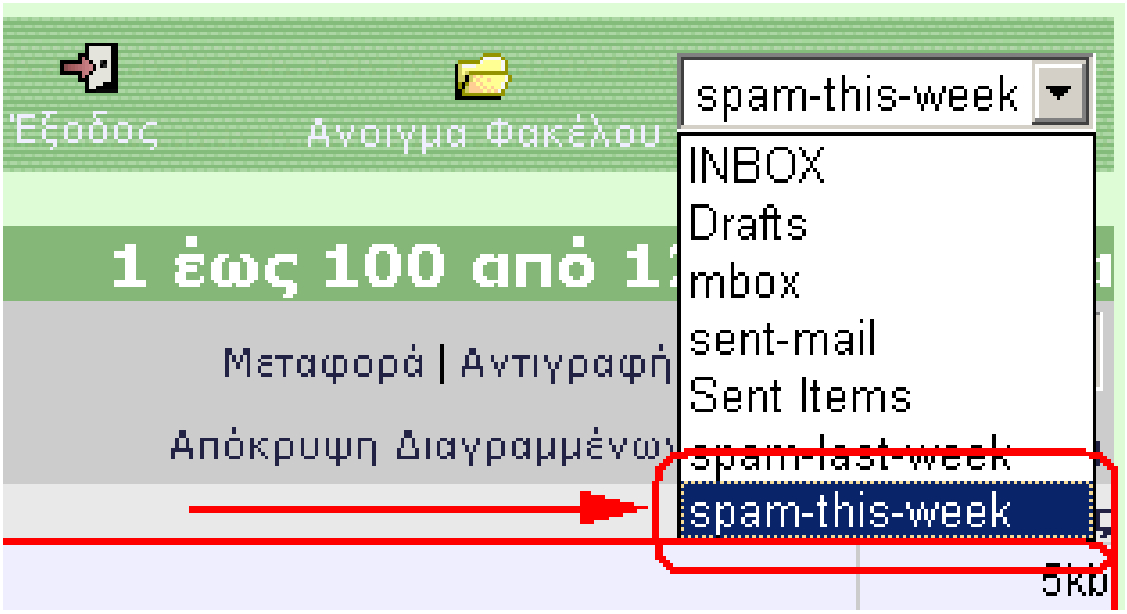
Οδηγίες Χρήσης

Παρακάτω περιγράφονται οι οδηγίες χρήσης του μηχανισμού anti-spam ανάλογα με τον τρόπο πρόσβασης στον λογαριασμό του Α.Π.Θ. του ηλεκτρονικού ταχυδρομείου σας.

Μέσω της ιστοσελίδας webmail.auth.gr (WebMail)

Πρώτα, ο χρήστης πρέπει να συνδεθεί με το γραμματοκιβώτιό του στην ηλεκτρονική διεύθυνση http://webmail.auth.gr

Στο κεντρικό παράθυρο μπορεί να επιλέξει να δει τα διαχωρισμένα μηνύματα **spam** που βρίσκονται στον φάκελο με την ονομασία **spam-this-week**, κάνοντας από το ΄**Ανοιγμα Φακέλου** την επιλογή **spam-this-week**. Θα εμφανιστούν (αν υπάρχουν) τα περιεχόμενα μηνύματα του φακέλου:

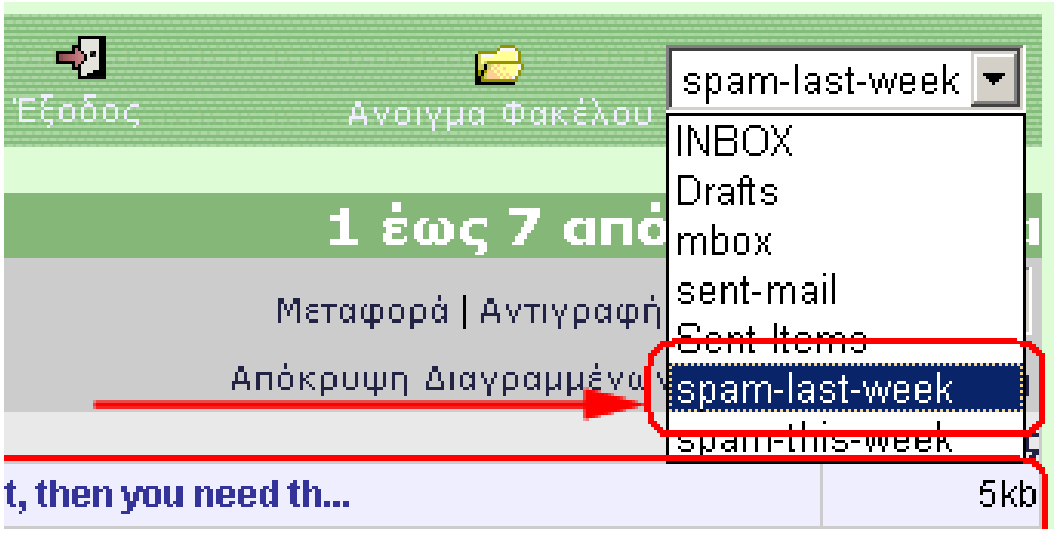


Τα μηνύματα αυτά μπορεί να επεξεργαστεί όπως κάθε άλλο μήνυμα, ωστόσο υπάρχουν κάποιες οδηγίες που καλό θα ήταν να ακολουθήσει αναφορικά με την χρήση των μηνυμάτων αυτών, ώστε να μην αντιμετωπίσει μελλοντικά προβλήματα. Πιο συγκεκριμένα, θα πρέπει:

- Να μην απαντάει στα μηνύματα spam

- Να μην επισκέπτεται τις προτεινόμενες από το μήνυμα σελίδες
- Να μην γνωστοποιεί τα προσωπικά του δεδομένα
- Να μην γνωστοποιεί αριθμούς πιστωτικών (κυρίως) καρτών στο Διαδίκτυο.

Αντίστοιχα μπορεί, ακολουθώντας την ίδια διαδικασία, να δει και τα διαχωρισμένα μηνύματα spam της προηγούμενης εβδομάδας, τα οποία αποθηκεύονται στον φάκελο **spam-last-week**:

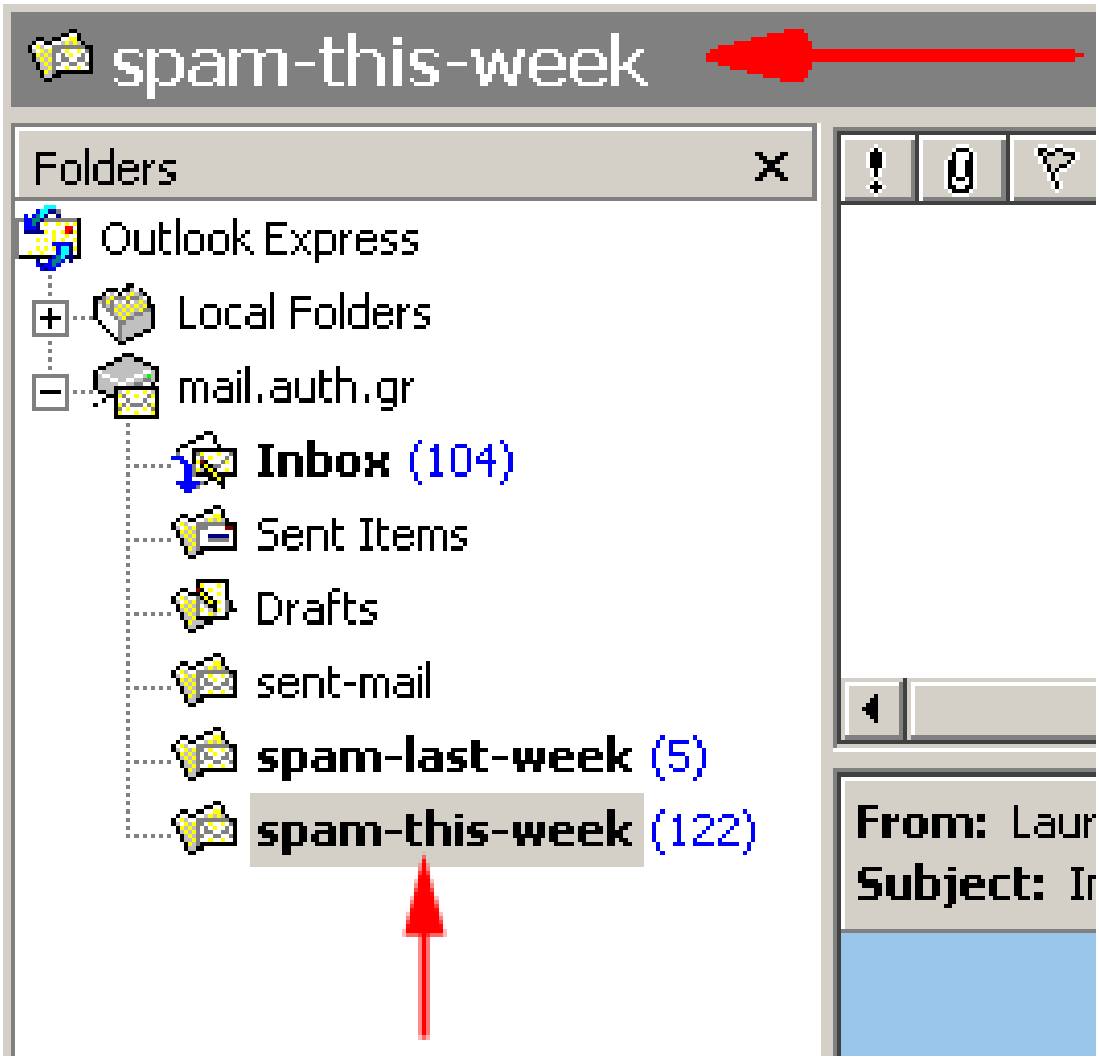


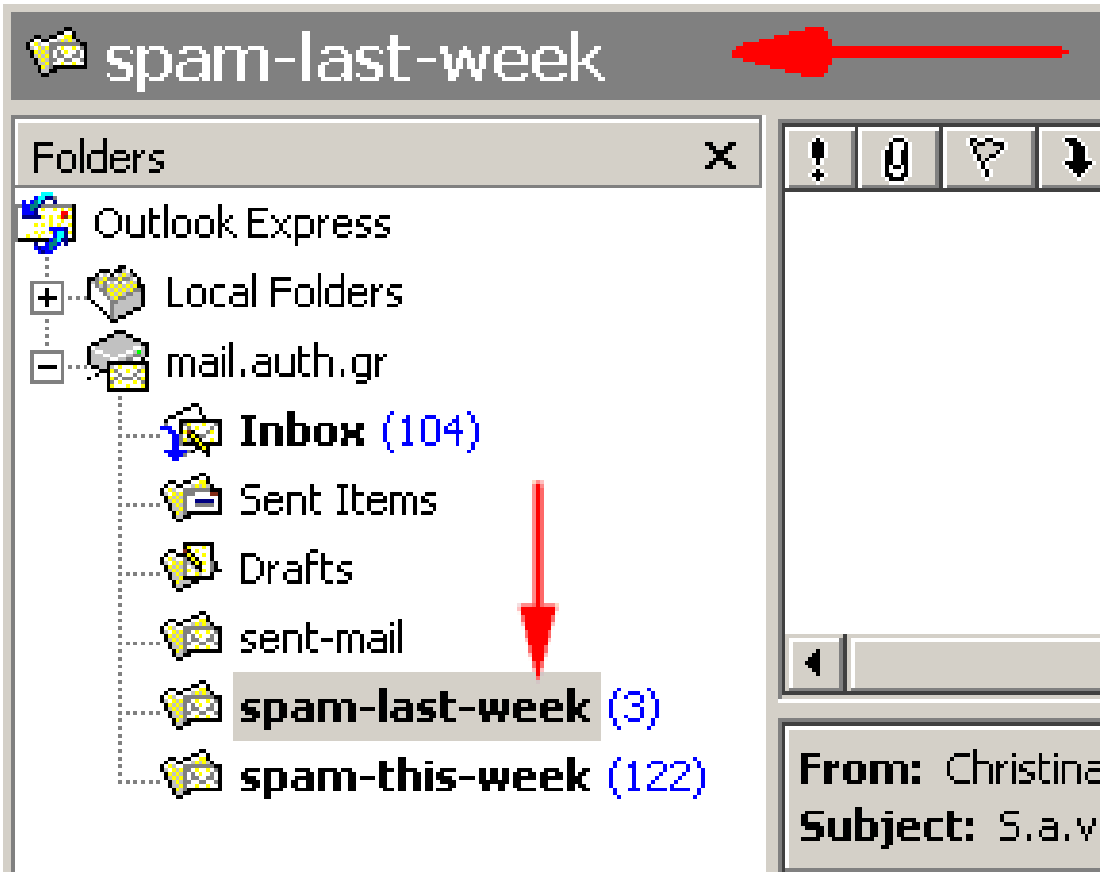
Μέσω IMAP

Οδηγίες για να ρυθμίσει το περιβάλλον αλληλογραφίας του υπολογιστή του ώστε να λαμβάνει και να στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου (μέσω IMAP) με χρήση του λογαριασμού που έχει λάβει από το ΚΛ&ΔΔ.

Outlook Express

Στο Outlook Express, οι σχετικοί με τον μηχανισμό anti-spam φάκελοι βρίσκονται ιεραρχικά κάτω από τον φάκελο με τα εισερχόμενα μηνύματα **(Inbox)**:





Netscape Messenger

Στο Netsape Messenger, οι σχετικοί με τον μηχανισμό anti-spam φάκελοι βρίσκονται επίσης ιεραρχικά κάτω από τον φάκελο με τα εισερχόμενα μηνύματα **(Inbox):**

Μέσω POP3

Οδηγίες για να ρυθμίσει ο χρήστης το περιβάλλον αλληλογραφίας του υπολογιστή του ώστε να λαμβάνει και να στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου (μέσω POP3) με χρήση του λογαριασμού που έχει λάβει από το ΚΛ&ΔΔ.

Χρησιμοποιώντας POP3, οι σχετικοί με τον μηχανισμό anti-spam φάκελοι **δεν εμφανίζονται** λόγω του τρόπου λειτουργίας του συγκεκριμένου πρωτοκόλλου, παρά μόνο εμφανίζονται τα περιεχόμενα μηνύματα στον φάκελο εισερχόμενων **(Inbox)**.

Επομένως, θα πρέπει ο χρήστης να προσανατολιστεί σε εναλλακτικό τρόπο χρήσης του μηχανισμού, δηλαδή μέσω **WebMail** ή μέσω **IMAP.**

4.5.1 SpamEater

Είναι μια ιδιαίτερα αποτελεσματική λύση που παρέχεται από λογισμικό που σταματά spam και ιούς στις διαδικτυακές πύλες. Χρησιμοποιώντας έναν ισχυρό συνδυασμό τεχνικών λογισμικού και ανάλυσης, το δίκτυο SpamEater προσφέρει μια από τις καλύτερες εκτιμήσεις ακρίβειας, διατηρώντας ένα σχεδόν ανύπαρκτο ποσοστό λάθους. Και όντας διαχειριζόμενη υπηρεσία, δεν χρειάζεται χρόνος εγκατάστασης ή συντήρησης από τον τελικό χρήστη.

4.5.2 SpamNet

Το σε κοινοτικό επίπεδο φιλτράρισμα Spamnet κάνει μια αξιοπρόσεκτη εργασία του φραξίματος spam χωρίς να αποκλείει τα έγκυρα ηλεκτρονικά μηνύματα. Εφόσον χρησιμοποιείται το Outlook Express είναι μια πολύ καλή επιλογή. Υποστηρίζει POP3, IMAP, ανταλλαγή accounts στο Outlook (χωριστή έκδοση διαθέσιμη για το Outlook Express). Το σε κοινοτικό επίπεδο φιλτράρισμα δεν εμπόδισε κανένα έγκυρο ηλεκτρονικό μήνυμα και επιτρέπει λίγα μόνο μηνύματα spam να φτάσουν στο inbox.

4.5.3 SpamAssasin

Το SpamAssassin είναι ένα φίλτρο ηλεκτρονικού ταχυδρομείου που προσπαθεί να προσδιορίσει τα μηνύματα spam χρησιμοποιώντας ποικίλους μηχανισμούς συμπεριλαμβανομένης της ανάλυσης κειμένων, Μπεϋζιανό φιλτράρισμα, blocklists, και φιλτράροντας βάσεις δεδομένων.

Χρησιμοποιώντας τη βάση κανόνων του, χρησιμοποιεί ένα ευρύ φάσμα των ευρετικών δοκιμών σε επιγραφές και κείμενο σωμάτων για να προσδιορίσει τα "spam". Μόλις προσδιοριστεί, το ταχυδρομείο μπορεί έπειτα να κολληθεί προαιρετικά ως spam για να φιλτραριστεί αργότερα .

Το SpamAssassin διαφοροποιεί επιτυχώς τα χαρακτηριστικά μεταξύ του spam και του -μη-spam μεταξύ του 95% και 100% των περιπτώσεων και ανάλογα με το είδος του μηνύματος χρησιμοποιεί και ανάλογο Μπεϋζιανό φίλτρο.

4.5.4 SpamPal

Το SpamPal είναι ένα πρόγραμμα ταξινόμησης ταχυδρομείου που μπορεί να βοηθήσει να ξεχωρίσει το spam από τα μηνύματα που θέλει πραγματικά να διαβάσει ο χρήστης.

Τι χρειάζεται για να χρησιμοποιηθεί το SpamPal;

1. Λειτουργικό σύστημα Windows 95, 98, ME, NT, 2000, 2003 ή XP.
2. Ένα mailbox POP3 ή IMAP4.
3. Ένα τυποποιημένο πρόγραμμα ηλεκτρονικού ταχυδρομείου όπως Outlook, Outlook Express ή Eudora.

Το SpamPal δεν εργάζεται με;

- AOL
- Hotmail
- Yahoo
- Juno
- MSN
- Ή οποιοδήποτε άλλο ιδιόκτητο ταχυδρομικό σύστημα.

Πως λειτουργεί το SpamPal:

Το SpamPal εφαρμόζεται μεταξύ του προγράμματος (πελάτη) ηλεκτρονικού ταχυδρομείου και της ταχυδρομικής θυρίδας, ελέγχοντας το ηλεκτρονικό ταχυδρομείο την στιγμή που αυτό ανακτάται. Οποιαδήποτε μηνύματα ηλεκτρονικού ταχυδρομείου που το SpamPal θεωρεί spam θα αντιγραφούν σε έναν χωριστό φάκελλο με ειδική επιγραφή και το spam δεν θα αναμιχθεί με τα υπόλοιπα μηνύματα του ηλεκτρονικού ταχυδρομείου. Αλλά πώς το SpamPal αναγνωρίζει τι είναι spam και τι δεν είναι; Χρησιμοποιεί καταλόγους DNSBL. Διαμορφωμένοι μετά από τους διάσημους ΧΑΡΤΕΣ RBL αυτοί είναι κατάλογοι τοποθεσιών του Διαδικτύου που διευκολύνουν με κάποιο τρόπο το spam. Οποιοδήποτε ηλεκτρονικό μήνυμα που λαμβάνεται από μια τέτοια τοποθεσία, έχει μια αυξανόμενη πιθανότητα να περιέχει spam. Μερικοί ISPs εμποδίζουν ήδη όλα τα ηλεκτρονικά μηνύματα που προέρχονται από αυτές τις τοποθεσίες, άλλοι πάλι, καθόλου.

Μπορεί ο χρήστης να επιλέξει να χρησιμοποιήσει οποιοδήποτε ή όλους τους καταλόγους DNSBL. Το SpamPal θα εξετάσει κάθε μήνυμα ηλεκτρονικού ταχυδρομείου που περνά μέσα στην ταχυδρομική θυρίδα τους, και εάν κάποιο είναι σε ένα από τους καταλόγους DNSBL μπορεί να επιλέξει έπειτα αν το μήνυμα θα χαρακτηριστεί σαν spam.

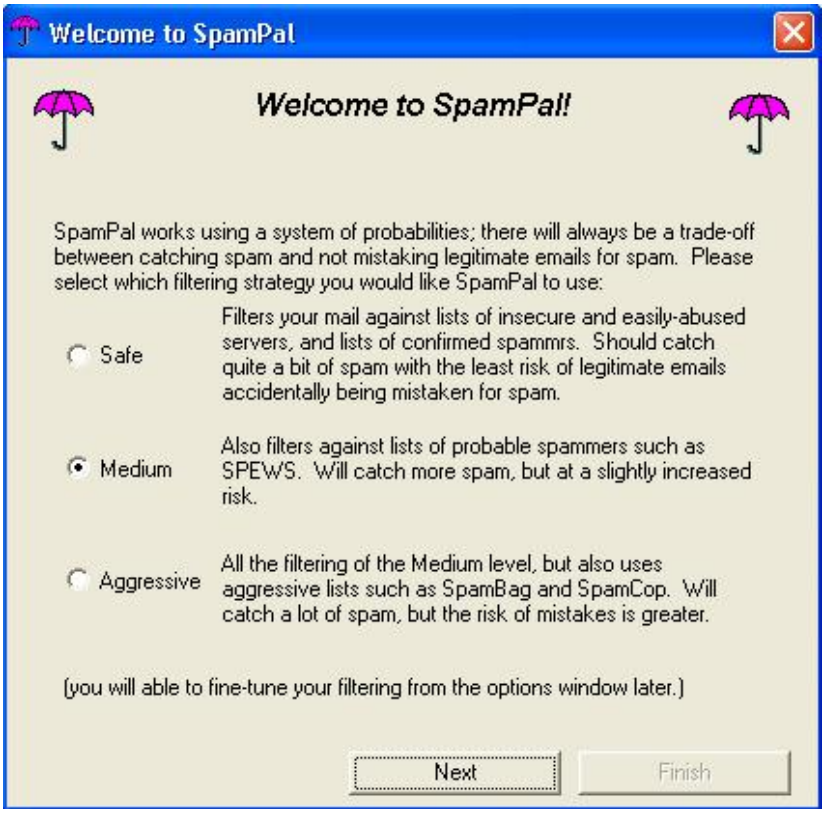
Βήμα 1: Εκκινώντας το πρόγραμμα Spam Pal

Την πρώτη φορά που εκκινούμε το Spam Pal θα δούμε το ακόλουθο παράθυρο

ΣΗΜΕΙΩΣΗ 1: Standard Ports

Μπορεί σε αυτό το σημείο να εμφανιστεί μήνυμα σφάλματος ότι το Spam Pal δεν είναι ικανό να " ακούσει " το standard POP3 port. Σεν θα πρέπει να ανησυχήσομε . Άπλα γράφουμε το port number που μας υποδεικνύει το Spam Pal και συνεχίζουμε με τον οδηγό. Αυτό το μήνυμα σημαίνει ότι το Spam Pal χρησιμοποιεί Port 1110 αντί 110. Δεν χρειάζεται να το εισάγουμε στο Spam Pal επειδή είδη το ξέρει και χρησιμοποιεί Port 110. Αντιθέτως πρέπει να το εισάγουμε στο πρόγραμμα E-mail που έχουμε (Π.χ. Το Outlook Express) να χρησιμοποιήσει Port 1110 αντί 110.

Στην συνέχεια επιλέγουμε το επίπεδο φιλτραρίσματος που θα πρέπει να εκκινεί το Spam Pal, το εξ ορισμού επίπεδο είναι το Medium ωστόσο μπορείτε να επιλέξετε το Safe για μεγαλύτερη ασφάλεια.



ΣΗΜΕΙΩΣΗ 2: Στρατηγική φιλτραρίσματος

Το επίπεδο φιλτραρίσματος που επιλέξαμε παραπάνω μπορεί να αλλαχτεί στην συνέχεια μέσα απ το πρόγραμμα

Όταν το Spam Pal εγκατασταθεί θα εκτελεσθεί αυτόματα θα πρέπει να δούμε το παρακάτω εικονίδιο.

<u>Βήμα 2:Προετοιμασία του προγράμματος E-mail</u>

Σ’αυτό το σημείο θα πρέπει να προετοιμάσουμε το Spam Pal και να διαμορφώσομε το πρόγραμμα E-mail έτσι ώστε όλα τα e-mail να λαμβάνονται διαμέσου του Spam Pal POP3/IMAP4 Proxy αντί να λαμβάνονται διαμέσου του POP3 Server του ISP μας. Εάν θέλουμε να χρησιμοποιήσουμε το Hotmail ή το Yahoo τότε θα πρέπει να χρησιμοποιήσουμε επιπρόσθετα τις εφαρμογές Hotmail Popper και YahooPops αντίστοιχα.

Οι επόμενες γενικές οδηγίες μπορούν να χρησιμοποιηθούν για την διαμόρφωση του προγράμματος

Παράδειγμα

Εάν οι πρότυπες τιμές είναι:

Host: your.mailserver.com
Username: fred.bloggs

Τότε στο παράδειγμα θα αλλαχτούν σε

Host: 127.0.0.1
Username: fred.bloggs@your.mailserver.com

Για παράδειγμα προτού χρησιμοποιήσουμε το SPAM Pal η διαμόρφωση του προγράμματος E-mail θα πρέπει να είναι κάπως έτσι:

POP Server:	mail.btopenworld.com	Port: 110
Username:	my_login_name	
Password:	********	

Έπειτα η διαμόρφωση του προγράμματος e-mail για παράδειγμα θα είναι :

POP Server:	127.0.0.1	Port: 110
Username:	my_login_name@mail.btopenworld.com	
Password:	********	

ΤΥΠΙΚΑ ΠΑΡΑΔΕΙΡΜΑΤΑ POP3 Server (Να μην χρησιμοποιούνται απευθείας)

ΣΗΜΕΙΩΣΗ 3: Το παραπάνω " Incoming POP3 Server Name " μπορεί να αποκαλείται

Incoming Mail Server, POP3 server, POP3 Username ή Account Name ανάλογα με το πρόγραμμα e-mail που διαθέτουμε. Επίσης υπάρχουν δυο τρόποι για να καθορίσουμε το όνομα του τοπικού server,οπού σημαίνει ακριβώς το ίδιο πράγμα (αλλά σε ένα σύστημα μόνο ένα από αυτά θα λειτουργήσει): localhost ή 127.0.0.1

Στην συνέχεια κάνουμε κλικ στο Send/Receive του προγράμματος e-mail.

ΣΗΜΕΙΩΣΗ 4: Εάν εμπλακεί το firewall μας είναι απώλητος φυσιολογικό. Αυτό που έχουμε να κάνουμε είναι διαμορφώσουμε το Firewall έτσι ώστε να επιτρέψει στο Spam Pal πρόσβαση στο internet.

Πλέον θα λαμβάνουμε φυσιολογικά e-mail, ωστόσο εάν το Spam Pal θεωρεί ότι ένα e-mail είναι spam τότε η πριν την θεματική ενότητα του κάθε μηνύματος θα εμφανίζεται η λέξη ” **SPAM** ” πρώτη. Επιπλέον μια επικεφαλίδα θα προστεθεί στο μήνυμα “ X-SpamPal: SPAM “

From: i_am_a@spammer.co.uk
To: yourname@yourisp.co.uk
Subject: **SPAM** FREE $ FOR YOU !!!
Date: Tue, 24 Jun 2003 13:30:40 +0100
X-SpamPal: SPAM SPCOP xxx.xxx.xxx.xxx

Για να ξεχωρίσουμε αυτό το spam απ το inbox πρέπει να διαμορφώσουμε έναν κανόνα για τα μηνύματα όπου θα πρέπει να μεταφέρει τα Spam μηνύματα μέσα σε έναν spamtrap φάκελο.

Πόσο κοστίζει:

Το SpamPal είναι ελεύθερο λογισμικό (δωρεάν) που μπορεί να το «κατεβάσει» κάποιος ελεύθερα και να το εγκαταστήσει στο PC του. Δεν είναι μια δοκιμαστική έκδοση η οποία έχει σαν στόχο να βάλει σε πειρασμό κάποιους να αγοράσουν μια «πλήρη» αλλά ακριβή έκδοση του λογισμικού, ή μια συσκευασία

που περιέχει spyware για να κλέψει προσωπικά δεδομένα σας. Η πλήρης έκδοση του λογισμικού SpamPal μπορεί να «κατέβει» και να χρησιμοποιηθεί χωρίς καταβολή χρηματικού ποσού και χωρίς καμιά δέσμευση.

4.5.5 Spamihilator

Το Spamihilator εφαρμόζεται μεταξύ του πελάτη ηλεκτρονικού ταχυδρομείου και του Διαδικτύου και εξετάζει κάθε εισερχόμενο ηλεκτρονικό μήνυμα. Με την βοήθειά του τα άχρηστα μηνύματα spam (junk) φιλτράρονται και διαγράφονται. Αυτή η διαδικασία εκτελείται εξ ολοκλήρου στο υπόβαθρο.

Το φίλτρο εκμάθησης (Μπεϋζιανό φίλτρο) χρησιμοποιεί τους κανόνες του Thomas Bayes (Άγγλος μαθηματικός, 18ος αιώνας) και υπολογίζει για κάθε ηλεκτρονικό μήνυμα την πιθανότητα να περιέχει spam. Επίσης, μπορεί κάποιος να εκπαιδεύσει αυτό το φίλτρο. Έτσι θα αυξάνεται συνεχώς η ικανότητά του να αναγνωρίζει το spam. Επιπλέον το Spamihilator χρησιμοποιεί φίλτρα που ψάχνουν τα μηνύματα για γνωστές λέξεις κλειδιά.

Το Spamihilator δέχεται επίσης και Plug ins (διάφορα πρόσθετα) τα οποία του προσδίδουν ακόμη μεγαλύτερη ικανότητα αναγνώρισης.

ΠΕΡΙΓΡΑΦΗ

1. Το Spamihilator είναι ένα anti-spam εργαλείο για τα πρωτόκολλα POP και IMAP, υποστηρίζει τις ασφαλείς συνδέσεις TLS/SSL.
2. Το Spamihilator εργάζεται χωρίς proxy ως πληρεξούσιο μεταξύ του πελάτη ηλεκτρονικού ταχυδρομείου και του κεντρικού υπολογιστή ηλεκτρονικού ταχυδρομείου.

3. Φιλτράρει το spam προτού να εισαχθεί στο inbox, και μπορεί να διαγράφει τα άχρηστα μηνύματα χωρίς να τα "κατεβάζει".
4. Το spam που έχει εντοπιστεί, μπορεί να κοιταχτεί βιαστικά και να διαβαστεί και τα ωφέλιμα μηνύματα μπορούν να ανακτηθούν εύκολα.
5. Το Spamihilator χρησιμοποιεί τις μαύρες και άσπρες λίστες φίλτρων και ένα κατανεμημένο ληξιαρχείο για spam που έχουν αναγνωριστεί.
6. Επιπλέον μπορεί να χρησιμοποιήσει τις Μπεϋζιανές στατιστικές για να επιτύχει ένα υψηλότερο ποσοστό ανίχνευσης.
7. Το Spamihilator κρατά όλο το πρόσφατο ταχυδρομείο για την εύκολη κατάρτιση των προσαρμοστικών φίλτρων
8. Το Spamihilator συλλέγει και επιδεικνύει τις καθημερινές στατιστικές ανιχνευμένου spam.
9. το Spamihilator μπορεί να επεκταθεί με PLUGINS (όπως π.χ. αυτόματη ανακοίνωση μηνυμάτων, παραδοσιακά φίλτρα και άλλα)

Το Spamihilator υποστηρίζει τα Windows 9x/ME/NT/2000/3/XP.

4.6 Τρόποι προστασίας από ανεπιθύμητη αλληλογραφία

1. Ο χρήστης δεν πρέπει να απαντάει σε spam mail. Στα άτομα που στέλνουν spam μηνύματα, μια απάντηση ή ένα "hit" ανάμεσα σε χιλιάδες αποστολές μηνυμάτων είναι αρκετό για να δικαιώσει αυτή τους την πράξη. αυτό απλώς θα επιβεβαιώσει την εγκυρότητα της ηλεκτρονικής διεύθυνσης τους...
2. Ο χρήστης ποτέ δεν ακολουθεί τις οδηγίες ενός spam μηνύματος π.χ. να απαντήσει με την λέξη "remove", εκτός αν εμπιστευτεί τον αποστολέα που τους στέλνει το μήνυμα. Συνήθως οι οδηγίες αυτές αποτελούν μια τακτική για να προκαλέσει την αντίδραση τους στο μήνυμα και με αυτόν τον τρόπο θα

ειδοποιηθεί ο αποστολέας ότι η ηλεκτρονική τους διεύθυνση είναι ανοιχτή και διαθέσιμη ως προς τη λήψη ηλεκτρονικών μηνυμάτων, αυξάνοντας κατά πολύ την αξία της. Αν απαντήσει, η ηλεκτρονική τους διεύθυνση μπορεί να προστεθεί και σε άλλες λίστες, έχοντας ως αποτέλεσμα περισσότερο spamming.

3. Ο χρήστης ποτέ δεν πρέπει να κάνει κλικ σε ένα url ή διεύθυνση που περιέχεται σε ένα spam μήνυμα. Με αυτόν τον τρόπο μπορεί να ενημερωθεί η συγκεκριμένη ιστοσελίδα για την ισχύ της ηλεκτρονικής διεύθυνσης, έχοντας ως αποτέλεσμα περισσότερο spamming.

4. Να σβήνει όλα τα μηνύματα που εμφανίζονται να προωθούν κάτι για το οποίο δεν έχει ζητήσει πληροφορίες. Τέτοιου είδους μηνύματα μπορεί να ανήκουν στις κατηγορίες των spam ή junk μηνυμάτων. Μερικές εταιρίες αποστέλλουν ένα μεγάλο αριθμό ηλεκτρονικών μηνυμάτων, με σκοπό την προσέλκυση νέων πελατών, τα οποία όμως είναι ενοχλητικά και η διαγραφή τους χρονοβόρα.

5. Να επιλέγει την επιλογή "unsubscribe" μόνο από λίστες που φαίνονται νόμιμες. Ορισμένες φορές η επιλογή αυτή χρησιμοποιείται για τη συλλογή ή επιβεβαίωση επιπρόσθετων ηλεκτρονικών διευθύνσεων. Για το λόγο αυτό η διαγραφή από μια λίστα σε ορισμένες περιπτώσεις μπορεί να προκαλέσει περισσότερο spamming. Σε αυτές τις περιπτώσεις είναι προτιμότερο να συνεχίσει να σβήνει αυτά τα μηνύματα από το mailbox.

6. Να μην προωθεί τα spam μηνύματα σε γνωστούς και φίλους.

7. Να μην αφήνει ελκυστικούς τίτλους μηνυμάτων, όπως "urgent and confidential" ή "i have money for you", να τους δελεάσουν.

8. Χρησιμοποιεί τις λειτουργίες λογισμικού διαχείρισης αυτόματης διαγραφής ηλεκτρονικής αλληλογραφίας. Αρκετά προγράμματα επιτρέπουν την δημιουργία κανόνων αυτόματης διαγραφής. Χρησιμοποιώντας αυτή τη λειτουργία θα μειωθεί ο χρόνος που καταναλώνεται στη διαγραφή των spam μηνυμάτων.

9. Πληκτρολογεί την ηλεκτρονική τους διεύθυνση σε μια μηχανή αναζήτησης π.χ. google για να βρεί την ιστοσελίδα που τυχόν διαθέτει τη διεύθυνση τους και ζητά από τους υπεύθυνους αυτών να την αφαιρέσουν.
10. Δεν στέλνει δωρεάν ευχετήριες κάρτες από το διαδίκτυο. Ας αναρωτηθεί κανείς για ποιον λόγο είναι δωρεάν και πως αποκτώνται έσοδα με το να αποθηκεύεται η ηλεκτρονική του διεύθυνση, καθώς και αυτή του παραλήπτη και κατόπιν αυτές μεταπωλούνται στους "onlineadvertisers"
Να κρατάει κρυφά τα στοιχεία που έχει δώσει σε υπηρεσίες όπως intant messenger, ICQ κτλ οι οποίες αποτελούν περιοχές που εκμεταλλεύονται οι spammers. Πρέπει να επιβεβαιώσει κανείς ότι το προφίλ τους παραμένει κρυφό στους υπόλοιπους χρηστές όταν χρησιμοποιείται κάποια υπηρεσία instant messaging.

4.6.1 Πως μπορούν να καταγγελθούν οι spammers.

Αν θέλει κανείς να πάρει δραστικά μέτρα εναντίον αυτών που τον ενοχλούν με τα αυτόκλητα διαφημιστικά τους μηνύματα, δεν υπάρχει άλλος δρόμος από αυτόν της καταγγελίας. Σε προηγούμενη παράγραφο αναφέρθηκαν τρεις διευθύνσεις: Α) της Αρχής Προστασίας Προσωπικών Δεδομένων, Β) της γραμμής προστασίας Safenet και Γ) της διεθνούς antispam ένωσης Spamcop.

Μπορεί κανείς να καταγγείλει απευθείας τον spammer στον ISP που χρησιμοποιεί, π.χ. στο Yahoo, στο Hotmail κ.ά. (ISP: Internet Service Provider: εταιρείες παροχής υπηρεσιών διαδικτύου). Οι spammer ανοίγουν δωρεάν λογαριασμούς webmail και κάνουν μέσω αυτών τη δουλειά τους. Γνωρίζουν ότι ενοχλούν όπως επίσης γνωρίζουν ότι κινδυνεύουν, γι’ αυτό και παίρνουν τα μέτρα τους. Πολλές φορές χρησιμοποιούν πλασματικές ηλεκτρονικές διευθύνσεις που

έχουν υποκλέψει. Αρκετοί χρήστες του διαδικτύου έχουν πέσει θύματα, όταν είδαν χιλιάδες μηνύματα διαμαρτυρίας από κάθε γωνιά της γης να γεμίζει το φάκελο εισερχόμενων (inbox) τους, επειδή θεωρήθηκαν ως spammer, ενώ η αλήθεια ήταν ότι κάποιοι επαγγελματίες του είδους έκαναν τη δουλειά τους χρησιμοποιώντας τις ηλεκτρονικές διευθύνσεις τους. Υπάρχουν όλα τα προγράμματα και οι τεχνικές για να παρουσιαστούν σαν spammer, έστω κι αν δεν έχουν ιδέα για το έγκλημά τους (ακόμα και για το περί τίνος πρόκειται…). Βέβαια, δεν έχουν καμία ποινική ή άλλη ευθύνη, κι αυτό γιατί πολύ εύκολα οι ISP (και όχι μόνο) καταλαβαίνουν ότι είναι άμοιροι ευθυνών. Το πρόβλημα είναι ο κυκεώνας των διαμαρτυριών που προαναφέραμε.

Συχνά, όμως, τα πράγματα δεν είναι τόσο μπερδεμένα. Δεν είναι όλοι οι spammer εξαιρετικοί "επαγγελματίες" του είδους και πολύ συχνά κάνουν λάθη (άλλωστε, άνθρωποι είναι κι αυτοί όπως όλοι μας…). Λάθη που μπορούμε να τα εκμεταλλευτούμε και αργά ή γρήγορα να τους θέσουμε ενώπιον των ευθυνών τους. Για να μπούνε όμως στο επίπεδο της καταγγελίας, θα πρέπει να αναγνωρίζουμε τις κεφαλίδες (headers) των μηνυμάτων που λαμβάνονται, και αυτό δεν είναι και τόσο δύσκολο. Όλα τα προγράμματα (πελάτες) που χρησιμοποιούνται για λήψη ηλεκτρονικού ταχυδρομείου (π.χ. το Outlook Express) έχουν τη δυνατότητα αναγνώρισης των headers. Αν θέλει κανείς να μάθει τον τρόπο, επικοινωνεί με τον πάροχο της σύνδεσής του και θα διαπιστώσει ότι μέσα σε λίγα λεπτά θα γνωρίζει πώς να κάνει την καταγγελία του. Από τη στιγμή που μπορεί κανείς να αναγνωρίσει τις κεφαλίδες των μηνυμάτων, θα έχει και τη δυνατότητα να καταγγείλει τα ανεπιθύμητα μηνύματα στους ISP (ή όπου αλλού). Όλοι οι σοβαροί ISP απαγορεύουν το spamming – και αν πληροφορηθούν ότι κάποιος χρησιμοποιεί τους λογαριασμούς τους γι' αυτό το σκοπό, τον διαγράφουν αμέσως. Οι ISP διαθέτουν κάποια ηλεκτρονική διεύθυνση για να δέχονται τις καταγγελίες του είδους – συνήθως το πρώτο συνθετικό της είναι η λέξη abuse. Για παράδειγμα, αν

τα μηνύματα spam που φθάνουν στο ηλεκτρονικό ταχυδρομείο κάποιου χρήστη προέρχονται από κάποιο λογαριασμό του yahoo, θα αποστείλει το μήνυμα μαζί με τις κεφαλίδες του στη διεύθυνση: abuse@yahoo.com Αν έρχονται από λογαριασμό Hotmail, η διεύθυνση στην οποία θα κάνει την καταγγελία του θα είναι abuse@hotmail.com

Δείτε τώρα την απάντηση του Yahoo σε καταγγελία που κάναμε πριν από λίγες ημέρες:

“Hello. Thank you for writing to Yahoo! Mail. In this particular case, we have taken appropriate action against the Yahoo! account in question, as per our Terms of Service (TOS). For further details about the Yahoo! TOS, you can visit: http://docs.yahoo.com/info/terms/”

Με δυο λόγια, ο λογαριασμός του spammer έπαψε να υφίσταται.

Το ίδιο συνέβη και με κάποιον spammer που, μόλις σήμερα, μας πρότεινε να κάνουμε την τύχη μας παίζοντας σ’ ένα διαδικτυακό καζίνο. Το μόνο προαπαιτούμενο ήταν να ανοίξουμε ένα πρόγραμμα που ήταν συνημμένο σε αρχείο. Το πρόγραμμα όμως αυτό δεν ήταν τίποτε άλλο από έναν dialer (τα προγράμματα αυτά οδηγούν σε υπέρογκες χρεώσεις ανά λεπτό σύνδεσης). Ας αναρωτηθεί κανείς τι θα είχε συμβεί αν έπαιρνε αυτό το μήνυμα κάποιο μικρό παιδί που θα ήθελε να δοκιμάσει ένα ακόμα παιχνίδι. “Κυνηγήσαμε” τον συγκεκριμένο spammer, που κρυβόταν πίσω από ψεύτικες διευθύνσεις ώστε να μην είναι εύκολα αναγνωρίσιμη η πραγματική του διεύθυνση. Ενώ λοιπόν φαινόταν ότι επρόκειτο για έναν αλλοδαπό spammer, στην πραγματικότητα ήταν ένας καλός συμπατριώτης, που “μας σκέφτηκε” μέσω της Otenet. Βρήκαμε λοιπόν

τα στοιχεία που οδηγούσαν σε αυτόν και στη συνέχεια στείλαμε μια καταγγελία στην Otenet. Η απάντηση της εταιρίας ήταν άμεση, την οποία και παραθέτουμε:

"Αξιότιμοι κύριοι, Θα θέλαμε να σας ευχαριστήσουμε που επικοινωνήσατε με την OTEnet. Έχουμε εντοπίσει τον εμπλεκόμενο λογαριασμό κι έχουμε προβεί στις δέουσες ενέργειες, όπως αυτές ορίζονται από τους όρους χρήσης του δικτύου μας. Με εκτίμηση, Γενική Εμπορική Διεύθυνση, Τμήμα Εξυπηρέτησης Πελατών OTEnet (NEXT2U), Network Abuse Team"

Ο αγώνας ενάντια στο spamming δεν είναι εύκολος. Χρειάζεται συνεχής προσπάθεια και πάνω απ' όλα ενημέρωση, Αν οι χρήστες ακολουθήσουν τις οδηγίες που προαναφέραμε, θα δουν τις ποσότητες του spam που λαμβάνουν να περιορίζονται σε πολύ μεγάλο βαθμό ή ακόμα και να εξαλείφονται. Ασφαλώς, και επειδή το spamming παραμένει ιδιαίτερα αποδοτικό για τους δημιουργούς του, θα εξακολουθήσει να αποτελεί πρόβλημα καθώς νέες τεχνικές θα επινοούνται και νέοι spammer θα προσπαθούν να "επικοινωνήσουν" μαζί μας. Υπάρχουν όμως οι τρόποι για να τους αντιμετωπίσουμε και - γιατί όχι; - να τους δώσουμε ένα καλό μάθημα. Υπάρχουν κι άλλα όπλα…


SPAM

ΚΕΦΑΛΑΙΟ 5^{ο} :ΝΟΜΟΘΕΣΙΑ ΚΑΤΑ ΤΟΥ SPAM

5.1 Πρόχειροι Κανονισμοί κατά του Spamming , αυτοπεριορισμοί.

Μέχρι το 1996 οι κοινωνικές πιέσεις ήταν η μοναδική προσέγγιση για την αντιμετώπιση του spam. Ειδικότερα, κατά τα πρώτα βήματα του Internet, άτυποι κανόνες ευγένειας και κάποιες χαλαρά εφαρμοσμένες άδειες επιτρεπόμενης χρήσης του Internet, αρκούσαν από μόνα τους για να απαγορεύσουν ή τουλάχιστον να αποθαρρύνουν την εμπορική χρήση του. Επομένως το spam και κατά ευρύτερη έννοια όλη η εμπορική δραστηριότητα στο Διαδίκτυο είχε, κατά κάποιο τρόπο, στιγματιστεί σε τέτοιο βαθμό ώστε να αποτρέπει τους χρήστες να σκέφτονται να αναλάβουν τέτοιου είδους δραστηριότητες. Καθόσον όμως οι εμπορικές δραστηριότητες γίνονταν περισσότερο αποδεκτές στο Internet, οι διαδικτυακοί νόμοι και οι άδειες άρχισαν σταδιακά να εστιάζουν και να αναφέρονται στα νέα ζητήματα που προέκυπταν από την νέα αυτή χρήση, συμπεριλαμβανομένου και του spam.

Σήμερα σχεδόν όλοι οι πάροχοι υπηρεσιών Internet (“ISPs”) υιοθετούν πολιτικές που απαγορεύουν την χρήση των υπηρεσιών τους για την αποστολή spam. Επιπλέον, αυτοί που κάνουν χρήση του spam όπως και οι πάροχοι Internet που το επιτρέπουν, μπαίνουν σε μαύρη λίστα και απομονώνονται, παρόμοια με αυτούς που παρανομούν στον πραγματικό κόσμο. Βιομηχανικές ομάδες, που αντιπροσωπεύουν τους εμπόρους και τους ISPs, προσπαθούν να απευθυνθούν στο πρόβλημα του spam με αυτόνομες ενέργειες. Για παράδειγμα, τα μέλη του Συνεταιρισμού Άμεσου Marketing (“DMA”), ένας συνεταιρισμός ο οποίος αντιπροσωπεύει χρήστες και πάροχοι που έχουν να κάνουν με άμεσο, μέσω βάσεων δεδομένων ή αλληλεπιδραστικό marketing, είναι υποχρεωμένοι να

συμμορφώνονται με την συμφωνία τους με το DMA περί σεβασμού της μυστικότητας. Αυτή τους απαγορεύει να στέλνουν ανεπιθύμητα από τον δέκτη εμπορικά μηνύματα προς διευθύνσεις οι οποίες είναι καταχωρημένες στην βάση δεδομένων του DMA. Οι οδηγίες του Internet Alliance κατά του spam υποδεικνύουν ότι οι έμποροι δεν θα πρέπει να συλλέγουν διευθύνσεις ηλεκτρονικών ταχυδρομείων σε online συζητήσεις με σκοπό να στέλνουν διαφημιστικά μηνύματα, εκτός και αν αυτό τους επιτρέπεται από τους χρήστες. Η AIM ("Association for Interactive Media") έχει δηλώσει την αντίθεσή της για το spam, ωστόσο χωρίς να απαγορεύσει την χρήση του.

5.1.1 Προβλήματα αυτοπεριορισμών

Οι ανεπίσημες δυνάμεις, όπως η κοινωνικές πιέσεις και οι αυτοπεριορισμοί της βιομηχανίας, είχαν μικρή επιρροή στο spam. Το spamming θεωρούνταν πάντα μια περιθωριακή δραστηριότητα και οι κοινωνικές πιέσεις έτειναν πάντα να είναι σχετικά ανεπαρκείς στο να περιορίζουν εκείνους που ενεργούν στο περιθώριο της κοινωνίας. Επιπλέον οι κανόνες ευγένειας, γενικώς, δεν έχουν μηχανισμούς ενδυνάμωσης και οι ISPs βρίσκουν πολύ μικρή επιτυχία στο να επιβάλουν τις, αποδεκτές κατά τα άλλα, πολιτικές χρήσης τους σε χρήστες όπως οι spammers όταν αυτοί προσπαθήσουν να στείλουν μηνύματα στους εγγεγραμμένους των ISPs.

Ωστόσο είναι αλήθεια ότι το spam παραμένει στιγματισμένο και αυτό το στίγμα έχει βοηθήσει στην ανίχνευση του ίχνους του spam. Οι περισσότεροι χρήστες του Διαδικτύου δεν ενδίδουν στο spam όχι τόσο πολύ εξαιτίας αυτού του στίγματος όσο για το ότι οι πάροχοι Internet απαγορεύουν την χρήση του. Παρόλα

αυτά η συνεχής εξάπλωση του ηλεκτρονικού εμπορίου οδηγεί όλο και περισσότερο κόσμο στο να πειραματιστεί, τουλάχιστον, με το spam και το στίγμα του φαίνεται ολοένα να εξαφανίζεται. Οι εθελοντικές προσπάθειες της βιομηχανίας απέτυχαν για πολλούς λόγους, πιθανόν ο σπουδαιότερος να είναι γιατί απλά οι spammers αδιαφόρησαν και γιατί δεν είχαν συμφέρον να συμμετάσχουν σε τέτοιες προσπάθειες.

5.1.2 Πρώτες Νομικές Προσεγγίσεις

Πολλές μηνύσεις για περιπτώσεις spam έχουν ασκηθεί τα τελευταία χρόνια και ένας αριθμός από αυτές δικαιώθηκαν. Οι περισσότερες περιπτώσεις μέχρι σήμερα, ωστόσο, αφορούσαν στο λεγόμενο ‘ενοχλητικό ’ spam, δηλαδή μηνύματα με πλαστές επικεφαλίδες, μη εξουσιοδοτημένη εμπλοκή τρίτων και επίμονη άρνηση εξυπηρέτησης αιτήσεων για τερματισμό αποστολών. Επίσης σχεδόν όλες αυτές οι μηνύσεις εμφανίστηκαν σε περιπτώσεις που είχαν να κάνουν με το marketing.

Είναι λογικό ότι οι πιο ακραίες μορφές του spam είναι πιο πιθανές να καταλήξουν σε αγωγές, όμως οι μέχρι τώρα υποθέσεις έχουν συντελέσει λίγο στο να διευκρινιστεί η υπόσταση του νόμιμου spam. Ταυτόχρονα οι νομοθέτες επιδιώκουν να ανακαλύψουν όλο και περισσότερους τρόπους για να ελέγξουν το spam σε επίπεδο τόσο χρήστη όσο και πολιτείας. Μέχρι στιγμής έχουν παρουσιαστεί αρκετές προτάσεις εναντίον του spam στο Κογκρέσο των Η.Π.Α. ενώ πολλές Πολιτείες έχουν περάσει νομοθεσία κατά του spam, με ένα χαρακτηριστικό παράδειγμα την καθολική απαγόρευση στα εμπορικά διαφημιστικά ηλεκτρονικά μηνύματα που αποστέλλονται χωρίς την άδεια από τον

παραλήπτη. Η Ευρωπαϊκή ένωση από την πλευρά της εξετάζει το ενδεχόμενο να ενεργοποιήσει νομοθεσία εναντίον του spam.

5.1.3 Νομοθεσίες – η αρχή.

Το πρώτο νομοσχέδιο εναντίον του spam που εμφανίστηκε πήρε αφορμή από την μήνυση που έκανε ο Robert Arkow εναντίον της εταιρίας Compuserve στις αρχές του 1995. Ισχυρίστηκε ότι τα διαφημιστικά μηνύματα που δέχονταν από την εταιρία παραβίαζαν τον γενικότερο συνταγματικό νόμο κατά των διαφημίσεων οι οποίες γίνονταν χωρίς την συγκατάθεση του αποδέκτη, δηλαδή υποστήριξε ότι ο συγκεκριμένος νόμος κάλυπτε και τους ηλεκτρονικούς υπολογιστές που μπορούσαν να στείλουν και να λάβουν ηλεκτρονικά μηνύματα. Τελικά οι δύο πλευρές κατέληξαν σε συμβιβαστική λύση εκτός δικαστηρίου και έκτοτε η εφαρμογή των συγκεκριμένων νόμων στα ηλεκτρονικά μηνύματα δεν διευκρινίστηκε ούτε ρυθμίστηκε επισήμως. Μετά την προσφυγή του Arkow υπήρξε ένας σχετικά μικρός αριθμός μεμονωμένων αγωγών που είχαν να κάνουν με το spam. Οι περισσότερες δίκες διεξήχθησαν ύστερα από ενέργειες των διαφόρων Internet Service Providers οι οποίοι διαπίστωναν μεγάλες ποσότητες spam να αποστέλλονται στους χρήστες τους, ή από τρίτους οι οποίοι έβλεπαν το όνομά τους ή τις υπηρεσίες τους να βρίσκονται στο στόχαστρο των spammers.

5.1.4 Δράση από Διακομιστές Υπηρεσιών.

Οι πάροχοι υπηρεσιών έχουν κατά καιρούς μηνύσει τους spammers χρησιμοποιώντας διάφορες νομικές προσεγγίσεις. Η πιο συνηθισμένη είναι η

αυθαίρετη χρήση των υπηρεσιών τους από τους spammers, ισχυριζόμενοι καταπάτηση της περιουσίας τους ή παραποίηση των υπηρεσιών που προσφέρουν. Το μεν επιχείρημα περί καταπάτησης έχει χρησιμοποιηθεί σε πολλές υποθέσεις spam ενώ αυτό της παραποίησης συνήθως αποφεύγεται, γιατί απαιτεί εμβάθυνση σε πιο εξεζητημένα νομικά ζητήματα περί ιδιοκτησίας.

Το αδίκημα της καταπάτησης περιουσίας διαπράττεται όταν ένα άτομο δραστηριοποιείται με ξένη περιουσία χωρίς την άδεια από τον ιδιοκτήτη. Ο καταπατητής είναι υπόλογος στην δικαιοσύνη όταν μειώνει την αξία της ιδιοκτησίας ή προκαλεί προβλήματα στην τρέχουσα κατάστασή της ή ακόμα όταν ο νόμιμος κάτοχός της την στερείται για ένα ουσιαστικό χρονικό διάστημα. Οποιοσδήποτε, συμπεριλαμβανομένου και του spammer, επιθυμεί να στείλει ένα ηλεκτρονικό μήνυμα προς έναν εγγεγραμμένο ενός ISP θα πρέπει υποχρεωτικά να κάνει χρήση του SMTP server του ISP. Ωστόσο η καθημερινή χρήση του SMTP server για νόμιμη διακίνηση μηνυμάτων είναι καθόλα επιτρεπτή και πολύ σπάνια θα προκαλέσει την ζημιά εκείνη ώστε να επιφέρει νομική ευθύνη σε αυτόν που θα την κάνει. Για αυτό το λόγο η προσέγγιση της καταπάτησης περιουσίας φαίνεται να είναι περισσότερο αποτελεσματική σε περιπτώσεις όπου ο Διακομιστής Υπηρεσιών έχει προηγουμένως επικοινωνήσει με τον spammer προειδοποιώντας τον ότι η χρήση των υπηρεσιών του δεν του επιτρέπεται και εκείνος το έχει επανειλημμένα αγνοήσει, προξενώντας ζημιά στο σύστημα του Διακομιστή Υπηρεσιών.

Μια άλλη νομική προσέγγιση που επιχειρήθηκε από τους Διακομιστες Υπηρεσιών είναι οι ισχυρισμοί περί αισχροκέρδειας και κατάχρησης των υπηρεσιών τους από την πλευρά των spammers. Για παράδειγμα η America Online έχει υποστηρίξει ότι οι spammers έχουν καταχραστεί τις βασικές υπηρεσίες που προσφέρει. Πιο συγκεκριμένα, υποστηρίζει ότι όπως οι διαφημιστές πληρώνουν την εταιρία προς αντάλλαγμα για την εμφάνιση διαφημίσεων στις οθόνες των

πελατών της έτσι και οι spammers θα έπρεπε να κάνουν κάτι αντίστοιχο. Σε αντίθεση βγάζουν κέρδος μέσω των υπηρεσιών της εταιρίας παρακάμπτοντας την παραπάνω διαδικασία. Και άλλοι διάφοροι Διακομιστές έχουν διατυπώσει παρόμοια επιχειρήματα περί αισχροκέρδειας των spammers βασιζόμενοι στην κατάχρηση των υπολογιστικών πόρων τους. Η χρήση του SMTP server ή άλλων υπηρεσιών ενός διακομιστή υπηρεσιών από τους spammers, παρ' όλη την απαγόρευση από τον διακομιστή, μπορεί να οδηγήσει, στις Η.Π.Α., έναν spammer στην δικαιοσύνη με κατηγορίες παραβίασης τόσο πολιτειακών όσο και ομοσπονδιακών νόμων. Για παράδειγμα, η Πράξη περί Ομοσπονδιακής απάτης μέσω Η/Υ απαγορεύει στον οποιονδήποτε να παίρνει πληροφορίες είτε να προκαλεί ζημιά που προκαλείται μέσω πρόσβασης σε Η/Υ χωρίς άδεια, αποδίδοντας ποινές βαρύτητας εγκλήματος και λαμβάνοντας νομική δράση προστασίας των αδικημένων πλευρών. Συχνά παρατηρείται οι spammers να κάνουν χρήση του ονόματος του Διακομιστή Υπηρεσιών στις επικεφαλίδες των μηνύματα που στέλνουν. Αυτή η τακτική ακολουθείται για διάφορους λόγους. Ένας είναι για να κρύψουν την πραγματική προέλευση του μηνύματος από τον παραλήπτη ώστε να τον ξεγελάσουν. Επίσης το κάνουν ώστε να μην εντοπιστούν, κατά το φιλτράρισμα των μηνυμάτων τα μηνύματά τους από τους Διακομιστές και να μπλοκαριστούν, και ένας τρίτος λόγος να ανακατευθύνουν τα ενδεχόμενα παράπονα των πελατών προς τους ίδιους τους Διακομιστές και έτσι να τα αποφύγουν οι ίδιοι. Αυτή η πρακτική είναι κατά κάποια έννοια πιο επιβλαβής στον παραλήπτη και από την πρακτική της παρέμβασης του spammer ανάμεσα στον παραλήπτη και τον διακομιστή διότι το θύμα δεν μπορεί να κάνει και πολλά ώστε να αποτρέψει τον spammer από το να πάρει τα προσωπικά του δεδομένα και την ταυτότητα του και να τα καταχραστεί. Συχνά, οι Διακόμισες υπηρεσιών, οι οποίοι αντιλαμβάνονται τα ονόματά τους σε πλαστογραφημένες επικεφαλίδες τέτοιων μηνυμάτων, κάνουν διάφορες αγωγές εναντίον των spammers, ισχυριζόμενοι

αθέμιτο ανταγωνισμό και παραβίαση του Copyright του ονόματός τους. Εκτός από αυτά τα επιχειρήματα, έχουν ακολουθηθεί από τους διακομιστές υπηρεσιών και άλλες μέθοδοι όπως το να ισχυριστούν ενόχληση, κατάχρηση του ονόματός τους και της ταυτότητάς τους, απάτη, δυσφήμηση, εξαπατήσιμες πρακτικές από πλευράς των spammers όπως και αμέλεια και παρεμβολή στις επαγγελματικές τους σχέσεις με τους πελάτες τους.

5.2 Νομικές ρυθμίσεις κατά του spam στις Η.Π.Α

Τα έξοδα που επιφέρει μια μήνυση σε συνδυασμό με την αδιευκρίνιστη κατάσταση που επικρατεί γύρω από την νομοθεσία που αφορά το spam, έχει οδηγήσει στις Η.Π.Α. σε επικλήσεις για να θεσπιστεί ειδική νομοθεσία η οποία θα περιορίζει ή θα απαγορεύει το spam. Συγκεκριμένα, έχουν προταθεί διάφορα, τέτοιου περιεχομένου, νομοσχέδια στο Αμερικάνικο Κογκρέσο όπως και σε νομοθέτες διαφόρων Αμερικάνικων πολιτειών ενώ πολλές πολιτείες έχουν ήδη θέση σε ισχύ ποικίλους νόμους εναντίον του spam. Ωστόσο υπάρχουν περιπτώσεις στις Η.Π.Α, όπου νομοσχέδια τα οποία προτάθηκαν από ανώτατες πολιτικές αρχές της χώρας όπως η Αμερικάνικη Γερουσία, μία από τις δύο αρχές που εκλέγουν νόμους στις ΗΠΑ, το 1998,και το House of Representatives το 2000 δεν πέρασαν ως νόμοι. Και άλλες χώρες όπως και η Ευρωπαϊκή Ένωση έχουν επίσης σκεφτεί να θέσουν νομοθετικούς περιορισμούς στο spam. Ως συμπέρασμα θα λέγαμε ότι έχουν ακολουθηθεί διάφορες προσεγγίσεις για την αντιμετώπισή του με ποικιλία στο βαθμό αυστηρότητάς τους, οι οποίες ξεκινούν από αυτές που θέτουν στους spammers απλούς περιορισμούς και φτάνουν σε εκείνες που επιβάλλουν απόλυτη απαγόρευση αποστολής εμπορικών μηνυμάτων. Οι διάφορες περιπτώσεις αναφέρονται παρακάτω

Περιπτώσεις απαγόρευσης του spam

Στην πολιτεία Delaware των Η.Π.Α. έχει τεθεί σε ισχύ ο πιο περιοριστικός νόμος κατά του spam. Η αποστολή μαζικών εμπορικών μηνυμάτων συνιστά παραβίαση του νόμου της Delaware περί Η/Υ. Η εφαρμογή του γίνεται στις περιπτώσεις όπου τέτοιου είδους μηνύματα στέλνονται από αποστολείς εκτός της πολιτείας προς δέκτες μέσα στην πολιτεία, με την προϋπόθεση ότι ο αποστολέας γνωρίζει εκ των προτέρων ότι ο παραλήπτης βρίσκεται στην Delaware. Η Πράξη περί προστασίας Δικτύων του 1997, ένα από τα δύο πρώτα νομοσχέδια που συζητήθηκαν στο Αμερικάνικο Κογκρέσο προέβλεπε την επέκταση του ομοσπονδιακού νόμου, ο οποίος απαγορεύει την αποστολή ενοχλητικών διαφημίσεων, ώστε να απευθύνεται και στις διαφημίσεις που γίνονται μέσω ηλεκτρονικών μηνυμάτων.

Ωστόσο κανένα μέχρι στιγμής ομοσπονδιακό νομοσχέδιο δεν έχει προτείνει την άμεση απαγόρευση του spam. Όσον αφορά, τώρα, την Ευρωπαϊκή Ένωση, δεν απαγορεύει την αποστολή μη ενοχλητικών εμπορικών μηνυμάτων στις ανεξάρτητες χώρες μέλη της, όμως οι χώρες ανεξάρτητα έχουν επιβάλλει νόμους προς αυτή την κατεύθυνση. Η Φινλανδία, η Γερμανία και η Ιταλία, όλες έχουν θεσπίσει νόμους που απαγορεύουν τα UCE (μη ενοχλητικά εμπορικά ηλεκτρονικά μηνύματα), ενώ η Αυστρία απαγορεύει τόσο τα UCE όσο και τα UBE (μη ενοχλητικά, μαζικής αποστολής, ηλεκτρονικά μηνύματα). Εκτός από αυτές τις χώρες και άλλες επίσης ευρωπαϊκές χώρες σκέφτονται να ενεργοποιήσουν παρόμοιους περιορισμούς. Πέρα από τις Η.Π.Α. και την Ευρωπαϊκή Ένωση δεν έχει σημειωθεί κάποια επίσημη κίνηση επιβολής απαγορεύσεων στο spam. Ακόμη και η Αυστραλία ή ο Καναδάς, δύο χώρες που θεωρούνται ότι εφαρμόζουν

αυστηρούς νόμους περί παραβίασης της ιδιωτικότητας, δεν έχουν νόμους οι οποίοι να απαγορεύουν το spam.

Επιβολή πολιτικών αντί- Spam

Οι ISPs και άλλοι διακομιστές υπηρεσιών έχουν γενικά πολιτικές που οριοθετούν και προστατεύουν τη χρήση των εγκαταστάσεών τους για διάφορους σκοπούς. Σχεδόν όλοι τους απαγορεύουν το spam. Κατά διάφορες απόψεις η χρήση τέτοιων πολιτικών μπορεί να θεωρηθεί ως μια πιο ήπια, και ίσως πιο αρεστή, εναλλακτική λύση έναντι της θέσπισης μιας ολοκληρωτικής απαγόρευσης στο spam. Το να δίνουν νομική δύναμη ξεχωριστά στους διακομιστές, προέρχεται από το ακόλουθο σκεπτικό: εάν η τοποθέτηση ενός κεντρικού υπολογιστή SMTP στο διαδίκτυο επιτρέπει στους διάφορους χρήστες να χρησιμοποιήσουν τον κεντρικό υπολογιστή για την διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου κάτω από κάποιους όρους, τότε λογικό είναι, κάθε φορά που οι όροι αυτοί παραβιάζονται, να μπορεί ο πάροχος να διακόπτει την υπηρεσία.

Το πρόβλημα σε μια τέτοια προσέγγιση εστιάζεται στον καθορισμό των περιστάσεων κάτω από τις οποίες οι πολιτικές πρέπει να επιβάλλονται. Όλοι οι spammers δεν συμπεριφέρονται το ίδιο. Κάποιοι μπορεί να είναι πιο επιθετικοί έως αδίστακτοι και να προξενήσουν μεγαλύτερο πρόβλημα από κάποιους άλλους. Έτσι θα πρέπει να διευκρινιστεί η μορφή και το μέγεθος της αυστηρότητας της ειδοποίησης που θα γίνει στον εκάστοτε spammer ζητώντας του να σταματήσει την δραστηριότητά του, καθώς και ο περιορισμός που θα του επιβληθεί. Δεν θα πρέπει δηλαδή να αντιμετωπίζονται όλες οι περιπτώσεις με τον ίδιο τρόπο. Έχουν προταθεί πολλές μέθοδοι που εξασφαλίζουν την προσεκτική εφαρμογή αυτών των πολιτικών.

Καταρχήν, το να ανακοινώνει ο διακομιστής τους όρους χρήσης των υπηρεσιών του στο Διαδίκτυο, με προτίμηση τα σημεία, στα οποία ο καθένας μπορεί να έχει εύκολη πρόσβαση γνωρίζοντας μόνο την διεύθυνση ηλεκτρονικού ταχυδρομείου του παραλήπτη.

Μια δεύτερη μέθοδος είναι το να ρυθμίζουν οι κάθε λογής διακομιστές, τον SMTP server τους έτσι ώστε να στέλνουν στον αποστολέα μια σύντομη αναφορά στις πολιτικές του σε κάθε βήμα τους, μέχρι να συντάξουν το μήνυμα και να το στείλουν στον παραλήπτη.

Τέλος η τρίτη μέθοδος είναι να καταθέσουν τις πολιτικές τους σε μια κεντρική αρχή, όπως μια δημόσια υπηρεσία, έτσι ώστε η αποστολή του spam να ελέγχεται από την κεντρική αρχή. Οι spammers θα πρέπει να εγγράφονται σε ένα αρχείο της υπηρεσίας για να τους επιτρέπεται να στέλνουν spam, αφού πρώτα ενημερωθούν και αποδεχτούν τις πολιτικές και τους όρους των διακομιστών. Ένα παράδειγμα όπου δεν ακολουθούνται τέτοιες μέθοδοι είναι η πολιτεία Λουιζιάνα των Η.Π.Α, στην οποία έχει θεσπιστεί ένας νόμος που απαγορεύει την αποστολή μη ενοχλητικών μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου εφόσον ο αποστολέας χρησιμοποιεί τις εγκαταστάσεις ενός διακομιστή για να διαβιβάσει τα μηνύματά του, παραβιάζοντας τις πολιτικές του. Ο νόμος αυτός δεν διακρίνει το αν ο αποστολέας είχε ουσιαστική εκ των προτέρων γνώση ότι χρησιμοποιούσε ή όχι της υπηρεσίες του συγκεκριμένου διακομιστή, οπότε και δεν προβλέπει διαφορετική αντιμετώπιση. Αντίθετα στην Καλιφόρνια, η πολιτικές ενός διακομιστή για την απαγόρευση του spam, θα επιβληθούν από τη πολιτεία μόνο υπό την προϋπόθεση ότι ο αποστολέας γνωρίζει ότι θα χρησιμοποιήσει τις εγκαταστάσεις του διακομιστή πριν στείλει ένα μήνυμα.

Την προσέγγιση της Καλιφόρνιας ακολουθούν πολλές άλλες πολιτείες των Η.Π.Α. Σε ομοσπονδιακό επίπεδο, διάφορα νομοσχέδια που είχαν να κάνουν με την επιβολή των αντί-spam πολιτικών των διακομιστών υπηρεσιών προτάθηκαν

κατά τις συνεδριάσεις του αμερικάνικου Κογκρέσου το 1999. Επίσης, η Πράξη περί ανάπτυξης του Internet του 1999 προέβλεπε την επιβολή των απαγορεύσεων των (UCE) μη ενοχλητικών εμπορικών μηνυμάτων, σύμφωνα με τις αντί-spam πολιτικές των διακομιστών υπηρεσιών, στις περιπτώσεις όπου ο αποστολέας γνώριζε από πριν τις πολιτικές. Μια άλλη Πράξη της ίδιας χρονιάς περί προστασίας των χρηστών του Διαδικτύου επιβάλλει, και αυτή, την εφαρμογή των αντί-spam πολιτικών αλλά μόνο απέναντι στους ίδιους τους πελάτες των διακομιστών υπηρεσιών.

Τέλος, στις Η.Π.Α., έχουν προταθεί και άλλα νομοσχέδια επιβολής των, απαγορευτικών στα UCE, πολιτικών τα οποία στοχεύουν σε συγκεκριμένο τρόπο εμφάνισης του spam όπως ανακοίνωσης διαφημιστικών μηνυμάτων στο Παγκόσμιο Ιστό ή εμφάνισης SMTP banners. Το συμπέρασμα που προκύπτει από την επιβολή των πολιτικών αντί-spam και την προσεκτική εφαρμογή τους είναι το εξής. Εάν ένας νόμος επιβάλλει τις αντί-spam πολιτικές των διακομιστών υπηρεσιών και μια ή περισσότερες από αυτές προβλέπουν πριν από την απαγόρευση του UCE ενός αποστολέα την αποτελεσματική ειδοποίησή του, τότε το πρακτικό αποτέλεσμα θα είναι κατά προσέγγιση ισοδύναμο με την επιβολή μιας νομικής απαγόρευσης στο spam, δεδομένου ότι σχεδόν όλοι οι διακομιστές υπηρεσιών διαθέτουν αντί-spam πολιτικές και σχεδόν όλοι πιθανώς θα ειδοποιήσουν τον υποψήφιο spammer.

Διαδικασία διαγραφής από την λίστα αποστολής των spammers

Η περισσότερες νομικές προσεγγίσεις στο spam μοιράζονται έναν κοινό στόχο, να πετύχουν το να δώσουν στον αποδέκτη του spam την δυνατότητα να επιλέξει για το αν θα δεχτεί το μήνυμα που περιέχει spam, ή όχι. Η προσέγγιση της

απαγόρευσης του spam, ή παραπλήσια, η θέσπιση νόμων που επιτρέπουν στους διακομιστές υπηρεσιών να απαγορεύουν την διακίνησή του μέσα από τις εγκαταστάσεις τους, προϋποθέτουν έναν συγκεκριμένο κανόνα, το ότι θα επιτρέπεται στους διαφημιστές να στέλνουν ηλεκτρονικά μηνύματα μόνο στα άτομα τα οποία έχουν ζητήσει τα ίδια να μπορούν να τους αποστέλλονται.

Μια διαφορετική προσέγγιση είναι αυτή της διαδικασίας διαγραφής από την λίστα αποστολής των spammers, δηλαδή οι spammers θα μπορούν να στέλνουν μηνύματα σε οποιονδήποτε εκτός εκείνων που ζήτησαν να διαγραφούν από την λίστα αποστολής τους. Υπάρχουν διάφοροι τρόποι για να εφαρμοστεί αυτή η διαδικασία. Για παράδειγμα οι spammers να είναι υποχρεωμένοι να συμπεριλάβουν στα μηνύματά τους οδηγίες προς τους παραλήπτες για το πως να στείλουν αίτηση προς τους spammers ώστε να σταματήσουν να τους στέλνουν μηνύματα. Επίσης οι αιτήσεις θα μπορούσαν να γίνονται μέσω τηλεφωνήματος, χωρίς τέλη, προς τους spammers, οι οποίοι θα υπόκεινται σε τιμωρίες εάν τις αγνοούν.

Εναλλακτικά θα μπορούσαν, οι πάροχοι υπηρεσιών Internet, να διατηρούν λίστες με δικούς τους πελάτες ή μια κεντρική αρχή λίστες διευθύνσεων μηνυμάτων από χρήστες, που επιθυμούν να μην λαμβάνουν spam. Έτσι οι αιτήσεις θα γίνονται προς τους ISPs ή μια δημόσια υπηρεσία, οι οποίοι θα αποκλείουν την διακίνηση spam προς τους αιτούντες. Η Ευρωπαϊκή Ένωση εξετάζει την δημιουργία διεθνών καταλόγων ηλεκτρονικών ταχυδρομείων, στα οποία δεν επιθυμείτε η αποστολή spam, και στα οποία οι διάφορες διαφημιστικές εταιρίες θα απαγορεύονται να στείλουν spam. Όσον αφορά τις Η.Π.Α., η πολιτεία Washington δίνει την δυνατότητα στους πολίτες της να εγγραφούν σε μια κεντρική λίστα από εκείνους που επιθυμούν να διαγραφούν από την λίστα αποστολής των spammers, η οποία σκοπό έχει να ειδοποιεί τους spammers να μην στέλνουν μηνύματα στις εγγεγραμμένες διευθύνσεις και να τους γνωστοποιήσει ότι αν το κάνουν θα

βρεθούν αντιμέτωποι με την αντίστοιχη νομοθετική ρύθμιση της πολιτείας, αν και οι προβλεπόμενες κυρώσεις δεν διευκρινίζονται με σαφήνεια. Άλλες πολιτείες έχουν ενεργοποιήσει νομοθεσίες που προστατεύουν και επικυρώνουν νομικά, ξεχωριστές αιτήσεις διαγραφής από τους πολίτες προς τους spammers. Ωστόσο καμία πολιτεία δεν έχει υιοθετήσει μια κεντρική καταχώρηση για όλους τους χρήστες του Internet.

Περιορισμοί του περιεχομένου

Μια εναλλακτική στο να ελέγχονται οι συνθήκες κάτω από τις οποίες επιτρέπεται η αποστολή spam, είναι να ελέγχονται και να περιορίζονται οι πληροφορίες που περιέχονται σε αυτά τα μηνύματα. Συνήθως τέτοιοι περιορισμοί αφορούν στις επικεφαλίδες των μηνυμάτων αν και σε περιπτώσεις όπου πρόκειται για εμπορικά μηνύματα και ειδικότερα όσα έχουν πλαστές ή αποπροσανατολιστικές γραμμές θέματος, οι νόμοι προβλέπουν εκτός των επικεφαλίδων και αλλαγή του ίδιου του περιεχομένου του μηνύματος.

Πολλές δικαιοδοσίες απαγορεύουν την χρήση πλαστών ή ελλειπών επικεφαλίδων σε εμπορικά διαφημιστικά μηνύματα. Ο λόγος είναι πιθανώς το ότι οι έγκυρες πληροφορίες στην επικεφαλίδα ενός μηνύματος βοηθούν τόσο στο μπλοκάρισμα όσο και στο φιλτράρισμα του spam, όπως και στην ανίχνευσή του με σκοπό την υποβολή παραπόνων από τους παραλήπτες προς τους πάροχους υπηρεσιών των spammers. Η χρήση των παραπλανητικών γραμμών θέματος είναι απαγορευμένη σε μερικά κράτη για παρόμοιους λόγους. Ένα παράδειγμα τέτοιων πρακτικών είναι το παρακάτω. Οι spammers χρησιμοποιούν παραπλανητικές θεματικές γραμμές όπως “RE: your message” για να μπορέσουν να ξεγελάσουν τους παραλήπτες ώστε να νομίσουν ότι το εκάστοτε μήνυμα πρόκειται για

απάντηση σε δικό τους παλιότερο μήνυμα, οδηγώντας τους έτσι εκτός του να μην διαγράψουν κατευθείαν το μήνυμα spam να το διαβάσουν κιόλας. Έτσι η επιβολή νόμων που να απαγορεύουν αυτή τη πρακτική θα μπορούσε να διευκολύνει το χειρωνακτικά φιλτράρισμα των μηνυμάτων από τους παραλήπτες. Αυτό που θα βοηθούσε ουσιαστικά στο φιλτράρισμα των spam μηνυμάτων τόσο από τους παραλήπτες όσο και από τους διακομιστές υπηρεσιών θα ήταν η ανάθεση ετικετών σε αυτά. Ήδη, κάποιες ετυμηγορίες δικαστηρίων έχουν αναφερθεί στις προδιαγραφές που θα πρέπει να έχουν τέτοιες ετικέτες.

Υπάρχουν διάφορα παραδείγματα εφαρμογής τέτοιων προσεγγίσεων στις Η.Π.Α. Στην πολιτεία Nevada, η πρώτη πολιτεία που εφάρμοσε νόμο εναντίον του spam, ένα μήνυμα spam θα πρέπει υποχρεωτικά να έχει τις κατάλληλες επικεφαλίδες ώστε να είναι εύκολα αναγνωρίσιμο. Σε αρκετές πολιτείες επιβάλλεται συγκεκριμένη επικεφαλίδα για διαφημιστικά μηνύματα, στην οποία υποχρεούνται να συμπεριλαμβάνουν το πρόθεμα “ADV:”. Επίσης σε κάποιες πολιτείες απαιτούνται ακόμα πιο συγκεκριμένες επικεφαλίδες για μηνύματα spam με μη ενοχλητικό σεξουαλικό περιεχόμενο.

Άλλες νομικές ρυθμίσεις

Κλείνοντας με τις νομικές ρυθμίσεις κατά του spam, εκτός από τις αναφερόμενες, έχουν παρατηρηθεί και άλλοι, διαφορετικοί τύποι περιορισμών στις πρακτικές του spamming. Για παράδειγμα πολλές Αμερικάνικες πολιτείες απαγορεύουν την πώληση ή τη διανομή λογισμικού που είναι σχεδιασμένο να επεμβαίνει στην δρομολόγηση και τον έλεγχο των επικεφαλίδων των μηνυμάτων στις εγκαταστάσεις των διακομιστών υπηρεσιών, κάτι που θα μπορούσε να καλύψει τα ίχνη των spammers. Διάφοροι νόμοι περί προστασίας δεδομένων σε

μερικές χώρες θωρακίζουν την συλλογή, χρήση και μεταφορά των προσωπικών πληροφοριών, συμπεριλαμβανομένων και των διευθύνσεων ηλεκτρονικών ταχυδρομείων, ενώ στο αμερικάνικο Κονγκρέσο έχει προταθεί νομοθεσία η οποία θα περιορίζει την ευκαιρία των spammers να ψάχνουν και να ανακτούν μηνύματα από εγγραφές πελατών σε διάφορες τοποθεσίες στο Internet. Πολλοί ISPs συνηθίζουν να μπλοκάρουν το spam με προορισμό τους πελάτες τους επειδή οι χρήστες τείνουν να κατηγορούν εκείνους για το spam που δέχονται.

Εξαιτίας αυτού, έχουν δημιουργηθεί πολλοί νόμοι, οι οποίοι δίνουν άδεια στους διακομιστές υπηρεσιών και τους ISPs να σταματούν το spam. Επίσης έχουν γίνει προτάσεις να απαιτείται από τους ISPs να παρέχουν στους πελάτες τους υπηρεσίες φιλτραρίσματος των μηνυμάτων που λαμβάνουν, ή να καταγράφουν τις προτιμήσεις τους ώστε να γνωρίζουν τι είδους spam επιθυμούν να λαμβάνουν και να μπλοκάρουν τα υπόλοιπα.

5.3 Νομικές Ρυθμίσεις κατά του Spam στην Ευρώπη.

Η νομική προσέγγιση που ακολουθεί η Ευρωπαϊκή Ένωση για την αντιμετώπιση του spam εντάσσεται στην ευρύτερη προσπάθεια προτυποποίησης του ηλεκτρονικού εμπορίου μεταξύ των χωρών μελών της. Αυτό επιδιώκεται με την ανακοίνωση συγκεκριμένων οδηγιών-προτάσεων (Directives), οι οποίες θα πρέπει να ακολουθούνται από τις χώρες μέλη. Οι οδηγίες αυτές δεν αποτελούν νόμους και έτσι επαφίεται στην βούληση του κάθε μέλους η υλοποίησή τους ή όχι, και σε ποιο βαθμό. Το περιεχόμενο, όσον αφορά το spam, συμπεριλαμβάνει περιορισμούς ή και απαγορεύσεις.

Παρακάτω αναφέρεται η προσέγγιση που ακολουθείται στις μεγαλύτερες χώρες της Ευρωπαϊκής Ένωσης και στην Ελλάδα, δηλαδή παρουσιάζεται ποιες

από τις οδηγίες της, που έχουν να κάνουν με το spam, υλοποιεί η κάθε χώρα, αφού όμως πρώτα γίνει μια περιληπτική αναφορά σε αυτές τις οδηγίες, αναφέροντας εκείνα τα χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για την νομική αντιμετώπιση του spam.

<u>Οδηγίες της Ευρωπαϊκής Ένωσης για το ηλεκτρονικό εμπόριο</u>

Ø Οδηγία για την προστασία δεδομένων (Directive on Data Protection ή EU Privacy Directive 95/46/EC)

Σκοπό έχει την θέσπιση κανόνων στην κυβερνητική ή εμπορική χρήση των προσωπικών δεδομένων. Συγκεκριμένα

- ορίζει ότι τα προσωπικά δεδομένα δεν θα πρέπει να προσπελαύνονται χωρίς την έγκριση του ατόμου ενώ περιορίζει τις τεχνικές συλλογής προσωπικών πληροφοριών που εφαρμόζονται από οντότητες όπως οι διαχειριστές σελίδων στον Παγκόσμιο Ιστό.
- απαγορεύει την αποστολή προσωπικών δεδομένων προς χώρες εκτός της Ε.Ε., οι οποίες δεν παρέχουν αξιόπιστη προστασία προσωπικών δεδομένων.

Ø Distance Selling Directive 97/7/EC

Σκοπός αυτής της οδηγίας είναι να παρέχει ένα νομικό πλαίσιο για τις ηλεκτρονικές εμπορικές δοσοληψίες, στις οποίες ο πωλητής και ο αγοραστής δεν βρίσκονται στο ίδιο μέρος την στιγμή της συναλλαγής και μπορεί να υπάρχει μεγάλη απόσταση μεταξύ τους.

Ø Οδηγία για το ηλεκτρονικό εμπόριο 2000/31/EC (Directive On Electronic Commerce)

Προκειμένου να ενθαρρυνθεί το ηλεκτρονικό εμπόριο, αυτή η οδηγία απαιτεί από τα κράτη μέλη να αφαιρέσουν τα νομικά εμπόδια που έφραζαν την δυνατότητα επιβολής των διαφόρων ηλεκτρονικών συμβάσεων. Μεταξύ άλλων

- Αναγνωρίζει τις συμφωνίες που γίνονται με το πάτημα κουμπιών σε ηλεκτρονικά έγγραφα, με την προϋπόθεση ότι αυτά θα ικανοποιούν τις απαιτήσεις των παραδοσιακών εγγράφων.
- Προβλέπει απαλλαγή ευθύνης για τους μεσάζοντες που ενεργούν ως μοναδικός αγωγός πληροφοριών από τρίτους και περιορίζει την ευθύνη των φορέων παροχής υπηρεσιών για διάφορες ενδιάμεσες δραστηριότητες όπως η αποθήκευση των πληροφοριών.
- Απαιτεί οι εμπορικές επικοινωνίες μέσω ηλεκτρονικών μηνυμάτων να είναι σαφώς προσδιορισμένες.
- Επιτρέπει την παροχή online υπηρεσιών για νομικά κατοχυρωμένα επαγγέλματα (όπως δικηγόροι ή λογιστές).

Ø Οδηγία περί ιδιωτικών και ηλεκτρονικών επικοινωνιών (Directive on Privacy and Electronic Communications 2002/58/EC)

Η οδηγία αυτή εισάχθηκε από την Ευρωπαϊκή Ένωση ώστε να συμπληρώσει την Privacy Directive 95/46/EC σε θέματα ηλεκτρονικών μηνυμάτων συμπεριλαμβανομένου και του spam, ενώ υπερκαλύπτει μια οδηγία που θα αναφερθεί παρακάτω, την 97/66/EC.

Ουσιαστικά προτείνει στα κράτη μέλη να υιοθετήσουν μέτρα στους ακόλουθους τομείς:

- Διαδικασίες εγγραφής (Opt-in) για παραλαβή spam. Αυτό σημαίνει ότι προαπαιτείται η συγκατάθεση του παραλήπτη πριν του αποσταλούν εμπορικά μηνύματα.
- Λογισμικό με περιεχόμενο παρακολούθησης όπως spyware, web bugs και hidden identifiers θα μπορούσαν να επιτραπούν μόνο για νόμιμους σκοπούς και με την προϋπόθεση ότι οι χρήστες έχουν εκ των προτέρων ειδοποιηθεί.
- Cookies, τα οποία θα επιτρέπεται να χρησιμοποιηθούν μόνο για νόμιμους σκοπούς, όπως για παράδειγμα η αναγνώριση της ταυτότητας του χρήστη. Επίσης ο χρήστης θα πρέπει να ειδοποιείται με ξεκάθαρο τρόπο για την ύπαρξη cookies ή παρόμοιου λογισμικού όπως και να του δίνεται η επιλογή να τα αρνηθεί.
- Οι χρήστες που εγγράφονται σε μια υπηρεσία θα πρέπει να επιλέγουν εάν τα προσωπικά τους δεδομένα επιθυμούν να ανακοινώνονται σε τρίτους ή όχι.
- Οι πάροχοι ηλεκτρονικών υπηρεσιών επιβάλλεται να πληρούν κάποιες προδιαγραφές ασφάλειας.
- Τα προσωπικά δεδομένα των χρηστών που χρησιμοποιούνται για την παροχή ηλεκτρονικών υπηρεσιών θα πρέπει να αποθηκεύονται μόνο για τις

ανάγκες της υπηρεσίας, ενώ επιβάλλεται να διαγράφονται όταν η υπηρεσία παύσει να τα χρειάζεται.

- Η χρήση λογισμικού αυτόματης κλήσης επιτρέπεται μόνο ύστερα από συγκατάθεση του φυσικού προσώπου.

Νομική προσέγγιση κρατών της Ευρωπαϊκής Ένωσης

Ø Μεγάλη Βρετανία και Βόρεια Ιρλανδία

Υλοποιούνται τα Privacy Directive 95/46/EC, Electronic Commerce Directive(00/31/EC), Distance Selling Directive (97/7/EC) και η βελτίωσή του το Directive 2002/58/EC. Γενικότερα η προσέγγιση της Μεγάλης Βρετανίας και Βόρειας Ιρλανδίας είναι η εθελοντική αντιμετώπιση του spam από την πλευρά της βιομηχανίας, η οποία θα εφαρμόζει τις οδηγίες της Ευρωπαϊκής Ένωσης, και η επέμβαση της κυβέρνησης όπου η νομική δράση κρίνεται απαραίτητη. Ένα παράδειγμα αυτής της τακτικής είναι η Πολιτική Θεμιτής Χρήσης (Acceptable Use Policy) του Ακαδημαϊκού Δικτύου JANET (Joint Academic NETwork), που στόχο έχει να αντιμετωπίσει τον τεράστιο όγκο spam που διακινείται στα ακαδημαϊκά ιδρύματα της Μεγάλης Βρετανίας. Σύμφωνα με αυτήν, το JANET απαγορεύεται να χρησιμοποιείται για οποιονδήποτε από τους εξής λόγους:

- την δημιουργία ή αποστολή προσβλητικού ή άσεμνου περιεχομένου δεδομένων οποιουδήποτε τύπου.
- την δημιουργία ή αποστολή υλικού το οποίο σχεδιάστηκε ή ενδέχεται να προκαλέσει ενόχληση στον παραλήπτη.
- την δημιουργία ή αποστολή δυσφημιστικού υλικού.

- την δημιουργία ή αποστολή υλικού το οποίο προσβάλει κατοχυρωμένο copyright.
- Την αποστολή εμπορικού ή διαφημιστικού υλικού σε άλλους οργανισμούς χωρίς την συγκατάθεσή τους.

Όλα τα παραπάνω σημαίνουν, ανάμεσα σε πολλά, ότι απαγορεύεται η διακίνηση spam σε οποιοδήποτε Ακαδημαϊκό Ίδρυμα της Μεγάλης Βρετανίας.

Ø Γαλλία

Στην Γαλλία έχει συζητηθεί ένα νομοσχέδιο, το νομοσχέδιο του 26-02-2003, το οποίο προβλέπει την υλοποίηση της οδηγίας 2002/58/EC της Ευρωπαϊκής Ένωσης. Οι αντί-spam διευκρινίσεις περιέχονται στο άρθρο 12 του νομοσχεδίου και στην ουσία απαγορεύουν την αποστολή spam σε φυσικά πρόσωπα, τα οποία δεν έχουν προηγουμένως δηλώσει την συγκατάθεση τους. Επιπλέον έχει συσταθεί μια οργάνωση που ασχολείται εκτός των άλλων και με το spam, η Εθνική Επιτροπή Πληροφορικής και Ελευθεριών (Commission Nationale de l'Informatique et des Libertés [CNIL]). Στην δράση της συμπεριλαμβάνεται η συλλογή στοιχείων από περιπτώσεις spam, η οποία ξεκίνησε το 2002, και κατέληξε στην λήψη νομικής δράσης κατά των αποστολέων. Ωστόσο δεν υπάρχουν συγκεκριμένοι νόμοι ή δικαστικές αποφάσεις που να οριοθετούν την νομιμότητα του spam. Έτσι για παράδειγμα αν ένας spammer προκαλέσει ζημιά σε μια εταιρία, τότε ο ιδιοκτήτης της μπορεί να τον μηνύσει. Όμως αδιευκρίνιστο μένει το αν ένας Internet Service Provider μπορεί για παράδειγμα να μπλοκάρει spam μηνύματα. Και αυτό ίσως επειδή τα μηνύματα θεωρούνται προσωπικά δεδομένα. Παρόλα αυτά κάποιοι ISPs μπλοκάρουν μαζικά μηνύματα.

Ø Γερμανία

Η προσέγγιση που ακολουθείται στην Γερμανία είναι αυτή του opt-in που περιγράφεται στο Distance Selling Directive (97/7/EC) και αναφέραμε παραπάνω, το οποίο υλοποιείται σε σχετικό νομοσχέδιο. Σε αυτή την κατεύθυνση, ο γερμανικός οργανισμός πολυμέσων (German Multimedia Association) έχει καταπιαστεί με την δημιουργία συγκεκριμένων οδηγιών για θεμιτό marketing παράλληλα με τις διαδικασίες opt-in. Πέραν από την λογική του opt-in δεν έχει σημειωθεί άλλη νομική προσέγγιση για την αντιμετώπιση του spam. Μάλιστα η ετυμηγορία του δικαστηρίου του Dachau απέρριψε την μήνυση μιας εταιρίας πληροφορικής, η οποία δέχτηκε ένα αρχείο μεγέθους 2.5 Mbytes με διαφημιστικό περιεχόμενο. Το δικαστήριο υποστήριξε ότι τα διαφημιστικά μηνύματα δύσκολα εμποδίζουν την εργασία της εταιρίας αφού μπορούν εύκολα να διαγραφούν και επιπλέον θεωρεί τα διαφημιστικά μηνύματα αποδεκτά και απαραίτητα για την ανάπτυξη της Οικονομίας.

Ø Ελλάδα

Στην Ελλάδα έχει τεθεί σε ισχύ νομοθεσία η οποία υλοποιεί το Distance Selling Directive 97/7/EC. Πιο συγκεκριμένα απαιτείται η πληροφόρηση και συγκατάθεση του παραλήπτη πριν την αποστολή εμπορικών fax, ηλεκτρονικών μηνυμάτων, ή ηχογραφημένων μηνυμάτων.

ΚΕΦΑΛΑΙΟ 6^{ο} :ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Γενικό συμπέρασμα.

Η ηλεκτρονική αλληλογραφία είναι από τις πιο δημοφιλείς νέες υπηρεσίες που παρέχονται μέσω του Διαδικτύου. Με πολύ χαμηλό κόστος και σε ελάχιστα δευτερόλεπτα ή έστω μερικά λεπτά, μικρά ή εκτενή κείμενα, φωτογραφίες, video, ακόμα και ηχογραφημένα (ψηφιοποιημένα) μηνύματα μπορούν να φτάσουν στον παραλήπτη αυτής της νέας μορφής αλληλογραφίας, σε όποια γωνιά της γης και αν βρίσκεται.

Η αυθαίρετη ηλεκτρονική αλληλογραφία είναι απλά το σύνολο των μηνυμάτων που στέλνονται σε ένα χρήστη χωρίς την συναίνεσή του ή την εκδήλωση της επιθυμίας του να τα λαμβάνει. Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση των προϊόντων ή των υπηρεσιών τους.

Η μεγάλη διάδοση που γνωρίζει η αυθαίρετη ηλεκτρονική αλληλογραφία, θα κάνει το email προοδευτικά δυσκολότερο στη χρήση του, ίσως και ακόμη τελείως άχρηστο ως μέσο επικοινωνίας για καταναλωτές και επιχειρήσεις αν το πλήθος των μηνυμάτων συνεχίσει να αυξάνει αντί να μειωθεί δραστικά.

Συμπερασματικά αναφέρονται παρακάτω ορισμένοι «κανόνες» τους οποίους πρέπει να ακολουθήσει ένας χρήστης για την αποφυγή των ανεπιθύμητων ηλεκτρονικών μηνυμάτων έτσι ώστε να καταφέρει να «απολαύσει» τις δυνατότητες και τα πλεονεκτήματα που σήμερα προσφέρει η ηλεκτρονική αλληλογραφία χωρίς να αντιμετωπίσει κάποιο ιδιαίτερο πρόβλημα:

1.Μην δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας.

2.Μην δίνετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σε οργανισμούς που δεν εμπιστεύεστε.

3.Μην απαντάτε στο spam.

4.Αναφέρετε κάθε μήνυμα spam που λαμβάνετε.

5.Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το spam.

6.Ελέγξτε τα συστήματα σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή.

7.Προμηθευτείτε τα σωστά προγράμματα για την καταπολέμηση του spam.

ΒΙΒΛΙΟΓΡΑΦΙΑ

http://www.spamlaws.com/articles/usf.html

http://www.computerweekly.com/Article106123.htm

http://www.dataprivacy.ie/6aiii.htm

http://www.dti.gov.uk/industries/ecommunications/electronic_commerce_directive_0031ec.html

http://www.euro.cauce.org/en/countries/c_uk.html

http://www.euro.cauce.org/en/countries/c_fr.html

http://www.euro.cauce.org/en/countries/c_de.html

http://www.euro.cauce.org/en/countries/c_gr.html

Graphic: http://www.spam.com (12/10/2002).

Graphic:http://www.matterform.com/about/welcome/anti-spam.gif (12/10/2002).

Http://www.spam.com

http://www.idyllmtn.com/mush/what.html

http://warwick.ac.uk/jilt/01-3/khong.html

http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf

http://warwick.ac.uk/jilt/01-3/khong.html.

http://www.law.ed.ac.uk/script/spam.htm (12/19/2002).

http://www.law.ed.ac.uk/script/spam.htm.

www.emailspyder.com.

Cp Rowan Middleton, PDP 2002, 2.4(3).

http://dune.coam.net/mailstats/spam/spam.html (1/5/2003).

Cp Electronic Privacy Information Center / Privacy International, Privacy and Human Rights 2002,

http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf (1/8/2003).
slashdot.org, cited in Michael Jacobs / David Naylor / Megan Auchincloss
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector(Directive on privacy and electronic communications), Official Journal L 2002/201, 37.)

1) Ιστορία Διαδικτύου, διαθέσιμα στην ιστοσελίδα http:// www.uop.gr/cst/k15/ergasies-2004/istoria2004-papatheodorou.pdf (τελευταία πρόσβαση 17/02/2010)
2)Λέανδρος Νίκος, Το Διαδίκτυο. Ανάπτυξη και αλλαγή. (Αθήνα: εκδ. Καστανιώτη. 2005), σελ 28
3) Λέανδρος Νίκος, Το Διαδίκτυο. Ανάπτυξη και αλλαγή. (Αθήνα: εκδ. Καστανιώτη. 2005), σελ 27
4) Ιστορία Διαδικτύου διαθέσιμα στην ιστοσελίδα http:// www.uop.gr/cst/k15/ergasies-2004/istoria2004-papatheodorou.pdf (τελευταία πρόσβαση 17/02/2010)
5) Ιστορία Διαδικτύου διαθέσιμα στην ιστοσελίδα http:// www.uop.gr/cst/k15/ergasies-2004/istoria2004-papatheodorou.pdf (τελευταία πρόσβαση 17/02/2010)
6)Λέανδρος Νίκος, Το Διαδίκτυο. Ανάπτυξη και αλλαγή. (Αθήνα: εκδ. Καστανιώτη. 2005), σελ 28

ΠΑΡΑΡΤΗΜΑ

Απάτες με πιστωτικές κάρτες: Ανάγκη προστασίας του ηλεκτρονικού καταστήματος

Αρκετός λόγος έχει γίνει κατά καιρούς για τους κινδύνους που συνεπάγεται η χρήση πιστωτικών καρτών στις online συναλλαγές. Συνήθως δίνεται έμφαση σε κινδύνους που αντιμετωπίζει το καταναλωτικό κοινό, χωρίς να λαμβάνονται υπόψη οι κίνδυνοι που αντιμετωπίζει ο ίδιος ο επιχειρηματίας. Στο παρόν προτείνονται απλοί τρόποι, προκειμένου να μη βρεθεί κανείς ενώπιον δυσάρεστων εκπλήξεων στις online συναλλαγές του με το κοινό.

Τα φαινόμενα απάτης μέσω online χρήσης πιστωτικών καρτών δεν είναι ιδιαίτερα συχνά, ωστόσο υπάρχουν. Ο μικρομεσαίος επιχειρηματίας, πάντως, δεν έχει να φοβάται εάν είναι προσεκτικός και ακολουθεί ορισμένους απλούς κανόνες.

Η διαδικασία επαλήθευσης των στοιχείων μιας πιστωτικής κάρτας αρχίζει με την είσοδο της κάρτας στο τερματικό ή με την πληκτρολόγηση του κωδικού της αριθμού. Η διαδικασία αυτή ουσιαστικά ελέγχει το αν η κάρτα έχει αναφερθεί ως κλεμμένη και αν η παρεχόμενη πίστωση επιτρέπει τη συγκεκριμένη συναλλαγή.

Είναι γεγονός ότι το Διαδίκτυο καθιστά τις απάτες που σχετίζονται με τη χρήση πιστωτικών καρτών ευκολότερες. Στο Internet κυκλοφορούν λίστες κλεμμένων αριθμών ή και προγραμμάτων που παράγουν νέους κωδικούς αριθμούς

πιστωτικών καρτών. Επιπλέον, η έλλειψη επαφής πρόσωπο με πρόσωπο στο Διαδίκτυο τείνει να κάνει τους απατεώνες τολμηρότερους.

Οι τρέχουσες τεχνικές για την πρόληψη της απάτης μέσω πιστωτικών καρτών, που επικεντρώνονται στον έλεγχο των υπογραφών στο πίσω μέρος της κάρτας, των ολογραμμάτων ή και την τυπωμένη εικόνα του κατόχου της, δεν μπορούν να λειτουργήσουν στις online συναλλαγές, όπου ο κάτοχος δεν είναι παρών (συναλλαγή τύπου CNP, cardholder not present), δεδομένου ότι ο έμπορος δεν μπορεί να δει την πιστωτική κάρτα και να ελέγξει την υπογραφή.

Οι online συναλλαγές μέσω πιστωτικών καρτών εμπίπτουν στην κατηγορία MOTO (Mail Order/Telephone Order, παραγγελία ταχυδρομείου /τηλεφωνική παραγγελία), ή αλλιώς CNP. Οι περισσότερες εμπορικές συναλλαγές μέσω πιστωτικών καρτών καθιστούν τον έμπορο 100% υπεύθυνο για απάτες που πραγματοποιούνται μέσω αυτού του τύπου συναλλαγής. Σε περιπτώσεις online απάτης μέσω κλεμμένων καρτών που έχουν διεξαχθεί στο εξωτερικό, οι επιχειρηματίες δεν βρίσκουν την αναμενόμενη αρωγή των αστυνομικών αρχών. Αυτό οφείλεται στο γεγονός πως οι Αρχές θεωρούν πολύ μικρά τα ποσά που διακυβεύονται (κυρίως όταν πρόκειται για λίγες δεκάδες ευρώ). Επίσης, σε περιπτώσεις διεθνών συναλλαγών, υπάρχουν εμπόδια που σχετίζονται με την αρμοδιότητα των εκάστοτε εθνικών αστυνομικών αρχών.

Τέτοιου είδους προβλήματα όμως δεν πρόκειται να αντιμετωπίσει ένας προσεκτικός επιχειρηματίας. Υπάρχουν αρκετές δικλείδες ασφαλείας και μέθοδοι που διασφαλίζουν την καλή πίστη των συναλλαγών μέσω καρτών, ορισμένες από τις οποίες παραθέτουμε:

1. Πρέπει να υπάρχει ταύτιση της διεύθυνσης που δηλώνει ο πελάτης με τη διεύθυνση αποστολής του προϊόντος. Όσο υπερβολικό κι αν ακούγεται, πολλές επιχειρήσεις του εξωτερικού δεν δέχονται να αποστείλουν προϊόντα σε διεύθυνση διαφορετική από αυτήν που έχει δηλωθεί στην πιστωτική κάρτα του καταναλωτή. Σε περίπτωση που ο πελάτης επιθυμεί η παράδοση να γίνει σε διεύθυνση διαφορετική από τη δική του, θα πρέπει να γίνεται κατόπιν ειδικής συνεννόησης.

2. Να είναι προσεκτικοί σε παραγγελίες πελατών οι οποίοι παρέχουν διεύθυνση ηλεκτρονικού ταχυδρομείου δωρεάν υπηρεσίας. Πολλές online επιχειρήσεις του εξωτερικού δεν δέχονται παραγγελίες από πελάτες με μήνυμα του τύπου username @yahoo.com, username @hotmail.com κ.λπ. Αυτό γίνεται διότι απλούστατα ο ιδιοκτήτης ενός ελεύθερου λογαριασμού μηνυμάτων παραμένει ανώνυμος. Εάν ένας απατεώνας διαθέτει κλεμμένο κωδικό πιστωτικής κάρτας και κλεμμένη διεύθυνση κατοικίας, θα χρειαστεί και μια ηλεκτρονική διεύθυνση η οποία δεν μπορεί να ανιχνευθεί.

3. Ελέγχουν το δικτυακό τόπο των πελατών, εάν υπάρχει και εάν είναι εφικτό. Είναι πιθανό να βρείτε το URL των πελατών απλά πληκτρολογώντας www. μπροστά από το δεύτερο μέρος της διεύθυνσης ηλεκτρονικού ταχυδρομείου του. Για παράδειγμα, εάν ένας πελάτης παρέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείου username @domain.com, πληκτρολογήστε www. domain.com. Είναι αρκετά πιθανό να εντοπίσετε με αυτό τον τρόπο την ιστοσελίδα του. Εκεί θα πρέπει να ελέγξετε αν πρόκειται για δικτυακό τόπο υπό κατασκευή ή για site το οποίο παρέχει στοιχεία επικοινωνίας διαφορετικά από αυτά της κατατεθείσας παραγγελίας.

4. Προσέχουν τις ασυνήθιστες παραγγελίες. Οι επιτήδειοι συνηθίζουν να κάνουν παραγγελίες που διαφέρουν σημαντικά από αυτές ενός απλού (και νόμιμου) πελάτη, όπως για παράδειγμα ακριβά προϊόντα ή πολύ μεγάλες ποσότητες, και συχνά εμφανίζονται διατεθειμένοι να πληρώσουν πολύ περισσότερα χρήματα ώστε να λάβουν το εμπόρευμα ταχύτερα.

5. Τηλεφωνούν στον πελάτη εάν υπάρχουν αμφιβολίες. Ένα σύντομο τηλεφώνημα μπορεί να είναι αρκετό ώστε να εξασφαλίσει το έγκυρο της συναλλαγής.

6. Συλλέγουν όσο το δυνατόν περισσότερα στοιχεία για την παραγγελία: τη διεύθυνση του πελάτη και τον αριθμό τηλεφώνου, την τράπεζα που εξέδωσε την πιστωτική κάρτα και τη διεύθυνση IP του υπολογιστή από τον οποίο έγινε η παραγγελία. Βέβαια αυτό έρχεται σε αντίθεση με την πολιτική του να μη ζητάνε περισσότερα από τα απαραίτητα στοιχεία για τον πελάτη, ωστόσο οφείλουν να διασφαλίσουν τη νομιμότητα της συναλλαγής.

7. Προειδοποιούν τους επισκέπτες του ηλεκτρονικού τους καταστήματος για τις μεθόδους που χρησιμοποιούν κατά της απάτης, καθώς και τις συνέπειές της. Δείχνουν ότι έχουν τον τρόπο να εντοπίσουν τους επιτήδειους και πως είναι διατεθειμένοι να τους "κυνηγήσουν".

8. Εάν χρησιμοποιήσουν κάποια υπηρεσία λήψης και εκτέλεσης παραγγελιών σε πραγματικό χρόνο (real time service), θα βεβαιωθούν ότι είναι αξιόπιστη.

9. Χρησιμοποιούν κάποια προηγμένη υπηρεσία η οποία θα μπορέσει να τους βοηθήσει στον εντοπισμό των επίδοξων απατεώνων ή και στην αποτροπή τους. Υπηρεσίες όπως η CyberSource αυτοματοποιούν όλους τους ελέγχους που καλούνται να διεξάγουν προκειμένου να εξασφαλίσουν τη νομιμότητα και την

αξιοπιστία των συναλλαγών τους. Εάν βρίσκονται σε επαγρύπνηση και δεν αφήνουν τις online παραγγελίες που λαμβάνουν στην… τύχη τους, τότε η επιχείρησή τους δεν πρόκειται να αντιμετωπίσει σοβαρό πρόβλημα με τη χρήση πιστωτικών καρτών.

Οι οικονομικές συναλλαγές μέσω Διαδικτύου, και δη με τη χρήση πιστωτικής κάρτας, έχουν ακόμη μεγάλο περιθώριο διάδοσης στο μέλλον, καθώς η έλλειψη "εμπιστοσύνης" στα ηλεκτρονικά μέσα αποτρέπει σήμερα μεγάλο μέρος των χρηστών από το να πραγματοποιούν τις αγορές τους online. Προστατεύοντας λοιπόν το ηλεκτρονικό τους κατάστημα από ύποπτες συναλλαγές με πλαστές ή κλεμμένες πιστωτικές κάρτες ή άλλες απάτες, ουσιαστικά συμβάλλουν στην ενίσχυση του αισθήματος ασφάλειας των χρηστών και κατά συνέπεια στη διάδοση των ηλεκτρονικών συναλλαγών.

Σχετικοί Σύνδεσμοι

- AntiFraud.com
- Credit Info Center
- CyberSource: Credit Card Fraud Management
- Pago International

Σχετικά Αφιερώματα

- Ηλεκτρονικό Έγκλημα
- Πολιτικές Ασφάλειας Δικτύων
- Ασφάλεια στο Διαδίκτυο: Τι πρέπει να προσέξουν οι μικρομεσαίες επιχειρήσεις
- Κίνδυνοι του e-banking

Στη σημερινή εποχή του έντονου ανταγωνισμού, οι επιχειρηματίες που δραστηριοποιούνται στο Internet αναζητούν τους πλέον δημιουργικούς τρόπους για να προσελκύσουν νέους πελάτες. Πολλοί εξ αυτών χρησιμοποιούν υπηρεσίες σύγκρισης τιμών όπως οι BizRate.com, DealTime.com, Epinions.com και Pricechecker.co.uk. Οι περισσότερες από αυτές τις υπηρεσίες χρησιμοποιούν ειδικά προγράμματα τύπου ρομπότ (bots), τα οποία καταγράφουν και συγκρίνουν αυτόματα τις τιμές των προϊόντων σε πολλά διαφορετικά ηλεκτρονικά καταστήματα.

Πολλές από αυτές τις υπηρεσίες προσφέρουν ακόμη περισσότερα, καθοδηγώντας τους υποψήφιους πελάτες, βοηθώντας τους να επιλέξουν τον πιο αξιόπιστο και φερέγγυο έμπορο για κάθε προϊόν, και παρέχουν στοιχεία για τη διαθεσιμότητα των προϊόντων. Επιπλέον, αρκετές υπηρεσίες σύγκρισης τιμών αναλύουν τα σχόλια των πελατών και εξάγουν χρήσιμα συμπεράσματα για την ποιότητα εξυπηρέτησης και τους χρόνους παράδοσης.

Οι υπηρεσίες σύγκρισης τιμών παρέχονται δωρεάν στο κοινό και είναι εύκολες στη χρήση τους, λειτουργώντας ουσιαστικά σαν μηχανές αναζήτησης. Οι ίδιες οι περιοχές σύγκρισης τιμών δεν πραγματοποιούν πωλήσεις, αλλά συνδέουν τους δυνητικούς αγοραστές με τις ιστοσελίδες των ηλεκτρονικών καταστημάτων. Προτιμώνται δε από μεγάλο αριθμό αγοραστών, καθώς πρόσφατες έρευνες δείχνουν ότι τουλάχιστον το 30% των πελατών επισκέπτονται κάποια υπηρεσία σύγκρισης τιμών πριν από κάθε online αγορά τους.

Σύμφωνα με τους αναλυτές της Jupiter Media Metrix, "οι υπηρεσίες αυτές χρησιμοποιούνται ευρέως, και η αγοραστική κίνηση έχει αυξηθεί εντυπωσιακά στη διάρκεια των τελευταίων δύο ετών".

Επισημαίνουν ακόμη ότι εκατομμύρια καταναλωτών τις επισκέπτονται τακτικά κάθε μήνα. "Κατά συνέπεια οι υπηρεσίες σύγκρισης τιμών αποτελούν ιδανικά εργαλεία προσέλκυσης πελατών για τις επιχειρήσεις που δραστηριοποιούνται στο Διαδίκτυο" σημειώνει ο Ken Cassar, αναλυτής της Jupiter Media Metrix, και συμπληρώνει: "Είναι ιδανικές για τις μικρές επιχειρήσεις που έχουν τη δυνατότητα να αποστέλλουν τα προϊόντα τους εντός της χώρας στην οποία εδρεύουν και επιδιώκουν να αποκτήσουν μερίδιο στην αγορά".

Σύμφωνα με τον ίδιο, οι μόνες επιχειρήσεις που ενδεχομένως "απειλούνται" από τις υπηρεσίες σύγκρισης είναι οι μεγάλες, όπως το Amazon.com, καθώς "μέσω της σύγκρισης οι αγοραστές μπορούν να εντοπίζουν τις πραγματικές προσφορές, οι οποίες πολύ συχνά παρέχονται από τις μικρές και μεσαίες επιχειρήσεις".

Ωστόσο, ακόμη και στις περιπτώσεις που οι μικρότερες εταιρίες δεν προσφέρουν τις χαμηλότερες τιμές, "οι πελάτες συχνά προτιμούν μια ανταγωνιστική τιμή που παρέχει ένας μικρός έμπορος, ακόμη κι αν το Amazon.com πουλά το ίδιο προϊόν φθηνότερα". Αρκεί βέβαια ο μικρότερος έμπορος να έχει δημιουργήσει καλή φήμη στην αγορά και να εμπνέει εμπιστοσύνη στους τελικούς καταναλωτές.

Ηλεκτρονική πληρωμή

Με τα αυτόματα συστήματα επεξεργασίας συναλλαγών πιστωτικών καρτών, το ηλεκτρονικό κατάστημα δε "βλέπει" ποτέ τον αριθμό της πιστωτικής κάρτας. Αυτός προωθείται αυτόματα στην τράπεζα ή την υπηρεσία που είναι υπεύθυνη για την εκκαθάριση της συναλλαγής και το κατάστημα απλά ενημερώνεται αν η πληρωμή πραγματοποιήθηκε ή όχι. Με τον τρόπο αυτό εξασφαλίζεται ο πελάτης από πιθανή μη εξουσιοδοτημένη χρήση της πιστωτικής του κάρτας.

Τι πρέπει να προσέχει κανείς όταν αγοράζει από το Internet

- Να βεβαιωθεί ότι το ηλεκτρονικό κατάστημα από το οποίο αγοράζουν είναι αξιόπιστο. Μη διστάσει να αναζητήσει πληροφορίες για τη φήμη του καταστήματος. Στο Internet τα κακά νέα κυκλοφορούν γρήγορα.
- Να βεβαιωθεί ότι ο αριθμός της πιστωτικής του κάρτας και κάθε άλλη πληροφορία που απαιτείται κατά τη συναλλαγή, αποστέλλονται με ασφαλή σύνδεση στο ηλεκτρονικό κατάστημα. Αυτό είναι εύκολο να το ελέγξει κοιτώντας την ηλεκτρονική διεύθυνση της ιστοσελίδας που επισκέπτεται. Οι διευθύνσεις που χρησιμοποιούν ασφαλείς συνδέσεις ξεκινούν με τα αρχικά https:// αντί για το γνωστό http://. Επίσης, ο Internet Explorer εμφανίζει στη γραμμή κατάστασης του ένα κλειδωμένο λουκέτο όταν η σύνδεση που έχουμε είναι ασφαλής.
- Να κρατά ένα αρχείο με τις ηλεκτρονικές του συναλλαγές (γενικά είναι χρήσιμο να κρατά ένα αρχείο με τις συναλλαγές που πραγματοποιεί με την πιστωτική του κάρτα). Πολλά ηλεκτρονικά καταστήματα στέλνουν στους πελάτες τους με ηλεκτρονικό ταχυδρομείο, πληροφορίες για τις συναλλαγές που έχουν πραγματοποιήσει.
- Προτού αγοράσει, να διαβάσει προσεκτικά τους όρους παράδοσης και την πολιτική επιστροφής ενός προϊόντος. Αν ένα προϊόν που αγοράσει δε τον ικανοποιεί μπορεί να το επιστρέψει; Αν ένα προϊόν είναι ελαττωματικό μπορεί να αντικατασταθεί ή να πάρει τα χρήματά του πίσω; Οι πληροφορίες αυτές θα πρέπει να υπάρχουν στις σελίδες του ηλεκτρονικού καταστήματος.

Στις σελίδες του ηλεκτρονικού καταστήματος θα πρέπει να υπάρχουν σαφείς πληροφορίες για τα έξοδα αποστολής, πιθανούς φόρους και άλλα έξοδα που πιθανώς επιβαρύνουν τη συναλλαγή τους. Δεν πρέπει να παρασύρεται κανείς από τη χαμηλή τιμή ενός προϊόντος, αλλά πρέπει να συνυπολογίζει και όλα τα άλλα έξοδα που θα χρειαστεί να πληρώσει.

E-MAIL MARKETING

Το e-mail marketing, αν εφαρμοστεί σωστά, είναι ένα σύστημα υψηλής απόδοσης, που προσφέρει το καλύτερο ποσοστό απαντήσεων από κάθε άλλο σύστημα άμεσου marketing. Πρόκειται για τον πιο φθηνό τρόπο διαφημιστικής προσέγγισης και για ένα αποδεδειγμένα αποτελεσματικό εργαλείο διαδικτυακού marketing.

Όμως, κάποιες λάθος τακτικές στο e-mail marketing, αρκετές φορές καταλήγουν σε ένα ατέλειωτο spamming, δημιουργώντας έτσι μια πολύ σημαντική πηγή ενόχλησης για όσους χρήστες του διαδικτύου επιθυμούν να διατηρούν καθαρό το ηλεκτρονικό ταχυδρομείο τους. Το θέμα έχει ιδιαίτερο ενδιαφέρον, γι' αυτό θα γίνει εκτενής αναφορά στις δύο σελίδες που ακολουθούν.

Τι θα πρέπει να αποφεύγεται

Δεν πρέπει να αγοράζει κανείς έτοιμους καταλόγους με ηλεκτρονικές διευθύνσεις. Οι εταιρίες που κάνουν αυτή τη δουλειά, συνήθως κινούνται στα όρια του νόμου (και μερικές φορές ολότελα μέσα στην παρανομία). Το πιθανότερο είναι, απλά, να χρησιμοποιούν λογισμικό που έχει κατασκευαστεί με αυτή την αποστολή, δηλαδή τη συλλογή ηλεκτρονικών διευθύνσεων από το διαδίκτυο. Σε κάποιες περιπτώσεις (περισσότερο οργανωμένες) απασχολούν λίγους εργαζόμενους για να κάνουν το τελικό… σκούπισμα από το ελληνικό διαδίκτυο, επιδίδονται δηλαδή σε ένα ατέλειωτο σερφάρισμα συλλέγοντας όποια ηλεκτρονική διεύθυνση πέσει στη διαδρομή τους.

Γνωρίζουν πολύ καλά ότι οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αποτελούν τα καύσιμα για τις προσπάθειες που κάνουνε στο email Marketing.

Αγοράζοντας, όμως, από αυτούς ένα CD με “5.000 διευθύνσεις” (στο διαδίκτυο υπάρχουν ξένες εταιρείες που διαθέτουν CD με εκατομμύρια διευθύνσεις) γίνονται θύματα των επιτήδειων και της απληστίας τους. Πρώτα-πρώτα το να στέλνουνε διαφημιστικά μηνύματα επί “δικαίων και αδίκων” είναι παράνομο, αυτό θα πρέπει να τους γίνει απολύτως σαφές. Ας πάμε τώρα στο “πολύτιμο” CD που μόλις αγοράσανε και γεμάτοι προσδοκίες κρατάνε στα χέρια τους. Πολλές από αυτές τις διευθύνσεις δεν ισχύουν πλέον. Πρόκειται για webmail λογαριασμούς, δηλαδή για μηνύματα τύπου Hotmail, Yahoo! κ.ά. Οι ιδιοκτήτες τους, όταν είδαν να καταφθάνουν οι πρώτες μεγάλες ποσότητες spam, τους εγκατέλειψαν για να ανοίξουν καινούργιους. Αν κάποιοι δεν το έχουν κάνει ακόμη, να σκεφτούνε ότι μαζί με το δικό τους διαφημιστικό μήνυμα καταφθάνει στο κουτί μηνυμάτων τους και ένας μεγάλος αριθμός spam, που διαγράφουν εκνευρισμένοι χρησιμοποιώντας το… τυφλό σύστημα. Να σκεφτούν, επίσης, ότι το ηλεκτρονικό ταχυδρομείο τους έχει καταγραφεί από πολλούς spammer (εταιρίες ή άτομα που συλλέγουν ανεξέλεγκτα διευθύνσεις) σε ολόκληρο τον κόσμο, και έχει επιμελώς ταξινομηθεί στα προς πώληση CD τους, ενώ ακόμα και αυτός που τους πούλησε το CD που έχουνε στα χέρια τους, έχει ήδη αρκετούς σαν αυτούς στο πελατολόγιό του. Με δυο λόγια, έχουν ήδη ξεζουμίσει τον δυνητικό τους πελάτη, ο οποίος δεν αποκλείεται να επιθυμούσε μια επικοινωνία μαζί τους, μόνο και μόνο για να τους… ρίξει ένα γερό χέρι ξύλο.

Στη συγκεκριμένη σελίδα, όταν κάνουμε λόγο για το e-mail marketing αναφέρονται πάντα στη διαφημιστική επικοινωνία που γίνεται κατόπιν συναίνεσης του παραλήπτη. Π.χ. σε αυτόν που έχει εγγραφεί στην mailing list που διατίθεται ή σ’ εκείνους που αγόρασαν κάποιο προϊόν ή κάποια υπηρεσία από αυτούς (σε κάθε περίπτωση, θα πρέπει να υπάρχει η δυνατότητα της άμεσης διαγραφής από τις λίστες των παραληπτών της διαφημιστικής αλληλογραφίας τους.

Και κάτι ακόμα. Μια μικρή λεπτομέρεια… Όλοι όσοι βρίσκονται στον κύκλο πώλησης και αγοράς CD με συλλογές ηλεκτρονικών διευθύνσεων (σ.σ.: νέο είδος συλλογής, παλιά μάζευαν πεταλούδες) μέχρι πριν από λίγο καιρό ήτανε μια χαρά e-mail marketer. Σήμερα είναι μια χαρά spammer, δηλαδή παράνομοι, τουτέστιν ανά πάσα στιγμή κινδυνεύουνε από την τσιμπίδα του νόμου.

Είκοσι τρόποι για επιτυχημένο e-mail marketing

1) Πρέπει να γνωρίζει κανείς για το θέμα του spamming. Δεν θα πρέπει να κάνει καμία ενέργεια του τύπου e-mail marketing ή να μπει στην παραμικρή δαπάνη, αν δεν μάθει για το spamming και δεν μελετήσει διεξοδικά κάθε παράμετρό του. Μπορεί κανείς στο παγκόσμιο ιστό να βρει αναλυτικές αναφορές για το θέμα, οπότε αν ενδιαφέρεται να γίνει email Marketer τους προτείνουμε να δώσει τη δέουσα προσοχή. Ακόμα κι αν έχει τις καλύτερες προθέσεις στο e-mail marketing, ο τομέας αυτός έχει δυσφημιστεί στο μέγιστο βαθμό από ποικίλες δράσεις του διαδικτυακού εγκλήματος.

2) Μετά από τα παραπάνω, είναι λογικό να συμπληρώσουμε ότι το πρώτο που θα πρέπει να φροντίσει κάποιος είναι να προσφέρει στους παραλήπτες του τη δυνατότητα τής άμεσης διαγραφής του από τις λίστες του. Είναι εκπληκτικά μεγάλος ο αριθμός των παραληπτών που, χωρίς να έχουν καμία πρόθεση διαγραφής τους, ρίχνουν μια ματιά στην τελευταία γραμμή του μηνύματός τους για να δουν αν τους προσφέρουνε αυτή τη δυνατότητα. Ούτως ή άλλως πρόκειται για

κάτι υποχρεωτικό, αλλά ακόμα και σήμερα αρκετοί συνάδελφοί τους e-mail Marketer το παραβλέπουν ή το αγνοούν. Αν, όμως, κάποιοι ενημερωμένοι χρήστες λάβουνε από αυτούς ένα τέτοιο "απρόσεχτο" διαφημιστικό μήνυμα, μπορεί, αν το θελήσουν, να τους φέρουν σε δύσκολη θέση. Αν δεν το γνωρίζουν ήδη, να είναι σίγουροι ότι αργά ή γρήγορα θα το διαπιστώσουνε στην πράξη.

3) πρέπει να οργανώνει κανείς σωστά το περιεχόμενο του διαφημιστικού του μηνύματος ή του δελτίου του. Θα πρέπει οι αναγνώστες να έχουν τη δυνατότητα μιας πρώτης γρήγορης ανάγνωσης, ώστε να εντοπίσουν χωρίς χρονοτριβή και κόπο τα περιεχόμενα που ενδεχομένως να τους ενδιαφέρουν. Αυτό μπορεί να επιτευχθεί μέσω ενός πίνακα περιεχομένων στην αρχή του μηνύματος και με έντονα τονισμένα (bold) στοιχεία-τίτλους των παραγράφων που ακολουθούν.

4) Σίγουρα θα προβληματιστεί κανείς αν θα πρέπει να στέλνει "πλούσια" μηνύματα (με γραφικά κ.ά.) ή απλά (μόνο κείμενο). Αυτό είναι ένα αρκετά μεγάλο θέμα προς συζήτηση. Οι πεπειραμένοι χρήστες του διαδικτύου προτιμούν το απλό κείμενο, γιατί γνωρίζουν κάποιες "ιδιομορφίες" των HTML μηνυμάτων. Όλοι οι υπόλοιποι προτιμούν το HTML, γιατί, αν μη τι άλλο, φθάνει σ' αυτούς ένα καλαίσθητο μήνυμα που μπορεί να τους ενδιαφέρει (σημειώνουμε, όμως, ότι ακόμα και σήμερα υπάρχουν συστήματα που δεν μπορούν να διαβάσουν μηνύματα HTML, γι' αυτό καλό θα είναι, αν επιλέξουν τη λύση αυτή, να φτιάχνουν και ένα δεύτερο μήνυμα με απλό κείμενο). Σε γενικές γραμμές και επειδή οι πεπειραμένοι χρήστες δεν αποτελούν την πλειοψηφία, τα HTML μηνύματα έχουν μεγαλύτερη αποτελεσματικότητα και –σύμφωνα με στατιστικές- δίνουν μεγαλύτερα ποσοστά άμεσης ανταπόκρισης. Αξίζει να αναφερθεί ότι έχει πολύ μεγάλη διαφορά ένα HTML μήνυμα από μια ιστοσελίδα. Διαφορετικοί κανόνες ισχύουν –σε εικαστικό και κειμενογραφικό επίπεδο- σε κάθε είδος και θα χάσει κανείς "πόντους" αν

αγνοήσει αυτή την πραγματικότητα. Με τα HTML μηνύματα μπορεί κανείς να έχει τον πλήρη έλεγχο της αλληλογραφία του. Μπορεί να γνωρίζει αν ο παραλήπτης έλαβε το μήνυμα ή το δελτίο του, πού ακριβώς κλίκαρε κ.ά. Με τον τρόπο αυτό "παρακολουθεί" όλες τις κινήσεις των παραληπτών του και μπορεί να αναπροσαρμόσει τις κινήσεις του σύμφωνα με τις προτιμήσεις και τα ενδιαφέροντά του.

5) Πρέπει να αποφεύγει κανείς τα κεφαλαία γράμματα. Γενικά, στο διαδίκτυο, η χρήση των κεφαλαίων θα πρέπει να αποφεύγεται (εκτός των περιπτώσεων που κρίνεται ως απολύτως απαραίτητη) πόσο μάλλον σε μια προσπάθεια επικοινωνιακής προσέγγισης. Ποτέ να μην χρησιμοποιούνται κεφαλαία γράμματα στην περιοχή "Θέμα" του διαφημιστικού τους μηνύματος . Στην ίδια περιοχή ("Θέμα") να μην αποκρύβεται ο σκοπός για τον οποίο επικοινώνησε ο αποστολέας με τον παραλήπτη, χρησιμοποιώντας μάλιστα ανόητες και –πολύ συχνά- ύποπτες προσεγγίσεις (όπως π.χ. "Γεια σου!", "Σκεφτόμουν πώς μπορούμε να συνεργαστούμε", "Μια μεγάλη ευκαιρία!"). Ο παραλήπτης δεν είναι φίλος τους, δεν τον ξέρει από "χθες" και δεν είναι τόσο θύμα όσο κάποιοι μπορεί να θεωρούν. Έτσι, λοιπόν, ακόμα κι αν από μόνος του έχει εγγραφεί στη mailing list τους, θα θεωρήσει ότι τον κοροϊδεύουν και θα διαγραφεί αμέσως. Πάντως, είναι κατανοητή η προσπάθειά του καθενός να επινοεί έναν ιδιαίτερα επικοινωνιακό τίτλο που θα προκαλέσει τους παραλήπτες να διαβάσουν το μήνυμά του. Αυτό που θα θέλαμε να σημειώσουμε είναι ότι, όσο κι αν φαίνεται απλό, ένα θέμα διατυπωμένο περιληπτικά και με σαφήνεια, χωρίς λογοπαίγνια, εξυπνάδες και αινιγματικές φράσεις, πολύ συχνά λειτουργεί εκπληκτικά καλά! Οι χρήστες του ίντερνετ έχουν κουραστεί από τους δήθεν ευρηματικούς τίτλους και τις μεγάλες, χωρίς αντίκρισμα υποσχέσεις (αντίλογος: και στο ίντερνετ τα πάντα είναι σχετικά, ενώ καθημερινά προστίθεται ένας μεγάλος αριθμός "νέων χρηστών έτοιμων για όλα"…).

6) Το περιεχόμενο του διαφημιστικού μηνύματος θα πρέπει να είναι σύντομο, απλό και περιεκτικό. Να απευθύνονται στο μέσο χρήστη, που δεν έχει τον χρόνο και την όρεξη για κάτι περισσότερο. Υπάρχουν βέβαια περιπτώσεις στις οποίες τα περιεχόμενα θα πρέπει να είναι αναλυτικά, αλλά αυτό αφορά μόνον κάποιες εξειδικευμένες ενημερώσεις που έχουν ζητηθεί από τους παραλήπτες. Είναι όμως κατανοητό ότι, αρκετές φορές, δεν είναι δυνατόν να περάσει κανείς τα μηνύματά του σε "τίτλους" ή σε αποσπασματικές περιγραφές. Στην περίπτωση αυτή πρέπει να εντάξει κανείς στο μήνυμά του συνδέσμους (links) που θα οδηγούν στην ιστοσελίδα του, για περαιτέρω ενημέρωση. Έτσι, θα επιτύχει και ένα μεγαλύτερο αριθμό από κλικ, θα υποδεχτεί τους αναγνώστες στο "σπίτι" του και θα μπορέσει να μετρήσει ακόμα καλύτερα τα αποτελέσματα της διαφημιστικής του εκστρατείας. Κάθε κλικ είναι μετρήσιμο και η ανάλυσή του μπορεί, στη συνέχεια, να χρησιμοποιηθεί για να προσαρμόσει κανείς τα μελλοντικά του μηνύματα ή δελτία στα ενδιαφέροντα των παραληπτών του.

7) Το e-επιχειρείν, έχει πεδίο αναφοράς 24 ώρες το 24ωρο και 7 ημέρες την εβδομάδα. Δεν συμβαίνει το ίδιο στο e-mail marketing, κυρίως όταν ο κοινός στόχος είναι οι επιχειρήσεις. Στην περίπτωση αυτή καλό θα είναι να περιορίζεται σε 3 ημέρες την εβδομάδα. Να αποφεύγονται οι μέρες: Σάββατο, Κυριακή & Δευτέρα - κι αυτό γιατί ουσιαστικά όλη η αλληλογραφία καταλήγει στο άνοιγμα της Δευτέρας, όπου στο κουτί μηνυμάτων του παραλήπτη θα έχει συσσωρευτεί πολλή αλληλογραφία. Να αποφεύγεται όμως και η Παρασκευή, κατά την οποία οι περισσότεροι είναι λίγο… "φευγάτοι" ή βιάζονται να τακτοποιήσουν όλες τις εκκρεμότητές τους στο κλείσιμο του πενθήμερου. Οι πιο κατάλληλες ώρες για την αποστολή της διαφημιστικής αλληλογραφίας τους είναι μεταξύ 11 π.μ. και 3 μ.μ. Αν οι παραλήπτες είναι συνηθισμένοι χρήστες, να προτιμήσουν το τριήμερο της

Παρασκευής, του Σαββάτου και της Κυριακής, για ευνόητους λόγους. Γενικά, θα πρέπει να αποφεύγονται οι e-mail marketing καμπάνιες σε περιόδους όπου "μαζεύονται" αργίες ή στις διακοπές. Π.χ. οι περίοδοι των Χριστουγέννων και του Πάσχα και ο μήνας Αύγουστος θα πρέπει να αποκλειστούν, κι αυτό γιατί οι… απογοητευμένοι γυρνώντας στο σπίτι ή στη δουλειά τους, θα έχουν, πέρα από την κακή τους διάθεση, να αντιμετωπίσουν και ένα μεγάλο αριθμό αλληλογραφίας, προσωπικής και διαφημιστικής. Τέλος, καλό είναι να αποφεύγει κανείς τις πολύ πρωινές αποστολές, δεδομένου ότι ένας σημαντικός αριθμός παραληπτών τείνει στο να διαγράφει όλα τα μηνύματα μαζικού ηλεκτρονικού ταχυδρομείου ώστε να αρχίσει την ημέρα του με καθαρό inbox…

8) Μην είναι ποτέ κανείς σίγουρος για την αποτελεσματικότητα κάποιου διαφημιστικού του μηνύματος, εκτός αν διαθέτει αρκετή εμπειρία. Να κάνει λοιπόν πρώτα μια δοκιμή σε ένα περιορισμένο αριθμό παραληπτών, ενώ ακόμα καλύτερα θα ήταν να ξεκινήσει με κοντινά του πρόσωπα, από τα οποία θα ζητήσει να του πουν τις εντυπώσεις και τις όποιες παρατηρήσεις τους. Θα διαπιστώσει ότι ακολουθώντας αυτή τη διαδικασία θα βελτιώσει βασικά σημεία της προωθητικής τους ενέργειας και εν συνεχεία, από την ανταπόκριση που θα υπάρξει στο περιορισμένο δείγμα, από τις αντιδράσεις και τις απαντήσεις που θα λάβει, θα αναπροσαρμόσει το μήνυμά του ώστε να γίνει περισσότερο αποτελεσματικό.

9) Θα βοηθηθεί κανείς πολύ, αν χρησιμοποιήσει κάποιο λογισμικό που έχει δημιουργηθεί γι' αυτήν ακριβώς τη δουλειά του email marketing. Έτσι, θα μπορέσει να προγραμματίσει το χρόνο αποστολής των μηνυμάτων του, θα μπορεί να έχει καλύτερο έλεγχο στην ανάπτυξη της λίστας των παραληπτών τους (εύκολη διαγραφή όσων δεν επιθυμούν πλέον να λαμβάνουν τα διαφημιστικά μηνύματα ή τα newsletter σας ή των μηνυμάτων που επέστρεψαν ως "ανεπίδοτα", έστω κι αν

πρόκειται για τρικ κάποιου παραλήπτη που χρησιμοποίησε antispam λογισμικό). Στο εμπόριο κυκλοφορούν αρκετά τέτοια προγράμματα σε μια μεγάλη γκάμα τιμών (από 30 μέχρι 500 ευρώ, ανάλογα με τις δυνατότητές τους αλλά και ανάλογα με την τιμολογιακή πολιτική της κατασκευάστριας εταιρείας…). Να σημειωθεί, όμως, ότι τα προγράμματα αυτά είναι συνήθως περίπλοκα, γι' αυτό χρειάζεται κάποιος χρόνος εξοικείωσης και δοκιμών.

10) Να φροντίζει κανείς, ο υπολογιστής με τον οποίο διεκπεραιώνει το e-mail marketing της εταιρίας του να είναι απαλλαγμένος από ιούς! Μια καλή πρόταση είναι να τον χρησιμοποιεί μόνο για την αποστολή των διαφημιστικών του μηνυμάτων (και φυσικά θα πρέπει να έχει ένα καλό και ενημερωμένο antivirus), ενώ για την παραλαβή της αλληλογραφίας του και για οποιαδήποτε άλλη διαδικτυακή εργασία να χρησιμοποιεί άλλον ή άλλους υπολογιστές. Αν, χωρίς να το θέλει, το newsletter ή το διαφημιστικό μήνυμα που θα στείλει σε εκατοντάδες ή χιλιάδες παραλήπτες περιέχει κάποιον ιό, το επόμενο που θα πρέπει να κάνει είναι… να ψάχνει τρύπα για να κρυφτεί.

11) Να αποφεύγει τα "βαρυφορτωμένα" μηνύματα. Να σκεφτεί ότι πολλοί λογαριασμοί webmail προσφέρουν περιορισμένη χωρητικότητα (π.χ., το πιο δημοφιλές, το Hotmail, δίνει 2 MB), οπότε αν το δικό του μήνυμα βοηθήσει στο να γεμίσει πολύ γρήγορα το κουτί μηνυμάτων του παραλήπτη του (με συνέπεια να μην είναι δυνατή η παραλαβή της προσωπικής του αλληλογραφίας), θα τον κάνει να… βγει από τα ρούχα του, κάτι που σίγουρα θα έχει συνέπειες και σε αυτόν…

12) Το μήνυμα ή το newsletter του δεν θα πρέπει να έχει ορθογραφικά λάθη. Είναι κάτι που θα πρέπει να επισημανθεί ιδιαίτερα, διότι αν έστω και μόνο αυτή η παράμετρος παρουσιάσει προβλήματα, θα καταργήσει όλες τις άλλες προσπάθειές

του. Μηνύματα με ορθογραφικά λάθη αποτελούν τον χειρότερο πωλητή του. Να προσέξει, επίσης, να μη βασιστεί στα συστήματα αυτόματου ορθογραφικού ελέγχου των επεξεργαστών κειμένου. Παρότι έχουν πολλές δυνατότητες, δεν είναι σε θέση να ελέγξουν με επάρκεια τα ορθογραφικά, τα συντακτικά και τα εννοιολογικά λάθη ενός κειμένου. Θα πρέπει, λοιπόν, ο άνθρωπος που συντάσσει τα μηνύματά του να είναι πολύ καλός γνώστης της ορθογραφίας (και όχι μόνο), αλλά ακόμη και σ' αυτή την περίπτωση καλό θα είναι, πριν φύγουν τα μηνύματά του, να ρίξουν μια ματιά και δυο-τρεις άλλοι, επίσης υψηλού ορθογραφικού βεληνεκούς…

13) Το κείμενο του διαδικτυακού marketing δεν έχει σχέση με τα κείμενα των άλλων μορφών διαφήμισης και επικοινωνίας. Αυτό θα πρέπει να το γνωρίζει κανείς και ίσως χρειαστεί να ενημερώσει σχετικά τον κειμενογράφο με τον οποίο συνεργάζεται. Αρκετοί κειμενογράφοι ακολουθούν τις μανιέρες τους απαράλλαχτα, είτε γράφουν για μια καταχώριση, είτε για ένα άρθρο, είτε για το διαδικτυακό τους marketing, κάτι που είναι λάθος. Για παράδειγμα, θα πρέπει να αποφεύγεται η χρήση των θαυμαστικών στο θέμα του μηνύματός τους (κάποιοι χρησιμοποιούν ακόμα και διπλά – τριπλά κ.ο.κ…- θαυμαστικά…). Αυτό, όμως, θεωρείται από τους παραλήπτες υπερβολικό και απροκάλυπτα διαφημιστικό, καταργώντας ουσιαστικά όλο το κείμενο. Επιπλέον αρκετοί απ' όσους χρησιμοποιούν φίλτρα για το spam, έχουν ενεργοποιήσει ανάμεσα στις απαγορευμένες λέξεις-κλειδιά και το θαυμαστικό.

14) Δεν πρέπει να αποκαλύπτει κανείς ολόκληρο τον κατάλογο με τις διευθύνσεις των παραληπτών του, στον τομέα CC (αυτό όντως συμβαίνει πολύ συχνά!). Είναι το πιο παιδαριώδες λάθος που μπορεί να κάνει κανείς και δημιουργεί μεγάλη ενόχληση στους παραλήπτες του. Οι χρήστες του διαδικτύου επιθυμούν

προσωποποιημένες υπηρεσίες, πόσο μάλλον όταν ο συγκεκριμένος χώρος προσφέρεται για αυτού του είδους τις τακτικές.

15) Σχετικά με το πεδίο “Θέμα” του διαφημιστικού μηνύματος. Στους ανθρώπους αρέσει ιδιαίτερα η λέξη “ομάδα” (team). Δημιουργεί την αίσθηση ότι επικοινωνούν μαζί τους μια ομάδα εκπαιδευμένων, αφιερωμένων επαγγελματιών. Όλοι αρέσκονται στην ιδέα ότι μια τέτοια ομάδα βρίσκεται στο πλάι τους και νοιάζεται γι’ αυτούς (σε όλους τους ανθρώπους αρέσει η αλήθεια, αλλά τους αρέσει, επίσης, να ζουν με ψευδαισθήσεις…).

16) Και αφού παραπάνω κάναμε λόγο για την προσωποποιημένη επικοινωνία, στο σημείο αυτό θα θέλαμε να σημειώσουμε ότι το εξειδικευμένο λογισμικό για το e-mail marketing παρέχει αυτή τη δυνατότητα, μ’ έναν πολύ απλό τρόπο. Οι παραλήπτες αρέσκονται στο να έχουν την αίσθηση ότι απευθύνονται ειδικά σε αυτούς, με το όνομα και το επίθετό τους (πρέπει να αποφεύγεται η χρήση μόνο του ονόματος, αρκετοί το θεωρούν προσβλητικό), ακόμα κι αν γνωρίζουν πολύ καλά ότι η όποια προσφώνηση προήλθε από έναν αυτοματοποιημένο μηχανισμό. Αυτό έχει αποδειχθεί στατιστικά σε έρευνες που έχουν συμπεριλάβει ακόμα και ανώτατα στελέχη πολυεθνικών εταιρειών, κάτι που, αν μη τι άλλο, τους δείχνει ότι όλοι οι άνθρωποι έχουν ανάγκη από μια ζεστή προσέγγιση, έστω κι αν γνωρίζουν ότι προήλθε από μια αυτοματοποιημένη επεξεργασία και αξιοποίηση στοιχείων. Επίσης, οι αναγνώστες προτιμούν να διαβάζουν επώνυμα ενυπόγραφα σχόλια, άρθρα κ.ά. και όχι η οποιαδήποτε αναφορά τους να ακολουθείται -μόνο- από μια “ψυχρή” εταιρική επωνυμία. Πρέπει να αποφεύγεται όμως ένα λάθος που γίνεται αρκετά συχνά. Μετά την προσπάθειά για προσωποποίηση του διαφημιστικού μηνύματος πρέπει και το κείμενο που ακολουθεί να κινείται στις ίδιες γραμμές.

Πολλές φορές, μετά τη φιλική, προσωποποιημένη προσφώνηση, ακολουθεί ένα εντελώς απρόσωπο κείμενο (!)

17) Το ύφος στα κείμενα του ηλεκτρονικού τους ταχυδρομείου θα πρέπει να είναι πληροφοριακό, χρήσιμο και φιλικό. Να έχει γραφεί μ' έναν τρόπο σαφή και συνομιλητικό, χρησιμοποιώντας απλές καθημερινές λέξεις και φράσεις. Πρέπει να έχει προσέξει κανείς κάθε λεπτομέρεια. Επίσης πρέπει να λαμβάνεται σοβαρά υπόψιν ότι δεν πρέπει να γίνεται επίδειξη γνώσεων ή ικανοτήτων, άλλωστε με αυτό το τρόπο δεν πρόκειται να βρεθεί κανένας ενδιαφερόμενος. Το μόνο που θα πρέπει ενδιαφέρει είναι να περαστεί το διαφημιστικό μήνυμα - κάτι όμως που δεν θα επιτευχθεί αν οι παραλήπτες τους νιώσουν "μειονεκτικά" (εκτός κι αν απευθύνεται κανείς σ' ένα αυστηρά επιλεγμένο, εξειδικευμένο κοινό).

18) Να γίνονται προσφορές στους παραλήπτες: ένα προϊόν με σημαντική έκπτωση, ένα e-book ή κάποια υπηρεσία. Στους περισσότερους αρέσει ένα μικρό δωράκι αλλά, αυτό είναι ευνόητο. Κάτι όμως που διαφεύγει πολλές φορές είναι ότι στην προσφορά θα πρέπει ΠΑΝΤΑ να μπαίνει κάποια προθεσμία. Μπορεί να υπάρχει λόγος ώστε να περιμένει κανείς τους πελάτες του για μεγάλο χρονικό διάστημα, όμως οι προθεσμίες προσδίδουν σοβαρότητα στην εταιρεία, ενώ παράλληλα πολλαπλασιάζουν την ανταπόκριση της προσφοράς και της δίνουν πρόσθετη αξία.

19) Πρέπει να αποφασίζει κανείς με ποια συχνότητα θα επικοινωνεί με τους παραλήπτες τους. Μια πολύ συχνή αλλά και μια πολύ σπάνια επικοινωνία μπορεί να οδηγήσει στα ίδια αποτελέσματα. Στο "τι θέλει πάλι αυτός;", όσο κι αν φαίνεται παράξενο, μπορεί να οδηγήσουν και οι δύο περιπτώσεις. Ένα διαφημιστικό μήνυμα ανά μήνα θεωρείται η πιο καλή συχνότητα, αν και κάποιες μικρές αποκλίσεις είναι θεμιτές. Μπορεί κατά καιρούς και αν κάτι έκτακτο προκύψει να

επικοινωνεί κανείς και πιο συχνά, αυτό όμως σε καμία περίπτωση δεν θα πρέπει να γίνει ο κανόνας. Αν υπάρχει η δυνατότητα οργάνωσης ενός πολύ αξιόλογου και ενημερωτικού μηνύματος (οι αντιδράσεις των παραληπτών θα δείξουν το σωστό δρόμο…), μπορούν να αποστέλλεται κάθε 2-3 εβδομάδες. Σε περίπτωση που συντάσσεται ένα πλήρες newsletter η καλύτερη συχνότητα είναι ανά 15 ημέρες. Πρέπει επίσης να προσεχθεί πως θα οργανωθούν σωστά οι αποστολές του. Θεωρείται σοβαρό λάθος να στέλνεται δύο φορές το ίδιο μήνυμα στον ίδιο παραλήπτη. Ο παραλήπτης του ενοχλείται, ενώ η κίνησή αυτή προδίδει προχειρότητα.

20) Πρέπει να υπενθυμίζεται στους παραλήπτες ότι αν εξακολουθήσουν να δέχονται τα μηνύματά, θα έχουν πολλαπλά οφέλη (σε ενημέρωση, προσφορές κ.ά.). Επίσης, πρέπει να δείχνεται η εικόνα μιας συνεχούς βελτίωσης και να δίνεται η υπόσχεση ότι με την πάροδο του χρόνου η βελτίωση αυτή θα είναι όλο και πιο έντονη, κάτι που θα πρέπει να τηρήσουν, τουλάχιστον σε επαρκή βαθμό, ώστε να φανούν αξιόπιστοι