ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΕΠΙΘΥΜΗΤΗ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (SPAM)

ΝΙΚΟΛΑΟΥ ΓΕΩΡΓΙΑ

ΡΟΥΣΕΛΑΤΟΣ ΜΑΡΙΝΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:

ΧΡΙΣΤΟΔΟΥΛΟΥ ΙΩΑΝΝΗΣ

ΠΑΤΡΑ 2010

.....

Γεωργία Β. Νικολάου
Πτυχιούχος Τμήματος Λογιστικής Α.Τ.Ε.Ι. Πατρών.

.....

Μαρίνος Φ. Ρουσελάτος
Πτυχιούχος Τμήματος Λογιστικής Α.Τ.Ε.Ι. Πατρών.

Ευχαριστίες

Θα θέλαμε να εκφράσουμε από κοινού την ευγνωμοσύνη μας στον καθηγητή κ. Ιωάννη Χριστοδούλου, καθώς με τις πολύτιμες συμβουλές του, τις εύστοχες παρατηρήσεις και τις εμπνευσμένες προτάσεις του, συνεισέφερε ουσιαστικά, τόσο στην διεύρυνση του γνωστικού μας υπόβαθρου όσο και στην επιτυχή εκπόνηση, εκ μέρους μας της παρούσας διπλωματικής εργασίας.

Επίσης θα θέλαμε να ευχαριστήσουμε τους γονείς μας, για την κατανόηση και την συμπαράσταση τους, καθόλη την διάρκεια των σπουδών μας.

Γεωργία Β. Νικολάου, **Μαρίνος Φ. Ρουσελάτος**
Πάτρα, **Σεπτέμβριος** 2009

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Στην συγκεκριμένη εργασία καλούμαστε να ασχοληθούμε με το spam η αλλιώς το αυτόκλητο μήνυμα ηλεκτρονικού ταχυδρομείου, δηλαδή το ηλεκτρονικό μήνυμα, κυρίως εμπορικού ή διαφημιστικού περιεχομένου, το οποίο αποστέλλεται μαζικά σε παραλήπτες, οι οποίοι βέβαια δεν το έχουν ζητήσει. Εκτιμάται άλλωστε ότι στις μέρες μας το μεγαλύτερο ποσοστό ηλεκτρονικής αλληλογραφίας που αποστέλλεται στους χρήστες του διαδικτύου, είναι τύπου spam.

Το spamming ως δραστηριότητα, αναφέρεται στην πρακτική της αδιάκριτης διανομής μηνυμάτων, χωρίς την άδεια αλλά και χωρίς σκέψη για το αν ενδιαφέρει η όχι το μήνυμα τον παραλήπτη.

Το λογισμικό εξέτασης και το πλήκτρο διαγραφής (delete) ίσως είναι τα καλύτερα εργαλεία του ατόμου για αυτοάμυνα από τον ηλεκτρονικό αυτό πόλεμο. Δικτυακοί τόποι παρέχουν δωρεάν λογισμικό που μπλοκάρει ανεπιθύμητες διαφημίσεις και προστατεύει τους χρήστες από cookies και άλλες απειλές.

Στα επόμενα κεφάλαια θα εξετάσουμε, τους λόγους που οδηγούν στο φαινόμενο του spam, τις μεθόδους που χρησιμοποιούν οι spammers, το κόστος που προκαλεί σε ιδιώτες και επιχειρήσεις, τις τεχνικές – μεθόδους καταπολέμησης του, τα ειδικά λογισμικά αντιμετώπισης, τα μέτρα πρόληψης, τις ομάδες εργασίας και τις πρωτοβουλίες anti-spam καθώς και την σχετική νομοθεσία.

Στην συνέχεια προτού προβούμε στα τελικά συμπεράσματα και αφού εξετάσουμε τις υπάρχουσες λύσεις σε άλλα εκπαιδευτικά ιδρύματα, θα επιχειρήσουμε να προτείνουμε έναν συνδυασμό μεθόδων για την αντιμετώπιση του spam, από το Α.Τ.Ε.Ι. Πατρών.

Τέλος μετά την βιβλιογραφία ο αναγνώστης μπορεί να ενημερωθεί μέσω παραρτημάτων για τα ακόλουθα:

i. Παράρτημα Α : Προτεινόμενη Πολιτική Anti-Spam Α.Τ.Ε.Ι. Πατρών.
ii. Παράρτημα Β : Χαρακτηριστικές Περιπτώσεις Spamming.
iii. Παράρτημα Γ : Στατιστικά Στοιχεία Spam.
iv. Παράρτημα Δ : Διαδικτυακά Διαθέσιμος Οδηγός για το SPAM.

Κεφάλαιο 2

Βασικές Έννοιες γύρω από το SPAM

1. Ορισμός και κατηγοριοποίηση της έννοιας spam

Ο όρος spam, έχει καθιερωθεί ως η διεθνής ονομασία των ανεπιθύμητων - αυτόκλητων διαφημιστικών μηνυμάτων που λαμβάνονται είτε μέσω ηλεκτρονικού ταχυδρομείου είτε μέσω γραπτών μηνυμάτων (sms) στο κινητό τηλέφωνο. Η λέξη spam είναι ένα αρκτικόλεξο, και προέρχεται από τα αρχικά των λέξεων Spiced Pork And Meat.

Η ιστορία του αρκτικόλεξου ξεκινά πίσω στο 1937, όταν ένα καινούριο είδος κρέατος (σε κονσέρβα) εμφανίστηκε στην αγορά. Η καινοτομία του συγκεκριμένου προϊόντος ήταν ότι προσέφερε «φρέσκο» κρέας, το οποίο δεν χρειαζόταν να αποθηκευτεί στην κατάψυξη, σε μια εποχή που τα ψυγεία ήταν δυσεύρετα και το φρέσκο κρέας είδος πολυτελείας.

Η λήξη του πολέμου και η ανάπτυξη της τεχνολογίας και της οικονομίας που έκανε προσιτό το φρέσκο κρέας μετέτρεψε το SPAM σε ένα αζήτητο προϊόν. Η έννοια του αζήτητου συνεπώς ήταν ο συνδετικός κρίκος για την επικράτηση του όρου spam, για την ανεπιθύμητη αποστολή ηλεκτρονικών μηνυμάτων.

Το πρώτο εμπορικό spam καταγράφηκε σε ένα τηλεγράφημα το 1904, ενώ το πρώτο ηλεκτρονικό spam καταγράφηκε το 1978. Αργότερα το 1980, ο όρος χρησιμοποιήθηκε για να χαρακτηρίσει αυτούς που στα BBSs και MUDs επαναλάμβαναν πάρα πολλές φορές την λέξη spam για να κατακλύσουν τις οθόνες των άλλων χρηστών Ο σκοπός του spam σε αυτό το στάδιο ήταν να βγουν “εκτός δωματίου συζήτησης” οι νεοεισερχόμενοι, έτσι ώστε να συνεχίσουν οι παλαιότεροι επισκέπτες την συνομιλία τους. Συνακολούθως, χρησιμοποίησαν το spam για να παρεμποδίσουν ομάδες συνομιλητών να συνεχίσουν την συζήτησή τους.

Η επόμενη φάση ήταν η χρήση του όρου στο Usenet με την έννοια της επαναλαμβανόμενης αποστολής του ίδιου μηνύματος. Πρώτος χρησιμοποίησε τον όρο ο Joel Furr στις 31 Μαρτίου το 1993, ενώ το spamming για εμπορικούς σκοπούς ξεκίνησαν οι δικηγόροι Laurence Canter και Martha Siegel, στις 5 Μαρτίου 1994 (Green Card Spam).

Στο spam συμπεριλαμβάνεται το Unsolicited Bulk Email (UBE), δηλαδή η μαζική αποστολή μηνυμάτων σε παραλήπτες, χωρίς οι τελευταίοι να τα έχουν ζητήσει, ενώ δίδεται και ο ορισμός Unsolicited Commercial Email (UCE), που επικεντρώνεται στα αυτόκλητα μηνύματα εμπορικού περιεχομένου.

Ακολούθως θα πρέπει να εξεταστούν τα βασικά χαρακτηριστικά του spam ώστε να οριοθετηθεί το πεδίο της έρευνας. Πρώτον, ως ανεπιθύμητο ορίζεται το μήνυμα το οποίο στέλνεται από ένα αποστολέα που δεν έχει προηγούμενη σχέση με τον παραλήπτη, ώστε να δικαιολογείται η αποστολή του διαφημιστικού μηνύματος. Αυτό είναι και το βασικό κριτήριο για το χαρακτηρισμό ενός μηνύματος ως spam.

Δεύτερον, δεν θα πρέπει να δίνεται η δυνατότητα στο παραλήπτη του μηνύματος να διαγραφεί από την λίστα αλληλογραφίας του αποστολέα, ώστε να αποφύγει μελλοντικά μηνύματα.

Τρίτον, θα πρέπει να λείπει από το μήνυμα μια έγκυρη διεύθυνση επικοινωνίας με τον αποστολέα του μηνύματος.

Η Τετάρτη προϋπόθεση χαρακτηρισμού ως spam ενός μηνύματος αφορά το περιεχόμενό του το οποίο θα πρέπει να περιλαμβάνει ή να προωθεί δυσάρεστο ή παράνομο υλικό το οποίο είναι ψευδές ή παραπλανητικό.

Η Πέμπτη και τελευταία προϋπόθεση, αφορά τον τρόπο αποστολής ό οποίος θα πρέπει να είναι αυτοματοποιημένος, ενώ οι ηλεκτρονικές διευθύνσεις θα πρέπει να έχουν αποκτηθεί με λογισμικό ανίχνευσης του παγκόσμιου ιστού, για συλλογή διευθύνσεων ("αράχνες") ή να έχουν αγοραστεί από εταιρείες που συλλέγουν e-mails και τα διακινούν παράνομα μέσω CD.

Σε αυτό το σημείο θα πρέπει να τονιστεί ο ρόλος του spam. Συνήθως χρησιμοποιείται για διαφημιστικούς λόγους, δηλαδή ως μέσω προώθησης προϊόντων.

Δεν θα πρέπει όμως να παραβλέπονται και οι άλλες μορφές spam που δεν χρησιμοποιούνται για εμπορικούς σκοπούς. Έτσι ως spam χαρακτηρίζονται και μηνύματα προώθησης υπηρεσιών ή σκοπών φιλανθρωπικών ιδρυμάτων, σωματείων, και ενώσεων.

Χαρακτηριστικό παράδειγμα είναι η 19/2001 Απόφαση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η οποία αφορά την μετάδοση μέσω ηλεκτρονικού ταχυδρομείου ενός υπερκείμενου συνδέσμου (link) που παρέπεμπε στην ηλεκτρονική εφημερίδα του αποστολέα του μηνύματος. Παράλληλα, ειδική διακήρυξη της Διεθνούς Συνόδου των Επιτρόπων για την προστασία των προσωπικών δεδομένων του 2005, αναφέρει ότι «*ακόμα και η πολιτική επικοινωνία οφείλει να συμμορφώνεται με τους κανόνες που ισχύουν για το spam*».

2. Το Spam στην καθημερινή ηλεκτρονική αλληλογραφία

Το spam δεν ήταν απο την αρχή, μια ενοχλητική ή απειλητική τακτική για τους χρήστες του διαδικτύου. Μάλιστα, η ανάγνωση αυτών των μηνυμάτων μπορούσε να θεωρηθεί ως ένα ευχάριστο διάλειμμα από τη δουλειά.

Σήμερα όμως λόγω των διαστάσεων που έχει λάβει, είναι μαζί με τους ιούς (worms & viruses) ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Ο κύριος λόγος που συμβαίνει αυτό είναι ότι οι αποδέκτες του spam λαμβάνουν περισσότερο όγκο δεδομένων από αυτόν που χρειάζονται και επιθυμούν γεγονός που προκαλεί απώλεια χρόνου και χρήματος.

Χαρακτηριστικά αναφέρεται ότι, σύμφωνα με στοιχεία του 2005 ο χρόνος που χάνεται για το σβήσιμο των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου κοστίζει στις αμερικανικές επιχειρήσεις σχεδόν 22 δισ. δολάρια ετησίως. Παράλληλα επιβαρύνει τη διαχείριση των ηλεκτρονικών μηνυμάτων στους κεντρικούς εξυπηρετητές καταναλώνοντας υπολογιστικούς και αποθηκευτικούς πόρους.

Συνεπώς, όταν πλέον το 70% περίπου των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι σήμερα spam, γίνεται φανερό ότι δημιουργούνται πολλά προβλήματα για τους χρήστες.

Συνακολούθως, το spam, εκτός από ενοχλητικό, μπορεί περιέχει απατηλό ή ακόμα και επικίνδυνο περιεχόμενο.

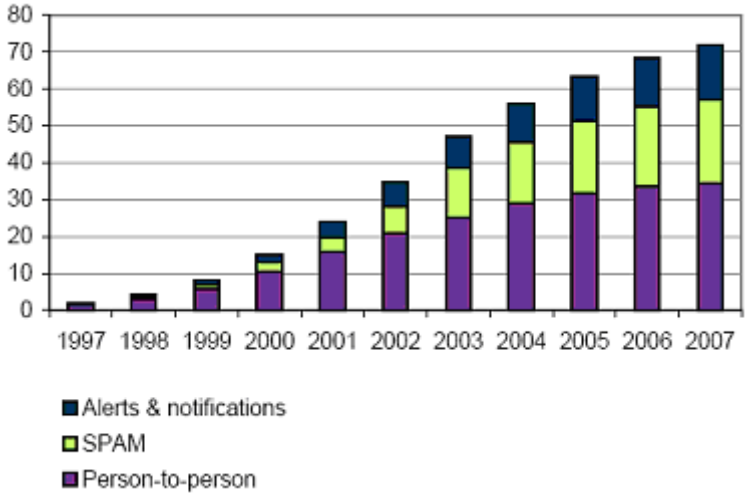
Για παράδειγμα spam που διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις (όπως π.χ. σχετικά με τη "δύναμη" συγκεκριμένων μετοχών), ή προωθούν προϊόντα και υπηρεσίες πορνογραφικού χαρακτήρα.

Επίσης τον τελευταίο καιρό έχει παρατηρηθεί η χρήση spam ως μέσο μετάδοσης ιών ή άλλων επιβλαβών λογισμικών που σκοπεύουν στην "κατάληψη" του υπολογιστή του χρήστη (*zombie computer*) ώστε να χρησιμοποιηθεί ως μέσο αποστολής spam.

Επίσης επεκτείνεται συνεχώς και το spam τύπου *phising* που στοχεύει στην εκμαίευση προσωπικών δεδομένων των χρηστών, με συνήθη σκοπό την απόσπαση χρηματικών ποσών, μέσω τραπεζικών λογαριασμών. Αναφορικά με

το μέλλον του spam σύμφωνα με έρευνα της IDC το spam θα αυξάνεται σταδιακά και αναλογικά πάντα με τον συνολικό όγκο της ηλεκτρονικής αλληλογραφίας.

Αριθμός e-mails ανά ημέρα σε παγκόσμιο επίπεδο
(Διάφορες ειδοποιήσεις λαθών, Spam και προσωπική αλληλογραφία)



Πηγή: IDC, 2003

Ο χρήστης όμως του ηλεκτρονικού ταχυδρομείου δεν είναι απροστάτευτος απέναντι στην επέκταση του spam. Για την αντιμετώπιση του φαινομένου έχει δημιουργηθεί θεσμικό πλαίσιο τόσο σε διεθνές όσο και σε εθνικό επίπεδο.

Συγκεκριμένα στην Ελλάδα το spam ρυθμίζεται από το αρ. 11 του Νόμου 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Σύμφωνα με την παρ. 1 του αρ. 11 "Μη ζητηθείσα επικοινωνία": "Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς."

Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα «opt-in». Ειδικά για τα μηνύματα ηλεκτρονικού ταχυδρομείου, εξαίρεση αποτελεί, σύμφωνα με την παρ. 3 του αρ. 11, η περίπτωση στην οποία η ηλεκτρονική

διεύθυνση του χρήστη αποκτήθηκε από τον αποστολέα νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής.

Στην περίπτωση αυτή μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση (σύστημα "opt-out").

Επίσης, ως προς την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, ορίζεται ότι θα πρέπει να αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητά τον τερματισμό της επικοινωνίας.
Η εφαρμογή των παραπάνω ρυθμίσεων επεκτείνεται, πέρα από τα φυσικά, και στα νομικά πρόσωπα.

3. Άλλες μορφές ηλεκτρονικών διαφημιστικών απορριμμάτων

Το spam αν και έχει γίνει γνωστό από την ηλεκτρονική αλληλογραφία δεν περιορίζεται εκεί. Αντιθέτως, ταυτόχρονα με την ανάπτυξη των ηλεκτρονικών μέσων διαφήμισης αναπτύχθηκαν και οι ανεπιθύμητες ηλεκτρονικές διαφημίσεις. Για να προσδιορίσουμε το όριο ανάμεσα στις ηλεκτρονικές διαφημίσεις, οι οποίες είναι νόμιμες και θεμιτές, και αυτές οι οποίες είναι αθέμιτες και καταχρηστικές, θα πρέπει να ανατρέξουμε στο αντίστοιχο θεσμικό πλαίσιο, το οποίο είναι τα ακόλουθο:

Άμεση διαφήμιση είναι η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή, μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, (Απόφαση αμερικανικού δικαστηρίου για το spam του 2003) αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας. Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή.

Με βάση τα παραπάνω μπορούμε να κατηγοριοποιήσουμε ως ηλεκτρονικά διαφημιστικά απορρίμματα τα spam sms που είναι γνωστά κυρίως ως mobile spam ή m-spam, αλλά και ως SMS spam ή SpaSMS.

Το σημαντικό στοιχείο που τα διαχωρίζει από το spam ηλεκτρονικού ταχυδρομείου είναι ότι ο παραλήπτης συνήθως υποχρεώνεται να τα ανοίξει προτού τα διαγράψει, με αποτέλεσμα να είναι διπλά ενοχλητικά. Παρουσιαστήκαν πρώτη φορά ανάμεσα στο 2001 και στο 2002 στην Ιαπωνία, παραλύοντας τα συστήματα της DoCoMo, της μεγαλύτερης εταιρείας κινητής τηλεφωνίας στη χώρα: οι γραμμές μπλοκάρισαν, οι οθόνες των χρηστών πάγωσαν και τα κινητά τους άρχισαν να καλούν από μόνα τους, αριθμούς κλήσης έκτακτης ανάγκης. Σύντομα, εμφανίστηκαν στη Βόρεια Αμερική και στην Ευρώπη, όχι όμως στην ίδια έκταση.

Συνήθως τα spam sms προτρέπουν τον παραλήπτη να καλέσει έναν αριθμό. Ο αριθμός αυτός μπορεί να έχει υψηλή χρέωση, την οποία εισπράττει ο κάτοχός του. Μια άλλη μορφή spam στα κινητά είναι μέσω αναπάντητων κλήσεων, δηλαδή αυτό το spam είναι σχεδιασμένο ώστε να στέλνει κλήσεις οι οποίες «χτυπούν» μόνο μία φορά και καταχωρίζονται ως αναπάντητες, έτσι ώστε ο

παραλήπτης όταν καλεί για να δει ποιος του τηλεφώνησε χρεώνεται προς όφελος των spammers.

Αρκετοί αναλυτές προειδοποιούν ότι τα spam sms θα λάβουν ανάλογες διαστάσεις με τα spam e-mails.

Υπάρχει όμως και μια μερίδα αναλυτών που διαφωνώντας επικαλούνται το επιχείρημα του κόστους. Δηλαδή, το ότι στο διαδίκτυο, το κόστος είναι ελάχιστο έως μηδενικό, αν χρησιμοποιεί κανείς botnet, ενώ τα κινητά τηλέφωνα χρεώνονται.

Μια άλλη νέα και διαδεδομένη μορφή ηλεκτρονικών διαφημιστικών απορριμμάτων είναι τα Spam blogs. Πρόκειται για «blogs», τα οποία αναπαράγουν το περιεχόμενο άλλων blogs, είτε τραβώντας με rss τα posts τους, είτε αναδημοσιεύοντάς τα «χειροκίνητα» και παρουσιάζοντάς τα ως πρωτότυπα.

Βασικό χαρακτηριστικό είναι ότι τα spam blogs είναι γεμάτα διαφημίσεις, τις περισσότερες φορές Google AdSense, αφού μοναδικός σκοπός είναι το χρηματικό κέρδος. Αυτή η κατηγορία εκτός από ανεπιθύμητη διαφήμιση, συνιστά και κλοπή πνευματικής ιδιοκτησίας.

Επίσης έχει αναπτυχθεί ως ανεπιθύμητος τρόπος διαφήμισης η αποστολή spam κατά την άμεση αποστολή μηνυμάτων γνωστό ευρέως και ως “spim”.

Ακόμα η χρήση spam, έχει προχωρήσει και στην ομιλία μέσω διαδικτύου. Πρόκειται για το spit (έχει προκύψει από το Spam Over Internet Telephony: ενοχλητική αλληλογραφία μέσω τηλεφωνίας Διαδικτύου, ωστόσο η κατά λέξη μετάφραση είναι ‘φτύσιμο').

Το spit έχει τη δυνατότητα να καταστρέψει ολοσχερώς το VoIP , αφού κανένας χρήστης δεν θα εγκαθιστούσε το σύστημα, με το φόβο ότι θα λάμβανε δεκάδες τηλεφωνήματα ηχητικού spam . Τέλος, ως ηλεκτρονικά διαφημιστικά απορρίμματα χαρακτηρίζονται και οι μαζικές κλήσεις σε σταθερά τηλέφωνα, που όταν απαντηθούν ακούγεται ένα προηχογραφημένο διαφημιστικό μήνυμα.

4. Λόγοι αποστολής ανεπιθύμητων μαζικών μηνυμάτων

Ο κύριος λόγος αποστολής των ανεπιθύμητων μαζικών μηνυμάτων spam είναι εμπορικός. Δηλαδή επιδιώκεται μέσα από το spam η διαφήμιση ενός προϊόντος.

Η επιλογή του spam ως μέσο δικαιολογείται από το μηδενικό κόστος αποστολής τεράστιου αριθμού μηνυμάτων, ώστε όσο μικρή και αν είναι η ανταπόκριση του κοινού στο διαφημιστικό μήνυμα, ο αποστολέας να είναι κερδισμένος.

Σε γενικές γραμμές, η παραπάνω συλλογιστική είναι κοινά αποδεκτή, όμως δεν λείπουν και οι αντίθετες απόψεις. Αμερικανοί ερευνητές κατάφεραν να αποκαλύψουν τα οικονομικά στοιχεία μιας ομάδας spammers εισχωρώντας στους υπολογιστές τους.

Η συγκεκριμένη έρευνα απέδειξε παράλληλα ότι ακόμα και οι Spammers είναι ευάλωτοι σε επιθέσεις που κάνουν την αποστολή κακόβουλων μηνυμάτων ιδιαίτερα δαπανηρή υπόθεση, με αποτέλεσμα να καθιστάται το spamming μια «επιχείρηση» λιγότερο επικερδής από όσο πιστεύεται.

Η έρευνα διεξήχθη από τα τμήματα πληροφορικής των πανεπιστημίων του Μπέρκλι, του Σικάγο και του Σαν Ντιέγκο και διήρκεσε αρκετούς μήνες, Μια ισχυρή ομάδα εφτά προγραμματιστών κατόρθωσε να διεισδύσει στους υπολογιστές του δικτύου Storm, να μελέτησει τις τεχνικές τους και τον τρόπο αποκόμισης κερδών.

Στον αποκορύφωμα της δράσης της, η Storm θεωρείται ότι είχε καταφέρει να έχει τον έλεγχο σε πάνω από ένα εκατομμύριο προσωπικούς υπολογιστές ανυποψίαστων πολιτών και μέσω αυτών να διεξάγει τις επιχειρήσεις της, χωρίς να φαίνεται.

Η ομάδα με επικεφαλής των αναπληρωτή Καθηγητή Στέφαν Σάβατζ κατάφερε με τις σειρά της να αποκτήσει τον έλεγχο μερικών από τους υπολογιστές της Storm και να καταλάβει πως λειτουργούσαν.

Οι ερευνητές κατέληξαν στο συμπέρασμα ότι το περιθώριο κέρδους τελικά είναι πολύ μικρό και πως οι Spammers πρέπει να είναι πολύ προσεκτικοί με τις λεπτομέρειες του τρόπου διεξαγωγής μιας τέτοια εκστρατείας, διαπιστώνοντας παράλληλα το πόσο ευάλωτοι είναι απέναντι σε νέα συστήματα προστασίας.

Συμπερασματικά θα μπορούσαμε να διακρίνουμε τις ακόλουθες χρήσεις που μπορεί να έχει το spam στο διαδίκτυο (Internet).

Πολιτικές ή θρησκευτικές χρήσεις spam:

i. Ιστορικές αναθεωρήσεις (π.χ. Serdar Argic)

Στο Internet υπάρχουν διάφορα γκρουπ συζητήσεων (newsgroups) για κάθε θέμα, με κάποια από αυτά να ασχολούνται με την ιστορία.

Το 1992, σε ένα από αυτά τα γκρουπ η συζήτηση έφτασε στην γενοκτονία των Αρμενίων που έγινε από τους Τούρκους το 1915. Τότε εμφανίζεται για πρώτη φορά κάποιος που υπογράφει ως Serdar Argic και σε έντονο ύφος, ούτε λίγο ούτε πολύ, ισχυρίζεται ότι οι Αρμένιοι έσφαξαν τους Τούρκους και όχι το αντίθετο.

Κάποιοι του επιτέθηκαν λεκτικά, άλλοι του απάντησαν σοβαρά, μα τότε ξεκίνησε ο εφιάλτης για τα συγκεκριμένα newsgroups. Ο Serdar Argic συνέχισε τον βομβαρδισμό τους με εκατοντάδες μηνύματα καθημερινά, μην επιτρέποντας τις συζητήσεις να προχωρήσουν.

ii. Πολιτικό SPAM – Πολιτική προπαγάνδα
iii. Ευαγγελιστές (μηνύματα κηρυγμάτων)

Διαφημιστικές χρήσεις spam:

i. Κλασσικά spam (διαφημιστικά) emails.
ii. Spam σε online ηλεκτρονικά παιχνίδια.
iii. Spam σε ιστοσελίδες κοινωνικής δικτύωσης και forums.

Spam για την καταπολέμηση των antispam εργαλείων:

i. Hobbit spam (SPAM το οποίο περιέχει μη συνήθεις λέξεις για spam και αποστέλλεται με σκοπό να μπερδέψει τα βασισμένα σε Bayesian filtering spam φίλτρα, με σκοπό να μην έχουν στην συνέχεια το ίδιο καλή «αντιμετώπιση» των «κανονικών» spam μηνυμάτων. (αλλάζει τα «βάρη» των λέξεων).

Κακόβουλο μη εμπορικό Spam:

i. Spam ως παρεμπόδιση υπηρεσίας: Sporgery (spam + forgery).
ii. Αποστολή μηνυμάτων με σκοπό, απλά να ενοχληθούν οι παραλήπτες**.**

5. Πλεονεκτήματα του email σαν εμπορικού μέσου επικοινωνίας (email marketing).

Το ηλεκτρονικό ταχυδρομείο, είναι η χαρακτηριστική εκείνη εφαρμογή του Διαδικτύου, που μείωσε ριζικά τον χρόνο που απαιτείται, τόσο για την επικοινωνία, όσο και για την αποστολή δεδομένων.

Στις μέρες μας το e-mail αποτελεί ένα εξαιρετικό εργαλείο marketing, καθώς μέσω αυτού οι εταιρείες, έχουν τη δυνατότητα να προωθήσουν τα προϊόντα τους, να επικοινωνήσουν άμεσα και γρήγορα με τους πελάτες τους και κυρίως με ελάχιστα χρήματα.

Άλλο ένα θετικό σημείο που πρέπει να συνυπολογίσουμε στα πλεονεκτήματα του e-mail, είναι το ότι σας επιτρέπει να στοχεύσετε σε ένα κοινό, το οποίο είναι έτοιμο να ακούσει τον μήνυμά σας. Μπορείτε επίσης να χωρίσετε αυτό το κοινό σε δημογραφικές ομάδες και να στείλετε διαφορετικό μήνυμα στην κάθε ομάδα ώστε να επιτύχεται καλύτερη ανταπόκριση.

Επίσης οι καμπάνιες ηλεκτρονικού ταχυδρομείου, ολοκληρώνονται μέσα σε λίγες μέρες (για εκατοντάδες χιλιάδες emails σε διαφορετικές δημογραφικές ομάδες), σε αντίθεση με τις καμπάνιες κλασσικού ταχυδρομείου, όπου απαιτούνται εβδομάδες ή ακόμη και μήνες.

Πρόσφατη έρευνα κατέδειξε πως το 78% των Αμερικανών καταναλωτών θεωρούν το e-mail ως την καλύτερο μέθοδο επικοινωνίας. Είναι πιθανό λοιπόν οι πελάτες μιας επιχείρησης να προτιμούν να λαμβάνουν τα νέα της μέσω e-mail, παρά με άλλες μορφές επικοινωνίας. Αποδεικνύεται λοιπόν πώς πέρα από ένα σημαντικό εργαλείο μείωσης του κόστους, αποτελεί και ισχυρό εργαλείο για την αύξηση της πελατειακής βάσης της εταιρείας. Άλλωστε μέσω email μια εταιρεία δύναται ακόμη, να δημιουργήσει με τους πελάτες της, πιο προσωπικές σχέσεις.

Σημαντικό είναι επίσης να τονίσουμε το ότι το email, έχει διευκολύνει πάνω από όλες τις μικρές και μεσαίες επιχειρήσεις, δίνοντας τους την δυνατότητα να υπερκαλύψουν το διαφημιστικό πλεονέκτημα των μεγαλύτερων επιχειρήσεων, με έναν ανέξοδο τρόπο.

Τα πλεονεκτήματα του e-mail marketing

i. Άμεση επικοινωνία με τους πελάτες. (business-to-consumer) & (business-to-business).

Η επικοινωνία μπορεί να διαφέρει από απλό μήνυμα κειμένου (text), μέχρι email εμπλουτισμένο με χρώματα κινούμενες εικόνες, videos, ηλεκτρονικούς καταλόγους, μουσική κ.α. Το μήνυμα επίσης μπορεί να διαφέρει και στην γλώσσα επικοινωνίας, καθώς μπορεί να είτε φιλικό, είτε καθαρά επαγγελματικό.

ii. Δυνατότητα άμεσης αμφίδρομης επικοινωνίας.

Αντίθετα με τα έντυπα διαφημιστικά μέσα, τα ραδιοφωνικά spot και την τηλεόραση, το email ενθαρρύνει την άμεση και γρήγορη απάντηση εκ μέρους του καταναλωτή στις καμπάνιες της κάθε εταιρείας.

Μια φόρμα επικοινωνίας προσαρτημένη μέσω συνδέσμου στο email, του δίνει την δυνατότητα να ζητήσεις λεπτομέρειες για οποιοδήποτε προϊόν ή υπηρεσία του έχει “τραβήξει” την προσοχή, με τρόπο εύκολο και γρήγορο.

Επίσης το e-mail ενθαρρύνει το διάλογο ανάμεσα στην εταιρεία και τους πελάτες, επιτρέποντας του να μοιράζονται απόψεις και σχόλια, είτε μέσα από έρευνες, είτε από άλλες μορφές. Με αποτέλεσμα οι εταιρείες να καταλαβαίνουν τελικά καλύτερα τις ανάγκες των πελατών τους και να επαναπροσδιορίζουν τις προωθητικές τους ενέργειες.

iii. Χαμηλά κόστη δημιουργίας καμπάνιας.

Το κόστος της δημιουργίας της ηλεκτρονικής καμπάνιας, είναι στην ουσία μονάχα το κόστος του σχεδιασμού των γραφικών της, καθώς δεν απαιτούνται καθόλου υλικά εκτύπωσης για την προσέγγιση πελατών.

iv. Χαμηλά κόστη Αποστολής.

Το e-mail marketing είναι εξαιρετικά οικονομικό, ειδικά αν συγκριθεί με άλλες μορφές marketing, καθώς το κόστος του μπορεί να κυμαίνεται από μηδενικό, ως κάποια ελάχιστα χρήματα, αν η εταιρεία επιθυμεί να χρησιμοποιήσει είτε ειδικό λογισμικό είτε τις υπηρεσίες ενός εξωτερικού e-mail solutions provider.

v. Σωστή Στόχευση.

Μια εταιρεία έχει την δυνατότητα είτε να καταρτίσει, είτε να προμηθευτεί (επι πληρωμή) λίστες με ηλεκτρονικές διευθύνσεις με εξαιρετικά ακριβή και λεπτομερειακά κριτήρια, όπως οι γεωγραφικές και δημογραφικές πληροφορίες, καταφέρνοντας με αυτό τον τρόπο είτε να προσαρμόζει την καμπάνια της στις διαφορετικές κατηγορίες, είτε να στοχεύει συγκεκριμένες μόνο κατηγορίες.

vi. Αύξηση αναγνωρισιμότητας brandname & επισκεψιμότητας ιστοσελίδας.

Προσθέτοντας σε όλα τα e-mail, υπερσυνδέσμους προς την ιστοσελίδα τους, οι εταιρείες καταφέρνουν να αυξάνουν την επισκεψιμότητας τους. Το e-mail δρα σε αυτή την περίπτωση σαν “mobile website” που διαφημίζει ειδικές προσφορές και καμπάνιες, που διαφορετικά πιθανά να περνούσαν απαρατήρητες.

Το μήνυμα κάποιας εταιρείας μπορεί να επαναπροωθηθεί εύκολα από κάποιο πελάτη σε κάποιο φίλο ο οποίος πιστεύει ότι θα ενδιαφέρεται για συγκεκριμένο προϊόν. Με αυτό τον τρόπο η εταιρεία κερδίζει μια δεύτερη ομάδα πωλήσεων (τους πελάτες), οι οποίοι δουλεύουν για αυτήν δωρεάν.

vii. Προσφέρει εύκολες & γρήγορες τροποποιήσεις στις καμπάνιες.

Σε αντίθεση με τα έντυπα διαφημιστικά φυλλάδια, τα ηλεκτρονικά μπορούν να αλλαχθούν εύκολα και γρήγορα, είτε προσθέτοντας νέες προσφορές, είτε αλλάζοντας την στρατηγική προσέγγισης των πελατών.

viii. Εύκολη επισκόπηση της καμπάνιας.

Κάνοντας χρήση των νέων τεχνολογιών μια εταιρεία μπορεί να βρει πόσοι άνθρωποι είδαν και άνοιξαν το e-mail τους, ποιο περιεχόμενο ήταν το πιο δημοφιλές και πόσες φορές το e-mail τους προωθήθηκε προς κάποια νέα ηλεκτρονική διεύθυνση.

6. Μέθοδοι που εφαρμόζονται από τους Spammers για την απόκτηση ηλεκτρονικών διευθύνσεων.

Στις μέρες μας είναι πραγματικά πολύ δύσκολο κάποιος να μην έχει έρθει αντιμέτωπος με το φαινόμενο του spam. Ο μόνος τρόπος πρόληψης που μπορεί να χρησιμοποιηθεί και να αποδειχθεί αποδοτικός, είναι το να αποφεύγεται συστηματικά, η δημοσιοποίηση των ηλεκτρονικών μας διευθύνσεων στο internet, καθώς και η κοινοποίηση τους σε μη έμπιστα άτομα.

Οι spammers άλλωστε είναι γνωστό πως έχουν αναπτύξει πολλαπλές μεθόδους απόκτησης ηλεκτρονικών διευθύνσεων, που καθιστούν την μάχη απέναντι στο spam άνιση. Οι συγκεκριμένοι μέθοδοι αναλύονται στην συνέχεια της συγκεκριμένης ενότητας.

Αποστολή μηνυμάτων σε τυχαίες διευθύνσεις.

Μια συνήθη τακτική των spammers αποτελεί η αποστολή μηνυμάτων σε τυχαίες διευθύνσεις. Βέβαια οι συγκεκριμένες διευθύνσεις δεν είναι και τόσο τυχαίες καθώς χρησιμοποιούν, συγκεκριμένα patterns, δηλαδή μια σειρά κοινών ονομάτων όπως webmaster@, admin@, info@, news@ καθώς και πληθώρα συνδυασμών, ονομάτων, γραμμάτων και αριθμών.

Στη συνέχεια στέλνουν χιλιάδες μηνύματα σε όσα domains προκύπτουν από τους συγκεκριμένους συνδυασμούς και περιμένουν οποιουδήποτε είδους απάντηση για να μπορέσουν να επαληθεύσουν με αυτοματοποιημένα προγράμματα, ότι η συγκεκριμένη διεύθυνση είναι πράγματι ενεργή.

Άλλωστε η επιλογή μιας ηλεκτρονικής διεύθυνσης του τύπου webmaster@domain.com (Συνήθης επιλογής σε νέα ιστοσελίδα) έχει τις περισσότερες πιθανότητες να γίνει «θύμα» του spam μέσα σε λίγες μόνο ώρες από την στιγμή της ενεργοποίησης της.

Ψεύτικοι Σύνδεσμοι

Μια άλλη τεχνική που χρησιμοποιείται σε συνδυασμό με την προηγούμενη είναι αυτή των ψεύτικων συνδέσμων (fake links).

Στην συγκεκριμένη μέθοδο τα μηνύματα spam, περιέχουν κάποια ψεύτικο σύνδεσμο τον οποίο καλούνται οι παραλήπτες να χρησιμοποιήσουν προκειμένου να μην ξαναλάβουν παρόμοιο μήνυμα.

Βέβαια μονάχα την συγκεκριμένη λειτουργία δεν επιτελεί ο εν λόγω σύνδεσμος καθώς όταν ο χρήστης τον επιλέγει στην ουσία ειδοποιεί τον αποστολέα ότι η ηλεκτρονική του διεύθυνση είναι τόσο υπαρκτή, όσο και ενεργή.

Στην συνέχεια η διεύθυνση τοποθετείται σε μια άλλη λίστα ενεργών διευθύνσεων για συστηματικότερη αποστολή νέων spam ή ακόμα χειρότερα, πωλείται σε άλλες εταιρείες προκειμένου να στείλουν και τα δικά τους μηνύματα, ανεπιθύμητης αλληλογραφίας.

Κακόβουλο λογισμικό

Πληθώρα ηλεκτρονικών ιών, οι οποίοι συνοδεύουν ένα μήνυμα ηλεκτρονικής αλληλογραφίας, είναι προγραμματισμένοι να ψάχνουν έγγραφα και ατζέντες που περιέχονται στον σκληρό δίσκο των μολυσμένων υπολογιστών, με σκοπό την εύρεση διευθύνσεων ηλεκτρονικής αλληλογραφίας.

Στην συνέχεια ο ιός στέλνει τις συγκεκριμένες διευθύνσεις που έχει συγκεντρώσει σε κάποιον server, από τον οποίο τις προμηθεύεται ο εκάστοτε spammer. Παράλληλα, ενσωματώνει πάντα την δυνατότητα να εξαπλώνει τον εαυτό του, στις διευθύνσεις που έχει βρει.

Μ’ αυτόν τον τρόπο ακόμα και αν έχουμε στείλει έστω και ένα ηλεκτρονικό μήνυμα σε κάποιον γνωστό μας του οποίου ο υπολογιστής είναι μολυσμένος από κάποιο σχετικό ιό, είναι εξαιρετικά πιθανό ν’ αρχίζουμε αμέσως να λαμβάνουμε μηνύματα spam.

Αυτόματη Σάρωση Ιστοσελίδων

Οι spammers τα τελευταία χρόνια εκτός από τους διάφορους ιούς, έχουν για αναπτύξει και άλλο εξειδικευμένο λογισμικό (harvesting software), το οποίο αυτόματα «σαρώνει» ιστοσελίδες (κυρίως σε forum) αναζητώντας κείμενα που να περιέχουν τον χαρακτήρα «@» ή τη λέξη «mailto:», στοιχεία που υποδηλώνουν την ύπαρξη μιας διεύθυνσης email.

Το πρόγραμμα αυτό στην συνέχεια στέλνει τα αποτελέσματα στον χρήστη του, μέσω μιας αυτοματοποιημένης και εξαιρετικά αποδοτικής διαδικασίας που δύναται να συγκεντρώσει χιλιάδες mail (από μεγάλα sites) ημερησίως.

Επιθέσεις brute-force σε mail servers.

Τέλος οι spammers προσλαμβάνουν hackers οι οποίοι εισβάλουν παράνομα στα συστήματα μεγάλων επιχειρήσεων προκειμένου να κλέψουν τα στοιχεία των πελατών τους. Θύματα των hackers πέφτουν και οι ιδιοκτήτες ιστοσελίδων που έχουν λίστες επικοινωνίας (mailing lists) και τις διαφημίζουν.

7. Εμπόριο με βάσεις δεδομένων διευθύνσεων

Είναι λογικό να σκεφτεί κάποιος πώς βάσει της εμπορικής αξίας, μιας λίστας με εκατοντάδες χιλιάδες ηλεκτρονικές διευθύνσεις, η εμπορεία τους αποτέλεσε σχετικά γρήγορα, αναπόφευκτη εξέλιξη του φαινομένου του spam.

Συνηθίζεται λοιπόν οι διευθύνσεις που συγκεντρώνει κάποιος spammer, με συνδυασμό των παραπάνω μεθόδων, να πωλούνται στην συνέχεια σε άλλους spammers.

Φτάνουμε λοιπόν στο σημείο, στο διαδίκτυο να πωλούνται λίστες με εκατομμύρια ηλεκτρονικές διευθύνσεις, σε τιμές που συχνά δεν ξεπερνούν τα 100 δολάρια. Μέσω αυτών των αγοραπωλησιών οι λίστες αυτές φτάνουν στα χέρια νέων φιλόδοξων spammers, με αποτέλεσμα να παρατηρείται μια συνεχής αύξηση του ποσοστού του spam, στο διαδίκτυο.

Επίσης θα πρέπει να σημειωθεί πως κατά την πώληση τους, οι διευθύνσεις αυτές φέρουν σε κάποιο συνοδευτικό έγγραφο την περιγραφή όπου αναφέρεται πώς οι κάτοχοι τους, έχουν αποδεχτεί να λαμβάνουν προσφορές, ισχυρισμός που σπάνια είναι αληθής.

Κεφάλαιο 3

Βασικές Αρχές Ηλεκτρονικού Ταχυδρομείου

1. Βασικές αρχές και δομή ηλεκτρονικών μηνυμάτων

Ηλεκτρονικό ταχυδρομείο ή αλλιώς e-mail ονομάζεται σήμερα βασικότερη μορφή επικοινωνίας στο διαδίκτυο. Το ηλεκτρονικό ταχυδρομείο υποστηρίζει την ανταλλαγή ηλεκτρονικών μηνυμάτων μεταξύ χρηστών, χάρη στην προσωπική ηλεκτρονική διεύθυνση του καθενός. Το περιεχόμενο του ηλεκτρονικού μηνύματος, μπορεί να είναι από κείμενο και εικόνα, μέχρι ήχος ή βίντεο.

Σε κάθε χρήστη αντιστοιχεί μια μοναδική διεύθυνση, η οποία χρησιμοποιεί αποκλειστικά λατινικούς χαρακτήρες και έχει την ακόλουθη μορφή: user@domain.gr (.gr για την περίπτωση της Ελλάδας).

Μια e-mail διεύθυνση λοιπόν αποτελείται από δύο τμήματα, τα οποία χωρίζονται μεταξύ τους από το σύμβολο «@» (προφέρεται «ατ» ή «παπάκι»).

Στο πρώτο μέρος βρίσκεται το όνομα χρήστη και στο δεύτερο μέρος δηλώνεται η ταυτότητα του παρόχου υπηρεσιών διαδικτύου ή της ιστοσελίδας στην οποία φιλοξενείται.

Για παράδειγμα, το e-mail ενός χρήστη που χρησιμοποιεί το gmail ως πάροχο, θα έχει την παρακάτω μορφή: user@gmail.com , όπου το πρώτο κομμάτι χαρακτηρίζει τον χρήστη και ονομάζεται όνομα χρήστη (login) και το δεύτερο δείχνει ότι η www.gmail.com (της εταιρείας Google), είναι ο πάροχος υπηρεσιών διαδικτύου.

Πως λειτουργεί το ηλεκτρονικό μήνυμα

Όταν κάποιος χρήστης γράφει, ένα ηλεκτρονικό μήνυμα και πατά το κουμπί «αποστολή», τότε το συγκεκριμένο μήνυμα ταξιδεύει προς τον πράκτορα μεταφοράς μηνυμάτων («Mail Transfer Agent» ή απλά MTA).

Το προς αποστολή ηλεκτρονικό μήνυμα περιλαμβάνει, τόσο την ηλεκτρονική διεύθυνση του αποστολέα όσο και την διεύθυνση του παραλήπτη.

Ακριβώς όπως και στο κανονικό ταχυδρομείο, ο πράκτορας ηλεκτρονικών μηνυμάτων εξετάζει τη διεύθυνση του παραλήπτη, και τοποθετεί στο μήνυμα

μια επικεφαλίδα (header), που περιέχει τόσο πληροφορίες σχετικά με την διεύθυνσή του αποστολέα, όσο και πληροφορίες που αφορούν το θέμα του μηνύματος και άλλες πληροφορίες.

Ένα ηλεκτρονικό μήνυμα περνά συνήθως από πολλούς πράκτορες μεταφοράς μηνυμάτων, προτού φτάσει στον προορισμό του, παίρνοντας από τον καθένα ξεχωριστά και μια ακόμα επικεφαλίδα. Βέβαια μονάχα η πρώτη από αυτές τις επικεφαλίδες περιέχει στοιχεία για τον αποστολέα καθώς οι υπόλοιπες περιγράφουν απλά την διαδρομή που ακολούθησε το μήνυμα, παρέχοντας πληροφορίες για τους ενδιάμεσους κόμβους.

Άμα τη αφίξει του ηλεκτρονικού μηνύματος στον υπολογιστή του παραλήπτη, αν ο παραλήπτης εξετάσει τα headers, μπορεί να ανακαλύψει από ποιόν υπολογιστή έχει σταλεί το μήνυμα ακόμη και αν ο αποστολέας έχει χρησιμοποιήσει, άλλη «ξένη» διεύθυνση ηλεκτρονικού ταχυδρομείου.

2. Εξάπλωση μαζικών μηνυμάτων μέσω ανοιχτών Relays

Open relays ονομάζονται οι mail transfer agents (MTA's) που δέχονται να προωθήσουν email μηνύματα, ακόμα και αν αυτά δεν προορίζονται για το δικό τους domain. Οι spammers λοιπόν χρησιμοποιούν open relays για να προωθήσουν τα κακόβουλα email τους, σε οποιαδήποτε διεύθυνση επιθυμούν.

Οι MTA's είναι συνήθως mail servers που έχουν ρυθμιστεί λάθος, γι'αυτό και επιτρέπουν την προώθηση μηνυμάτων από οποιονδήποτε host, σε οποιαδήποτε διεύθυνση, χωρίς να επιβεβαιώσουν πρώτα την ταυτότητα του αποστολέα.

3. Υπηρεσίες μαζικής αποστολής ηλεκτρονικών μηνυμάτων

Στις μέρες μας ολοένα και περισσότερες εταιρείες προσφέρουν πακέτα μαζικής αποστολής ηλεκτρονικών μηνυμάτων (emails), για διαφημιστικούς η επικοινωνιακούς σκοπούς

Στην Ελλάδα μερικές από αυτές τις εταιρείες είναι οι ακόλουθες:

i. www.myexcel.gr
ii. Ergobyte Πληροφορική (www.ergobyte.gr)

Η διαδικασία που ακολουθούν οι συγκεκριμένες εταιρείες για την χρήση των υπηρεσιών τους είναι σχετικά απλή. Οι πελάτες τους αποστέλλουν τόσο την λίστα των αποδεκτών όσο και τα μηνύματα τους.

Στην συνέχεια τα στελέχη των εταιρειών αναλαμβάνουν την αποστολή τους στο σύνολο των αποδεκτών, αποκομίζοντας τα ακόλουθα οφέλη σε σχέση με την παραδοσιακή αποστολή τους.

- Δεν υπάρχει όριο στο πλήθος των αποδεκτών.

§ Οι αποδέκτες δεν λαμβάνουν γνώση των διευθύνσεων άλλων αποδεκτών.

§ Η προσπάθεια για παράδοση του κάθε μηνύματος γίνεται συνεχόμενα και επί μία εβδομάδα για όσα μηνύματα συναντούν δυσκολία κατά την παράδοση.

Το κόστος των συγκεκριμένων υπηρεσιών υπολογίζεται κατά περίπτωση, ανάλογα με τον όγκο των μηνυμάτων, το πλήθος των αποδεκτών κ.α.

- Ενδεικτικά για 2000 παραλήπτες, 12 δελτία τον χρόνο και 250KB ανά email, το κόστος ανέρχεται στα 200€.

4. Προγράμματα μαζικής αποστολής ηλεκτρονικών μηνυμάτων

Πέρα από τις υπηρεσίες που προσφέρονται από διάφορες εταιρείες, πλέον είναι εμπορικά διαθέσιμα και λογισμικά αποστολής μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Μερικά από αυτά τα προγράμματα είναι τα ακόλουθα:

i. Emailer της WEBTECH (www.emailer.gr – www.webtech.gr)
ii. NewsMe της ONISIS web development (www.onisis.gr)

Μερικά από τα χαρακτηριστικά που προσφέρουν τα συγκεκριμένα προγράμματα, είναι τα ακόλουθα:

- Εισαγωγή παραληπτών από ASCII αρχεία με δυνατότητα αυτόματης ομαδοποίησης (Εξαγωγή από Excel, βάσεις δεδομένων κ.α.).
- Δημιουργία ομάδων με NewsLetters και Διαφημιστικές Καμπάνιες.
- Καταγραφή στατιστικών από τις προβολές της απεσταλμένης αλληλογραφίας.
- Αποστολή 2.500+ e-Mails την ώρα. (50.000 την ημέρα).

\

Κεφάλαιο 4

Προβληματισμός γύρω από το SPAM

1. Ζημιά από την οπτική γωνία του ιδιώτη τελικού χρήστη ηλεκτρονικού ταχυδρομείου

Πέρα από κάθε αμφιβολία η συσσώρευση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου επιβαρύνει τον τελικό χρήστη με πολλούς τρόπους. Αρχικά απαιτείται σημαντική σπατάλη χρόνου για την διαγραφή των ανεπιθύμητων μηνυμάτων. Δευτερευόντως, και ειδικότερα για τους λιγότερο υποψιασμένους χρήστες προκύπτουν κίνδυνοι από το ίδιο το περιεχόμενο των ανεπιθύμητων μηνυμάτων.

Αρκεί να αναλογιστούμε το ολοένα αυξανόμενο πλήθος μηνυμάτων ηλεκτρονικού ταχυδρομείου που είτε διαφημίζουν προγράμματα και υπηρεσίες, είτε αποσκοπούν στην παραπλάνηση του ιδιώτη μέσω κάποιου σημαντικού αλλά πάντοτε ψεύτικου "δολώματος". (Προτάσεις συνεργασίας, λοταρίες, κληρονομιές κ.α.).

Ακόμη ο ιδιώτης χρήστη θα πρέπει να είναι προσεκτικός, ώστε να αντιμετωπίσει τις απάτες τύπου phishing, στις οποίες το περιεχόμενο ενός spam mail ισχυρίζεται –ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα κ.λ.π.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά - οικονομικά δεδομένα.

Πιο συγκεκριμένα τα email αυτά ισχυρίζονται, ότι ο παραλήπτης απαιτείται είτε να ενημερώσει, είτε να επαληθεύσει άμεσα κάποιο από τα προσωπικά του στοιχεία, για λόγους ασφαλείας, και στην συνέχεια συγκεκριμένος σύνδεσμος τον οδηγεί σε πλαστά web sites, τα οποία μιμούνται πειστικά τους ιστότοπους υπαρκτών και αξιόπιστων οργανισμών.

Μάλιστα είναι πολύ πιθανό σε κάποιες περιπτώσεις, η αντιγραφή να είναι τόσο καλή που να «ξεγελιέται» μέχρι και ο φυλλομετρητής (π.χ. explorer) δείχνοντας στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση, του πλαστού ιστοτόπου.

Άλλοι κίνδυνοι που αντιμετωπίζει ο ιδιώτης χρήστης είναι η εγκατάσταση διαφημιζόμενων προγραμμάτων, που θα μπορούσε είτε να επιβραδύνει την απόδοση του υπολογιστή του, είτε να καταγράψει τις κινήσεις του στο διαδίκτυο, αλλά και τα προσωπικά του στοιχεία (Κωδικοί πιστωτικών καρτών, κωδικοί profil σε κοινωνικά δίκτυα κ.α.).

Σε ένα τρίτο στάδιο, η εγκατάσταση κακόβουλων προγραμμάτων μέσω των spam μηνυμάτων, θα μπορούσε εύκολα, να προκαλέσει σημαντικά κενά ασφαλείας, χρησιμοποιώντας τον υπολογιστή του ιδιώτη χρήστη, σαν "zombie", μετατρέποντας τον εν αγνοία του σε spammer.

Συμπερασματικά λοιπόν, η ανεπιθύμητη ηλεκτρονική αλληλογραφία έχει εξελιχθεί σε ένα εξαιρετικά πρόσφορο μέσο εξαπάτησης του μέσου χρήστη ηλεκτρονικού υπολογιστή.

Ακόμη οι επιβλαβείς επιπτώσεις από την ανεπιθύμητη ηλεκτρονική αλληλογραφία που περιγράφηκαν παραπάνω, αποτελούν καθημερινότητα για τους χρήστες του ηλεκτρονικού ταχυδρομείου, ενώ σύμφωνα με την Επιτροπή Ενάντια στην Ηλεκτρονική Απάτη, το 5% των ανθρώπων που λαμβάνουν τέτοια μηνύματα ανταποκρίνεται.

Ο καλύτερος τρόπος για να αποφύγει λοιπόν κάποιος το να συμπεριληφθεί σε αυτό το 5%, είναι να ενημερωθεί, να διαβάζει προσεκτικά τα μηνύματα που αναφέρονται στα οικονομικά του και βέβαια να αποφεύγει να δίνει πληροφορίες για τον τραπεζικό του λογαριασμό ή την πιστωτική του κάρτα αν δεν εξακριβώσει, σε ποιο ηλεκτρονικό τόπο βρίσκεστε.

2. Κόστος και προβλήματα των επιχειρήσεων

Η ανεπιθύμητη ηλεκτρονική αλληλογραφία συνεπάγεται σημαντικό κόστος και για τις εταιρείες - επιχειρήσεις που χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ως εργαλείο διεκπεραίωσης μερίδας των εργασιών τους.

Σύμφωνα με επίσημη έρευνα του Πανεπιστημίου του Μέριλαντ (Σχολή Επιχειρηματικών Σπουδών) και της Rockbridge Associates Inc, ο χρόνος που χάνεται στις προσπάθειες για το σβήσιμο των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, κοστίζει μόνο στις αμερικανικές επιχειρήσεις, δεκάδες δισ. δολάρια ετησίως.

Η συγκεκριμένη μελέτη, βασίστηκε στα ευρήματα τηλεφωνικής έρευνας στην οποία συμμετείχαν ενήλικοι που χρησιμοποιούν ανελλιπώς το Διαδίκτυο.

Βασικό συμπέρασμα ήταν ότι περισσότεροι από τα δύο τρίτα των συμμετεχόντων, λαμβάνουν ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου καθημερινά. Ο μέσος, όρος ανεπιθύμητων ηλεκτρονικών μηνυμάτων ανά ημέρα είναι 18,5 και ο μέσος χρόνος που αφιερώνεται καθημερινά για το σβήσιμό τους είναι 2,8 λεπτά.

Επίσης το 14% όσων λαμβάνουν ανεπιθύμητα ή διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου, τα διαβάζουν πρώτα, ώστε να δουν το περιεχόμενό τους, ενώ το 4% των παραληπτών έχουν υποκύψει και έχουν αγοράσει στη διάρκεια της περσινής χρονιάς, προϊόν το οποίο διαφημιζόταν σε ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου. Συμπερασματικά η απώλεια παραγωγικότητας, με βάση τα προαναφερθέντα νούμερα είναι ισοδύναμη με το ποσό των 21,6 δισ. δολαρίων ετησίως.

3. Κόστος και προβλήματα για τους ISPs

Στα προηγούμενα κεφάλαια αναλύθηκαν οι αρνητικές επιπτώσεις των ανεπιθύμητων μηνυμάτων αλληλογραφίας στους ιδιώτες χρήστες ηλεκτρονικού ταχυδρομείου και στις επιχειρήσεις.

Περισσότερο αρνητικά όμως και από τις δύο παραπάνω ομάδες επηρεάζονται οι ISPs. Αυτό συμβαίνει καθώς όλα τα μηνύματα ηλεκτρονικού εμπορίου που διακινούνται, είτε είναι επιθυμητά είτε είναι ανεπιθύμητα, περνούν πρώτα μέσα από τους κεντρικούς υπολογιστές τους. Είναι συνεπώς κατανοητό, ότι καλούνται να λάβουν δραστικά μέτρα τόσο για την κάλυψη των οικονομικών τους συμφερόντων, όσο και για την πλήρη κάλυψη της ασφάλειας των πελατών τους.

Ένας τρόπος εντοπισμού των αποστολέων των ανεπιθύμητων μηνυμάτων που έχουν δημιουργήσει οι ISPs είναι οι «μαύρες λίστες» που περιέχουν ηλεκτρονικές διευθύνσεις και ονόματα δικτυακών τόπων, για τους οποίους γνωρίζουν ότι ανήκουν σε spammers. Τις λίστες αυτές τις ανταλλάσσουν μεταξύ τους (π.χ. peer-to-peer), έτσι ώστε να πετυχαίνουν την καλύτερη δυνατή ενημέρωση τους.

Περεταίρω, έχουν ήδη αναπτύξει μια σειρά από τεχνικά μέτρα για τον εντοπισμό και τον αποκλεισμό των ανεπιθύμητων μηνυμάτων. Παρ' όλα αυτά όμως κανένας ISP δεν είναι ακόμα σε θέση, να μπορεί να προσδιορίσει την αποτελεσματικότητα των μεθόδων που χρησιμοποιεί, για την καταπολέμηση του προβλήματος.

Το ζήτημα όμως που προκύπτει με τις διάφορες μεθόδους φιλτραρίσματος των ηλεκτρονικών μηνυμάτων είναι το κατά πόσο μπορεί να θεωρηθεί νόμιμο και θεμιτό ένας ιδιωτικός φορέας παροχής υπηρεσιών, να αποφασίζει και να κρίνει για λογαριασμό των πελατών του, ποια μηνύματα θα παραδοθούν και ποια όχι.

Επιπλέον, κρίνεται και η αποτελεσματικότητα του εκάστοτε φίλτρου, καθώς είναι πολύ πιθανό να μη λειτουργήσει σωστά, στην περίπτωση που έχει χρησιμοποιηθεί πλαστή ταυτότητα, από τον αποστολέα των ανεπιθύμητων μηνυμάτων (spammer).

Σε κάθε περίπτωση όμως, πρέπει να τονιστεί πώς τα μέτρα που έχουν λαμβάνονται από τους ISPs, συμβάλλουν ουσιαστικά στη μείωση των ανεπιθύμητων μηνυμάτων, αλλά και στην επίπτωση του φαινομένου του spam στους πελάτες τους (τελικοί ιδιώτες χρήστες).

Μερικά στατιστικά στοιχεία:

i. Το 56% των ISPs θεωρούν το spam σοβαρή απειλή.
ii. Το 80% των ISPs προσπαθούν να έχουν σωστά DNS PTR records.
iii. Το 33% των ISPs έχει business contigency plan (Υπηρεσιακό Πλάνο Συνέχειας) και disaster recovery plan (Σχέδιο Ανάκαμψης απο Καταστροφή).
iv. Το 90% των ISPs προσφέρουν antispam filtering χωρίς χρέωση στους πελάτες τους.
v. Το 68% των ISPs μπλοκάρουν είτε την κίνηση SMTP είτε όλη την κίνηση IP από πηγή προσδιοριζόμενη ως πηγή spam.
vi. Το 81% των ISPs έχει υλοποιήσει SMTP-AUTH.
vii. Το 82% των ISPs χρησιμοποιούν blacklisting.
viii. Το 50% των ISPs χρησιμοποιούν greylisting.
ix. Το 75% των ISPs κάνουν content based filtering.
x. Το 50% των ISPs έχουν θέσει περιορισμούς στον όγκο του εξερχόμενου email.
xi. 60% των ISPs εκτελεί virus scan στην εξερχόμενη αλληλογραφία.
xii. 50% των ISPs κάνουν block στο port 25 και μόνοι οι μισοί από αυτούς υλοποιούν Message Submission (port 587).

Κεφάλαιο 5

Λήψη τεχνικών μέτρων για την καταπολέμηση του SPAM

1. Διαμόρφωση των mail servers για αποφυγή της AMA: Open Relays και Open Proxies

Οι open relays είναι mail transfer agents (MTA's) που δέχονται να προωθήσουν email μηνύματα ακόμα και αν αυτά δεν προορίζονται για το δικό τους domain.

Οι spammers χρησιμοποιούν open relays για να προωθήσουν τα email τους σε οποιαδήποτε διεύθυνση θέλουν. Οι MTA's βέβαια είναι συνήθως κανονικοί mail servers, που απλά έχουν ρυθμιστεί λάθος, γι'αυτό και επιτρέπουν την προώθηση μηνυμάτων, από οποιονδήποτε host επικοινωνεί μαζί τους.

Οι spammers από την άλλη, μπορούν είτε να συνδεθούν απευθείας στον απομακρυσμένο mail relay server, ώστε να στείλουν τα spam μηνυματά τους, είτε να συνδεθούν μέσω open proxies, ώστε να μην μπορούν να εντοπιστούν εύκολα, πετυχαίνοντας ουσιαστικά το να μένουν ανώνυμοι.

Open proxy ονομάζεται μια ανοικτή υπηρεσία στο internet που προωθεί οποιαδήποτε σχεδόν αίτηση, επιτρέποντας σε κάποιον να διατηρεί την ανωνυμία του. Οι proxy servers χρησιμοποιούνται ιδιαίτερα από τους spammers αλλά και γενικότερα από το υπόλοιπο internet undergroung, όπως οι hackers και οι crackers.

Συνήθως βέβαια οι spammers χρησιμοποιούν περισσότερους τους ενός proxy servers, καθώς όσο περισσότερα ενδιάμεσα σημεία υπάρχουν, τόσο πιο δύσκολη θα είναι η ανίχνευσή τους.

Αυτό συμβαίνει καθώς οι spammers φοβούνται την πιθανότητα να εντοπιστούν, αφού οι δραστηριότητες τους είναι παράνομες και μπορούν να επιφέρουν μεγάλα πρόστιμα αλλά και ποινές.

Με βάση τα παραπάνω μπορούμε πλέον να καταλάβουμε πόσο επιτακτική είναι η ανάγκη να είναι σωστά στημένοι οι mail servers για να μην υπάρχουν ανοιχτά open relays απο τα οποία θα δρούν οι spammers, αλλά και πόσο σημαντικό είναι να ενημερώνονται οι blacklists με τις IP διευθύνσεις των γνωστών για την διακίνηση spamming open proxies.

Στην επόμενη ενότητα θα αναφερθούμε σε επεκτάσεις πρωτοκόλλων και μεθόδους που απαιτούν την διαπίστευση των χρηστών και περιορίζουν σημαντικά τα παραπάνω φαινόμενα.

2. SMTP – POP3: Διαμόρφωση των mail servers με SMTP-Auth και POP-before-SMTP

Από τα τέλη της δεκαετίας του 1960 παρατηρείται μια συνεχώς αυξανόμενη ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ απομακρυσμένων χρηστών.

Με τα χρόνια ο αριθμός των χρηστών αλλά και των υπολογιστών αυξανόταν και έγινε σταδιακά φανερή η ανάγκη δημιουργίας ενός πρωτοκόλλου, για την ανταλλαγή των ηλεκτρονικών μηνυμάτων.

Εξέλιξη των αρχικών πρωτοκόλλων που αναπτύχθηκαν την δεκαετία του 1970, αποτελεί το SMTP. Πιο συγκεκριμένα οι ρίζες του SMTP εντοπίζονται στα πρωτόκολλα Mail Box Protocol του 1971, στο FTP Mail του 1973 αλλά και στο Mail Protocol.

Το 1982 λοιπόν ο Jon Postel, πρότεινε την δημιουργία ενός νέου πρωτοκόλλου με αποτέλεσμα να γεννηθεί το SMTP.

Το πρόγραμμα Sendmail ήταν ένα από τα πρώτα προγράμματα που υλοποίησε το SMTP, ενώ σήμερα περισσότερα από 50 προγράμματα υλοποιούν το πρωτόκολλο SMTP, είτε ως client (αποστολείς ηλεκτρονικών μηνυμάτων), είτε ως server (παραλήπτες ηλεκτρονικών μηνυμάτων).

Λειτουργία του SMTP

Για να αποστείλει ένα χρήστης κάποιο ηλεκτρονικό μήνυμα θα πρέπει να έχει πρόσβαση σε έναν SMTP Server. Πιο συγκεκριμένα ο χρήστης θα πρέπει να καθορίσει τον SMTP server που θα χρησιμοποιήσει, ώστε να μπορέσει τόσο να στείλει, όσο και να παραλάβει ηλεκτρονική αλληλογραφία.

Οι SMTP servers θα πρέπει με την σειρά τους, να έχουν ανοιχτή τουλάχιστον μια από τις πόρτες 25 και 587 (ή και τις δύο), ώστε να μπορούν μέσω αυτών να επικοινωνούν με άλλους SMTP servers

Ασφάλεια και SMTP

Ένας από τους βασικούς περιορισμούς του συγκεκριμένου πρωτοκόλλου, είναι το ότι δεν υπάρχει τρόπος αυθεντικοποίησης των χρηστών. Την αδυναμία αυτή ήρθε να καλύψει μια επέκταση του πρωτοκόλλου, που ονομάζεται **SMTP-AUTH**.

Η δυσκολία αλλά και το μειονέκτημα της συγκεκριμένης επέκτασης είναι πως είναι αρκετά πολύπλοκη για να χρησιμοποιηθεί ευρέως, γεγονός που περιορίζει την αξιοποίηση της για την αντιμετώπιση του Spamming.

Άλλωστε δεν είναι δυνατόν να γίνουν ριζικές αλλαγές στο πρωτόκολλο, καθώς αυτό σημαίνει ότι θα πρέπει οι αλλαγές αυτές να υιοθετηθούν από εκατομμύρια υπολογιστές που χρησιμοποιούν ήδη το SMTP, πράγμα αδύνατο.

Πολλοί servers επίσης παρότι διαθέτουν υπηρεσία SMTP, δεν εφαρμόζουν τους διάφορους περιορισμούς, του πρωτόκολλου και κατά συνέπεια αποθαρρύνουν όλους τους υπόλοιπους servers, που προσπαθούν να το εφαρμόσουν στο ακέραιο.

Με αυτό τον τρόπο ουσιαστικά, σχεδόν κανένας server δεν εφαρμόζει τους περιορισμούς που αναφέρονται στο πρωτόκολλο, επιτρέποντας την ανταλλαγή spam μηνυμάτων που θα μπορούσαν να είχαν αποφευχθεί.

SMTP –Auth

Η SMTP-AUTH επέκταση του SMTP παρέχει ένα μηχανισμό ελέγχου πρόσβασης, αποτελούμενη απο ένα στάδιο αυθεντικοποίησης κατά το οποίο ο χρήστης συνδέεται επιτυχώς στον mail server κατά την διαδικασία αποστολής email.
Η SMTP-AUTH μπορεί να χρησιμοποιηθεί για να αποτρέπει την χρήση του relay service από μη πιστοποιημένους χρήστες όπως οι spammers.

POP before SMTP

Η POP before SMTP η αλλιώς SMTP after POP είναι μια μέθοδος διαπίστευσης που χρησιμοποιείται από το λογισμικό του mail server.
Πιο συγκεκριμένα η POP before SMTP επιτρέπει στους χρήστες να χρησιμοποιήσουν το πρωτόκολλο SMTP από μια IP διεύθυνση αρκεί προηγουμένως να έχουν συνδεθεί επιτυχώς σε ένα POP λογαριασμό του ίδιου mail hosting παρόχου, από την ίδια διεύθυνση και σε ένα συγκεκριμένο χρονικό πλαίσιο.

Το μεγαλύτερο πλεονέκτημα της συγκεκριμένης μεθόδου αποτελεί το ότι είναι σχετικά διαφανής στον μέσο χρήστη ο οποίος συνδέεται με έναν email client.

Το μεγαλύτερο μειονέκτημα της συγκεκριμένης μεθόδου από την άλλη είναι πώς απαιτεί ένα αρκετά απαιτητικό «στήσιμο» από την πλευρά του mail hosting

παρόχου, το οποίο απαιτεί και ένα είδος καναλιού επικοινωνίας μεταξύ του POP service και του SMTP service.

3. Βασικές αρχές ταξινόμησης και φιλτραρίσματος κειμένου

Ο όρος «αυτόματη κατηγοριοποίηση κειμένου» (automatic text categorization) αναφέρεται στη διαδικασία αυτόματης κατάταξης κειμένων φυσικής γλώσσας, σε ένα προκαθορισμένο αριθμό θεματικών κατηγοριών, γνωστών εκ των προτέρων.

Ο λανθασμένος όρος «αυτόματη κατάταξη κειμένου» (automatic text classification) απο την άλλη, εμφανίζεται κυρίως στην παλαιότερη βιβλιογραφία.

Για την περαιτέρω κατανόηση του προβλήματος, είναι θεμελιώδεις δύο παρατηρήσεις:

i. Οι κατηγορίες είναι απλά συμβολικές ετικέτες, καθώς καμία επιπλέον γνώση, ως προς τη "σημασία" τους δεν θεωρείται διαθέσιμη για την κατασκευή του ταξινομητή.

ii. Η κατάταξη των κειμένων σε κατηγορίες θα πρέπει να βασίζεται στο περιεχόμενο τους και όχι στα τυχόν μεταδεδομένα που υπάρχουν σ' αυτό (π.χ. συγγραφέας, ημερομηνία δημοσίευσης, κ.α.). Δηλαδή, η κατηγοριοποίηση πρέπει να βασίζεται κυρίως σε ενδογενή γνώση (γνώση εξαχθείσα από το ίδιο το κείμενο), παρά σε εξωγενή γνώση (δεδομένα εξωτερικής πηγής).

Εφαρμογή της αυτόματης κατηγοριοποίησης κειμένου στην ανεπιθύμητη αλληλογραφία.

Η κατηγοριοποίηση κειμένου έχει ιστορία τεσσάρων τουλάχιστον δεκαετιών, κατά τη διάρκεια των οποίων έχει δώσει ένα αριθμό από διαφορετικές εφαρμογές.

Στις μέρες μας, είναι γεγονός πως το ηλεκτρονικό ταχυδρομείο αποτελεί σήμερα, μία από τις πιο γρήγορες οικονομικές και εύχρηστες μορφές επικοινωνίας. Τα σαφή πλεονεκτήματα που παρουσιάζει το έχουν κάνει ιδιαίτερα δημοφιλές, όχι μόνο για τους απλούς χρήστες που θέλουν να επικοινωνούν με φίλους και συναδέλφους τους, αλλά και για εταιρείες, οι οποίες βρήκαν δελεαστική την προοπτική να διαφημίζουν τα προϊόντα ή τις υπηρεσίες τους μέσω ηλεκτρονικών μηνυμάτων.

Η ύπαρξη λογισμικού μαζικής αποστολής e-mails, η αυξανόμενη διαθεσιμότητα τεράστιων λιστών από ηλεκτρονικές διευθύνσεις – οι οποίες έχουν συλλεχθεί κυρίως από ιστοσελίδες και αρχεία ομάδων συζήτησης (newsgroups) – και ο συνεχής πολλαπλασιασμός των εταιρειών που επιλέγουν να δραστηριοποιηθούν στο Διαδίκτυο έχουν διογκώσει υπερβολικά το πλήθος των διαφημιστικών e-mails, τα οποία στέλνονται "τυφλά" σε χιλιάδες υποψήφιους πελάτες ταυτόχρονα, με ελάχιστο κόστος και κόπο.

Σε αυτόν ακριβώς το τομέα βρίσκει στις μέρες πρόσφορο έδαφος να εφαρμοστεί αποδοτικά και η κατηγοριοποίηση κειμένων, καθώς το περιεχόμενο των συγκεκριμένων μηνυμάτων ποικίλει, από σχήματα γρήγορου πλουτισμού ("get-rich-quick") και πληροφορίες πρόσβασης σε πορνογραφικούς δικτυακούς τόπους, μέχρι μη ζητηθείσες διαφημίσεις για συγκεκριμένα προϊόντα. Καλείται λοιπόν η κατηγοριοποίηση κειμένων να διαχωρίσει τα συγκεκριμένα μηνύματα σε δύο μεγάλες κατηγορίες:

i. Επιθυμητή Αλληλογραφία
ii. Ανεπιθύμητη Αλληλογραφία

Το πρόβλημα της εφαρμογής της κατηγοριοποίησης κειμένου στην αντιμετώπιση του spamming, περιλαμβάνει 2 βασικές παραμέτρους.

i. Η πρώτη παράμετρος αφορά την επιλογή των κατάλληλων features. Δηλαδή εστιάζει στον καθορισμό των κατάλληλων χαρακτηριστικών γνωρισμάτων, για την ακριβέστερη ταξινόμηση του κειμένου.

ii. Η δεύτερη τεχνική από την άλλη, αφορά την επιλογή του κατάλληλου ταξινομητή, με επικρατέστερους, τον Naive Bayes, το Vector Space Model και τον Nearest Neighbor.

4. Μέθοδοι φιλτραρίσματος βασισμένοι σε κανόνες

Επιπλέον δίνεται οι δυνατότητα σε χρήστες που δεν επιθυμούν να ενεργοποιήσουν κάποιο φίλτρο ανεπιθύμητης αλληλογραφίας να δημιουργήσουν κανόνες για τη διαχείριση των μηνυμάτων που λαμβάνουν.

Οι κανόνες αυτοί λειτουργούν βάσει της βαθμολογίας που λαμβάνουν τα μηνύματα, από το σύστημα διαχείρισης του ηλεκτρονικού ταχυδρομείου. Κάθε εισερχόμενο μήνυμα λοιπόν, λαμβάνει ένα βαθμό από 0 έως 9, ο οποίος αντιστοιχεί στο επίπεδο βεβαιότητας (0 = κανονικό μήνυμα, ενώ 9 = spam) του κατά πόσο το συγκεκριμένο email, είναι spam ή όχι.

Ο βαθμός αυτός καταγράφεται στα headers (επικεφαλίδες) του μηνύματος με τη ακόλουθη μορφή:

X-MS-Exchange-Organization-SCL: N (όπου N από 0 έως 9)

Ακολουθεί ένα παράδειγμα κανόνα:

Μηνύματα με τις φράσεις:

"X-MS-Exchange-Organization-SCL: 9"
ή "X-MS-Exchange-Organization-SCL: 8"
ή "X-MS-Exchange-Organization-SCL: 7"
ή "X-MS-Exchange-Organization-SCL: 6"
ή "X-MS-Exchange-Organization-SCL: 5"

Στις επικεφαλίδες του μηνύματος να μετακινηθούν στο φάκελο «Ανεπιθύμητη Αλληλογραφία».

Ο συγκεκριμένο κανόνας θεωρεί ώς spam οποιοδήποτε μήνυμα λάβει βαθμολογία μεγαλύτερη ή ίση του 5.

5. Bayes φιλτράρισμα

Πολύ γνωστή επίσης μέθοδος, είναι το φιλτράρισμα του email με βάση το θέμα και το περιεχόμενο του, με λέξεις κλειδιά οι οποίες έχουν βρεθεί σε προηγούμενα email και τους έχουν δοθεί κάποιες πιθανότητες να θεωρηθούν ή όχι spam.

Η μέθοδος αυτή βασίζεται στο θεώρημα τους Bayes, το οποίο και αναφέρει ότι η πιθανότητα ένα email να είναι spam, είναι ίση με την πιθανότητα να βρεθούν συγκεκριμένες λέξεις σε ένα email spam, επί την πιθανότητα κάθε email να είναι spam, δια την πιθανότητα να βρεθούν οι συγκεκριμένες λέξεις σε οποιοδήποτε email.

Πιο συγκεκριμένα ο μαθηματικός τύπος του θεωρήματος του Bayes είναι:

$$Pr(spam|words)= Pr(words|spam)\cdot Pr(spam)/Pr(words)$$

Ένα από τα πλεονεκτήματα του θεωρήματος Bayes, είναι πως οι πιθανότητες των λέξεων να θεωρηθούν spam, είναι μοναδικές για κάθε χρήστη, και προσαρμόζονται με το πέρασμα κάποιου χρονικού διαστήματος, ανάλογα με το πόσα email δέχεται ο χρήστης, με αποτέλεσμα την αυξημένη αξιοπιστία της πιθανότητας του ποτέ μια λέξη μπορεί να θεωρηθεί spam και πότε όχι.

Ένα ακόμα πλεονέκτήμα της συγκεκριμένης μεθόδου είναι, το ότι μπορεί μια να λέξη να θεωρηθεί ως spam, αλλά όχι απαραίτητα και όλο το email. Αυτό συμβαίνει γιατί κατά το φιλτράρισμα, κάθε λέξη ξεχωριστά ελέγχεται για το εάν υπάρχει πιθανότητα η όχι, να θεωρηθεί spam.

6. Φίλτρα βασισμένα σε δίκτυα Peer-to-Peer (Collaborative Filtering)

Το Collaborative Filtering δεν είναι τίποτα άλλο παρα φίλτρα βασισμένα στις αρχές του peer-to-peer, τα οποία χρησιμοποιούν την γνώση που αποκόμισαν απο τα report συγκεκριμένων χρηστών, για να αποτρέψουν την μετάδοση συγκεκριμένων emails, στα mailboxes χιλιάδων άλλων χρηστών.

Οι κανόνες των συγκεκριμένων φίλτρων αναπτύσσονται συνεργατικά, και ανταλλάσσονται όπως ακριβώς ανταλλάσσονται και τα αρχεία στα peer to peer διαμοιρασμού αρχείων. Δεν είναι άλλωστε η πρώτη φορά που τεχνολογίες επικοινωνίας και διασκέδασης του internet, υιοθετήθηκαν και για τα θέματα ασφαλείας, εν προκειμένοις του ηλεκτρονικού ταχυδρομείου.

7. Blacklists/Whitelists: Realtime Blackhole Lists - Domain Name System Lists (RBLs – DNS)

Whitelists/Blacklists:

Οι whitelists είναι λίστες που σας δίνουν την δυνατότητα να ορίζετε από ποιες διευθύνσεις θέλετε να λαμβάνετε e-mails, δηλαδή ποιές διευθύνσεις δεν αποτελούν πηγή spamming.
Οι blacklists από την άλλη περιέχουν διευθύνσεις e-mails οι οποίες αποτελούν πηγή spamming και τις οποίες ο μέσος χρήστης επιθυμεί να «μπλοκάρει».
Η τεχνική των whitelists είναι ιδιαίτερα χρήσιμη, ώστε να μη χάνονται μηνύματα από γνωστούς, φίλους και συνεργάτες καθώς και για την ανίχνευση μηνυμάτων spam που δεν έχουν σταθερή διεύθυνση αλληλογραφίας.

DNS Blacklists

Μια πολύ γνωστή μέθοδος καταπολέμησης του email spam, είναι τα επονομαζόμενα DNS Blacklists (DNSBL), τα οποία βασίζονται στο Σύστημα Ονομάτων Τομέα (Domain Name System, DNS).

Τα DNSBLs τρέχουν από ανεξάρτητους οργανισμούς οι οποίοι συνιστούν μια στρατηγική συμμαχία για την καταπολέμηση των spam emails.

Η λειτουργία τους είναι σχετικά απλή, καθώς όταν ένα σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου, αντιληφθεί πως δέχεται πολλά spam emails, από συγκεκριμένη IP διεύθυνση του internet, τότε στέλνει την συγκεκριμένη διεύθυνση σε ένα η περισσότερα DNSBLs, με αποτέλεσμα την επόμενη φορά που φτάσει κάποιο email απο την συγκεκριμένη διεύθυνση, στο σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου να θεωρηθεί αυτόματα ως spam.

Γνωστά DNSBL είναι τα ακόλουθα:

i. Spamhaus
ii. Spam and Open Relay Blocking System (SORBS).

Το μεγάλο πλεονέκτημα των DNSBLs είναι ότι οι IP διεύθυνσεις που είναι υπεύθυνες για spam emails υπάρχουν διαθέσιμες σε κάποιο συγκεκριμένο σημείο, όπου έχουν πρόσβαση εκατομμύρια συστήματα διαχείρισης

ηλεκτρονικού ταχυδρομείου, με αποτέλεσμα την πιο αξιόπιστη και αποδοτική αποφυγή των spam emails.

RBLs

Λίστες που ενημερώνονται σε πραγματικό χρόνο και περιέχουν διευθύνσεις IP από spammers καθώς και λίστες με συνδέσμους (URIBL) που περιέχονται στα μηνύματα spam.

Οι λίστες αυτές χρησιμοποιούνται πολύ συχνά από τους παροχείς υπηρεσιών e-mails, για την απόρριψη των μηνυμάτων που προέρχονται από τις συγκεκριμένες διευθύνσεις ή των μηνυμάτων που περιέχουν συνδέσμους (links) σε αυτές.

Σημαντικές Λίστες

a. **zen.spamhaus.org:**
Η SBL λίστα είναι μια realtime βάση δεδομένων, των IP διευθύνσεων ελεγμένων πηγών spam, η οποία συντηρείται από την ομάδα έργου Spamhaus και παρέχεται ως ελεύθερη υπηρεσία, ώστε να βοηθήσει τους διαχειριστές ηλεκτρονικού ταχυδρομείου, να διαχειριστούν καλύτερα τις ροές εισερχόμενων μηνυμάτων e-mail.
http://www.spamhaus.org/zen

b. **list-dsbl-org.sch.gr**
Η λίστα DSBL περιέχει τις IP διευθύνσεις των IP servers που έχουν αποστείλει ειδικά test μηνύματα στο listme@listme.dsbl.org. Αυτό συμβαίνει μόνο σε servers που επιτρέπουν ελεύθερα την αποστολή μηνυμάτων χωρίς μέτρα ασφαλείας. (open relays, open proxies κ.α).

c. **bl.spamcop.net http://spamcop.net**
Η λίστα Spamcop περιέχει τις IP διευθύνσεις των servers που διακινούν μηνύματα, που έχουν σημανθεί ως spam, από τους χρήστες του SpamCop.

8. **dul.dnsbl.sorbs.net: http://www.dnsbl.sorbs.net**

Η λίστα Sorbs περιέχει τις IP διευθύνσεις των servers που επιτρέπουν ελεύθερα την αποστολή μηνυμάτων χωρίς μέτρα ασφαλείας.
(open relays, open proxies κ.α).

8. Εναλλακτικές μέθοδοι αποφυγής SPAM

Στο συγκεκριμένο κεφάλαιο θα εξετάσουμε μια σειρά από εναλλακτικές μεθόδους αποφυγής του SPAM, με το ενδιαφέρον μας να εκτείνεται από το Project Lumos, μέχρι το φιλτράρισμα βάσει της προηγούμενης αποδοχής του αποστολέα και το SpamCop.net

8.1. Το έργο Lumos

Το "Project Lumos" είναι ένα βασισμένο σε καταγραφές μοντέλο το οποίο αναπτύχθηκε για να καταπολεμήσει το spam, «κλειδώνοντας» το ποιοί αποστολείς, είναι υπεύθυνοι για ποιά μηνύματα.
Πιο συγκεκριμένα το Project Lumos, εγγυάται την πιστοποίηση – αυθυντικοποίηση του αποστολέα, καθώς και την διαφάνεια κατα την αποστολή του μηνύματος, απαιτώντας από τους αποστολείς να συμμορφωθούν με τις υποδείξεις του:

a. Χρήση βέλτιστων πρακτικών αποστολής email.
b. Πιστοποίηση της ταυτότητας τους (π.χ. ψηφιακή υπογραφή)
c. Παρακολούθηση της κινητικότητας των email.

Το Project Lumos αναπτύσσεται από ανεξάρτητη λειτουργικές δομές καταγραφής και χρησιμοποιεί ένα συνονθύλευμα σύγχρονών τεχνολογιών για την καταπολέμηση του spam.

Περισσότερες πληροφορίες για το Project Lumos, μπορείτε να βρείτε στην ακόλουθη ιστοσελίδα:
http://www.espcoalition.org/project_lumos.php

8.2. Φιλτράρισμα βασισμένο στην προηγούμενη αποδοχή του αποστολέα.

Το βασισμένο στην προηγούμενη αποδοχή του αποστολέα φιλτράρισμα, χρησιμοποιεί 2 αποθήκες διευθύνσεων ηλεκτρονικού ταχυδρομείου.

Κάθε φορά που ο χρήστης λαμβάνει ένα νέο mail, χαρακτηρίζει τον αποστολέα του μηνύματος ως «έμπιστο» ή spammer. Σε περίπτωση που μια διεύθυνση χαρακτηριστεί ως «έμπιστη», τότε οποιοδήποτε email ληφθεί από αυτήν στο μέλλον, θα χαρακτηρίζεται με την σειρά του ως «έμπιστο».

Από την άλλη αν κάποιος αποστολέας και κατ' επέκταση η ηλεκτρονική του διεύθυνση χαρακτηριστεί – σημανθεί ως «μη-έμπιστη», «κακόβουλη», «spam», οποιοδήποτε mail ληφθεί στο μέλλον από την συγκεκριμένη διεύθυνση, θα χαρακτηρίζεται με την σειρά του αυτόματα ως «spam».

8.3. SpamCop.net

Το SpamCop είναι μια από τις πρώτες αν όχι η πρώτη υπηρεσία αναφοράς Spam. Η λειτουργία του είναι να προσδιορίζει την προέλευση των ανεπιθύμητων ηλεκτρονικών μηνυμάτων και να τις αναφέρει στην συνέχεια στον αρμόδιο πάροχο.

Αναφέροντας τα Spam μηνύματα, το SpamCop και οι χρήστες του συμβάλλουν τόσο στην επίλυση του προβλήματος, μέσω τελικής διαμαρτυρία για συγκεκριμένους spammers, όσο και στην ενημέρωση των συστημάτων διαλογής μηνυμάτων Spam.

Εξυπακούεται πώς αποτελεί μια πολύ καλή πρακτική για τον μέσο χρήστη, η δωρεάν εγγραφή στην υπηρεσία Spamcop.net, καθώς μέσω αυτής της υπηρεσίας μπορεί να ενεργοποιήσει την προβολή όλων των κεφαλίδων (headers), για τα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνει.

Ακολούθως για κάθε μήνυμα spam που θα δέχεται, θα μπορεί να το προωθήσει με την μορφή συνημμένου στο spamcop, όπου θα τυγχάνει της δέουσας επεξεργασίας, ώστε να ανιχνευθεί η πηγή του.

Τέλος μόλις η παραπάνω διαδικασία ολοκληρωθεί, ο χρήστης λαμβάνει μια ειδοποίηση από το Spamcop, όπου προτρέπεται να ακολουθήσει ένα σύνδεσμο, από τον οποίο θα μπορέσει να αποστείλει την καταγγελία του, πλήρως τεκμηριωμένη.

Περισσότερες πληροφορίες για τον SpamCop.net, μπορείτε να βρείτε στην ακόλουθη διεύθυνση:
http://www.spamcop.net/

Κεφάλαιο 6

Anti-Spam Λογισμικό (Software)

1. Anti-Spam Λογισμικό (Software)

Στο συγκεκριμένο κεφάλαιο θα ασχοληθούμε με τα anti-spam προγράμματα, τα οποία αποτελούν ένα σημαντικό σύμμαχο μας, απέναντι στην μάστιγα του spam.

Θα αναλύσουμε λοιπόν, τόσο εμπορικά προϊόντα όσο και ελεύθερο λογισμικό, καθένα εκ των οποίων χρησιμοποιεί και διαφορετική λογική – μεθοδολογία αντιμετώπισης του spam.

Στις επόμενες σελίδες λοιπόν θα αναφερθούμε σε μια σειρά από προγράμματα όπως:

i. SpamAssassin
ii. SpamEater
iii. Spamihilator
iv. SpamPal
v. SPAMfighter
vi. SpamKiller
vii. Cloudmark

Για τα συγκεκριμένα προγράμματα, θα επιχειρήσουμε πέρα από την παράθεση των βασικότερων λειτουργιών τους, να παραθέσουμε και συνδέσμους, μέσω των οποίων θα μπορεί ο αναγνώστης της εργασίας να αναζητήσει περισσότερες πληροφορίες.

Τέλος η παρουσίαση κάθε προγράμματος θα συνοδεύεται από ένα χαρακτηρισμό για το αν το πρόγραμμα είναι εμπορικά διαθέσιμο, ή αν αποτελεί ελεύθερο λογισμικό και αν ανήκει στην πρώτη περίπτωση, θα συνοδεύεται και από την τιμή του.

1.1. SpamAssassin

Το SpamAssassin είναι ίσως η καλύτερη εφαρμογή αναγνώρισης μηνυμάτων spam και σίγουρα μια από τις πιο χρησιμοποιημένες, από όσες κυκλοφορούν στο χώρο του ελεύθερου λογισμικού.

Το SpamAssassin είναι γραμμένο σε Perl και συνεργάζεται με ένα μεγάλο πλήθος προγραμμάτων για mail gateways. Το MailScanner ενσωματώνει προαιρετικά τη δυνατότητα χρήσης του SpamAssassin ως εξωτερικού προγράμματος ελέγχου spam, για τα καλύτερα δυνατά αποτελέσματα.

Τα spam email ως γνωστόν ακολουθούν συγκεκριμένα μοτίβα στη διάρθρωση αλλά και το είδος των στοιχείων που φέρουν, για αυτόν ακριβώς τον λόγο το SpamAssassin, χρησιμοποιεί μια ενσωματωμένη λίστα σύγκρισης του κάθε μηνύματος με πρότυπα spam μηνυμάτων, ώστε να αποδώσει θετικούς ή αρνητικούς βαθμούς στο μήνυμα που καλείται να χαρακτηρίσει.

Τα tests που περιλαμβάνει η λίστα αφορούν κυρίως την κεφαλίδα (header) και το περιεχόμενο (body) του μηνύματος, επεκτείνονται όμως και σε άλλους τομείς, που αφορούν από τον εντοπισμό συγκεκριμένων φράσεων, μέχρι το είδος του email – client, που χρησιμοποιήθηκε για την αποστολή.

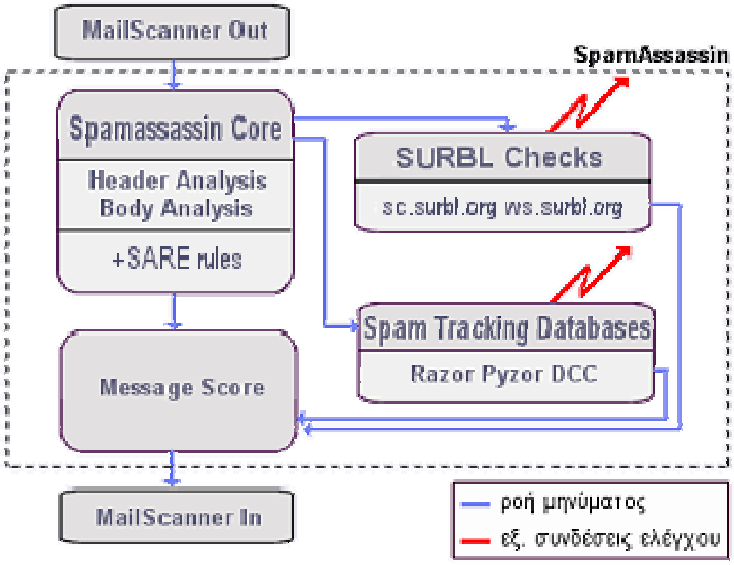
Όταν τμήματα του υπό εξέταση μηνύματος ταυτίζονται με spam πρότυπα, τότε προστίθενται βαθμοί στη συνολική βαθμολογία, ενώ στην αντίθετη περίπτωση, αφαιρούνται βαθμοί από τη συνολική βαθμολογία. Αν το μήνυμα ξεπεράσει ένα κάποιο ανώτερο όριο βαθμολογίας (threshold), το οποίο καθορίζεται είτε από τον χρήστη, είτε από τον διαχειριστή του συστήματος, τότε χαρακτηρίζεται ως spam.

Το όριο αυτό μπορεί να κυμανθεί από πολύ "αυστηρές" τιμές, μέχρι πολύ "ελαστικές", ανάλογα με τις ανάγκες κάθε χρήσης.

Για την ελαχιστοποίηση εμφάνισης ψευδών θετικών (false positives) και ψευδών αρνητικών (false negatives) βαθμών και για την καλύτερη προσαρμογή στο είδος των μηνυμάτων που λαμβάνονται κάθε φορά, το SpamAssassin περιλαμβάνει σύστημα αυτοεκμάθησης που στηρίζεται στην ανάλυση Bayes, πάνω σε μεγάλο δείγμα spam και μη spam μηνυμάτων.

Το δείγμα αυτό δημιουργείται σταδιακά, βάσει της χρήσης και περιλαμβάνει μηνύματα που βρίσκονται σε συγκεκριμένα όρια βαθμολογίας, ώστε να μπορούν να αποτελέσουν, έγκυρα δείγματα spam και μη spam email.

Τέλος το SpamAssasin μπορεί να χρησιμοποιήσει ταυτόχρονα και άλλα προγράμματα ή τεχνολογίες εντοπισμού spam και να ενσωματώσει τα αποτελέσματά τους στο σύστημα message scoring που διαθέτει.



[Η εικόνα προέρχεται από το mail.metal.ntua.gr ένα site που αναπτύχθηκε για την υποστήριξη των υπηρεσιών ηλεκτρονικής αλληλογραφίας της Σχολής Μηχανικών Μεταλλείων Μεταλλουργών του Ε.Μ.Π.]

Η διεύθυνση του SpamAssassin είναι: http://spamassassin.apache.org

Τιμή: Δωρεάν

1.2. SpamEater

Το SpamEater Pro είναι ένα πρόγραμμα της High Mountain Software, το οποίο είδε προσφάτως την τρίτη έκδοσή του. Πρόκειται για ένα εξαιρετικό πρόγραμμα, το οποίο αναλαμβάνει να καθαρίσει τα e-mail από τα μηνύματα spam προτού ακόμη τα κατεβάσει ο τελικός χρήστης στον υπολογιστή του.

Σημαντικό πλεονέκτημα του SpamEater Pro, είναι πως τα αποτελέσματα ακρίβειας που προσφέρει, φτάνουν κοντά στο 95%. Για την λειτουργία του χρησιμοποιεί μια σειρά από κανόνες, με βάση τους οποίους αναγνωρίζει τα e-mail εκείνα που δεν προορίζονται μόνο για κάποιο συγκεκριμένο χρήστη, αλλά για όλους τους παραλήπτες ενός καταλόγου.

Η standard έκδοση του SpamEater είναι freeware, ενώ η Pro είναι shareware.

Το πρόγραμμα μπορεί να μεταφορτωθεί από τη διεύθυνση της εταιρίας στο Internet: http://www.hms.com

1.3. Spamihilator

Το Spamihilator είναι ένα anti-spam freeware λογισμικό για να φιλτράρεται τα email σας. Είναι συμβατό με το λειτουργικό σύστημα των Windows (XP, Vista, 7), ενώ συνεργάζεται και με τα πιο γνωστά προγράμματα αλληλογραφίας όπως, το Outlook 2000/XP/2003/Express, Eudora, Mozilla, Netscape, IncrediMail, Pegasus Mail, Phoenix Mail, Opera κ.λ.π.

Το Spamihilator δέχεται εκπαίδευση ενώ μπορεί ακόμα να ρυθμίζει αυτόματα τις παραμέτρους του, ώστε να αναγνωρίζει πιο αποτελεσματικά τα ανεπιθύμητα email.

Το Spamihilator χρησιμοποιεί ένα ευφυέστατο φίλτρο (Bayesian Filter), μια επεξεργάσιμη λίστα από λέξεις κλειδιά καθώς και μια "μαύρη λίστα", ώστε να ελέγχει τα εισερχόμενα μηνύματα για spam. Το φίλτρο που χρησιμοποιεί υπολογίζει την πιθανότητα είναι ένα νέο μήνυμα, μήνυμα spam και αν αυτή η πιθανότητα ξεπερνά μια οριακή τιμή κατώφλι (threshold) χαρακτηρίζει το συγκεκριμένο μήνυμα ώς spam.

Επίσημη ιστοσελίδα του Spamihilator:
http://www.spamihilator.com/

Σελίδα μεταφόρτωσης:
http://www.spamihilator.com/download

Τιμή: Freeware

1.4. SpamPal

Το SpamPal είναι ένα δωρεάν anti-spam φίλτρο το οποίο στέκεται ανάμεσα στο πρόγραμμα διαχείρισης της αλληλογραφίας και στην POP3/IMAP4 θυρίδα ηλεκτρονικής αλληλογραφίας, τα mail που είναι χρήσιμα για τον χρήστη του απο τα άχρηστα spam.

Τα βασικά χαρακτηριστικά του SpamPal είναι τα ακόλουθα:

i. Πλήρως παραμετροποιήσιμη αναζήτηση σε μαύρες λίστες (blackhole lists (dnsbl)).
ii. Τοπικές μαύρες (black) and άσπρες (white) λίστες.
iii. Αυτόματη εισαγωγή στην άσπρη λίστα των φίλων.
iv. Υποστηρίζει πολλαπλούς POP3/IMAP4 servers.
v. Υποστηρίζει APOP αυθεντικοποίηση.
vi. Δωρεάν υποστήριξη.
vii. Υποστήριξη πολλών διαφορετικών γλωσσών.

Επίσημη ιστοσελίδα του SpamPal:
http://spampal.sanesecurity.com

Τιμή: Δωρεάν

1.5. SPAMfighter

Το SPAMfighter είναι ένα εργαλείο το οποίο χρησιμοποιείται για να σταματήσει το Spam από εκατομμύρια επιχειρήσεις και ιδιώτες είτε σε Η/Υ, είτε σε Διακομιστές, σε πάνω 224 χώρες.

Εάν ένας SPAMfighter λάβει ένα μήνυμα spam που δεν εντοπίστηκε από τον SPAMfighter, ο χρήστης το επισημαίνει με ένα μόνο κλικ, και αυτόματα το συγκεκριμένο μήνυμα μπλοκάρεται, για όλους τους υπόλοιπους χρήστες του SPAMfighter, μέσα σε μερικά δευτερόλεπτα.

Πιο συγκεκριμένο το SPAMfighter Standard, είναι ένα δωρεάν εργαλείο αντιμετώπισης του Spam για Outlook, Outlook Express, Windows Mail και Mozilla Thunderbird.

Κατεβάζοντας το SPAMfighter Pro, ο καθένας μπορεί να το δοκιμάσει για 30 ημέρες δωρεάν. Οι ιδιώτες χρήστες μετα την λήξη της δοκιμαστικής περιόδου, λαμβάνουν αυτομάτως και εντελώς δωρεάν τον SPAMfighter Standard, ενώ μπορούν ακόμα να αναβαθμιστούν στον SPAMfighter Pro, ο οποίος προσφέρει πολύ περισσότερες δυνατότητες για μόλις €25.

Χαρακτηριστικά

i. Βραβευμένη τεχνολογία αντί-spam.

ii. Προστασία εναντίον απάτης «phishing», κλοπή ταυτότητας και άλλες απάτες που αφορούν την ηλεκτρονική αλληλογραφία.

iii. Μοναδικό εργαλείο φίλτρου γλώσσας: Σταμάτημα των ανεπιθύμητων email σε μη κατανοητές γλώσσες.

iv. Αυτόματη Προστασία «real mail».

v. Καταχώρηση πεδίων ορισμού - διευθύνσεων emails σε μαύρη λίστα.

vi. Αναφορά Κατάχρησης Spam με ένα κλικ - Εκδικηθείτε τώρα!.

vii. Αυτόματη διαχείριση Άσπρης λίστας.

viii. Εγγυημένο προσωπικό απόρρητο.

ix. Υποστήριξη πολλών διαφορετικών γλωσσών: **Ελληνικά**, Αγγλικά, Βουλγαρικά, Γαλλικά, Γερμανικά, Δανέζικα, Ιαπωνέζικα, Ισπανικά, Ιταλικά, Κινέζικα, Νορβηγικά, Ολλανδικά, Πορτογαλικά, Ρωσικά, Σουηδικά και Σουόμι

Απαιτήσεις

Λειτουργικό Σύστημα : 98, ME, 2000, XP και Vista (Outlook και Windows Mail)

Εφαρμογή Email : Outlook 2000/2002(XP)/2003/2007, ή Outlook Express 5.5, ή Windows Mail (32 bit), ή Mozilla Thunderbird.

Απαιτούμενη Μνήμη : Ελάχιστη μνήμη 128 MB

Απαιτούμενος Χώρος Δίσκου : 10 MB

Η διεύθυνση του SPAMfighter είναι: www.spamfighter.com

Τιμή:
SPAMfighter Standard: Δωρεάν
SPAMfighter Pro: €25

1.6. SpamKiller

Ένα αρκετά πλήρες πρόγραμμα αντιμετώπισης των junk και spam mails, είναι το SpamKiller της McAfee, το οποίο ξεχωρίζει χάρις σε ένα εξαιρετικό σετ χαρακτηριστικών.

Η εξαιρετική του δυνατότητα ανίχνευσης και παρεμπόδισης του spam mail, οφείλεται στα προηγμένα τεχνολογικά "έξυπνα" φίλτρα που χρησιμοποιεί τα οποία με την σειρά τους βασίζονται σε συνδυασμούς κριτηρίων που αφορούν στον έλεγχο του περιεχομένου του μηνύματος, τη διεύθυνση του αποστολέα, το θέμα του μηνύματος, αλλά ακόμα και την προέλευσή του (χώρα προέλευσης αποστολέα, κόμβος κ.τ.λ.), στοιχεία που προκύπτουν μέσα από την ανάλυση του header του μηνύματος.

Σημαντικό πλεονέκτημα επίσης του SpamKiller είναι το ότι ενσωματώνεται στην επιθυμητή απο τον χρήστη εφαρμογή διαχείρισης ηλεκτρονικού ταχυδρομείου. Το SpamKiller υποστηρίζει προγράμματα όπως το Microsoft Outlook, Netscape Mail, Eudora κ.ά.

Επίσης το συγκεκριμένο πρόγραμμα δίνει στο χρήστη του τη δυνατότητα διαχείρισης, αξιολόγησης και ανάλυσης των εισερχόμενων μηνυμάτων πολλαπλών λογαριασμών, ενώ έχει ακόμα και τη δυνατότητα αναγνώρισης και “θετικής” επισήμανσης των e-mails που προέρχονται από φιλικά σας πρόσωπα.

Ο προχωρημένος χρήστης μπορεί μέσω του Spam Killer να δημιουργήσει ένα παραμετροποιημένο φίλτρο αντιμετώπισης spam, έτσι ώστε να μπορεί να αντιδράσει σε "ασυνήθιστες" περιπτώσεις spammers.

Τέλος, το συγκεκριμένο πρόγραμμα παρουσιάζει λειτουργίες αναφοράς των spam mails σε web sites και mail service providers, προκειμένου να αλλάξει προς το καλύτερο η κατάσταση με το spam.

ΚΑΤΑΣΚΕΥΑΣΤΗΣ: Network Associates Inc.,
http://www.mcafee-at-home.com/

ΔΙΑΘΕΣΗ: Interaxon,
210 - 6801015,
http://www.interaxon.gr/
ΤΙΜΗ: 23,5

1.7. Cloudmark

Το Cloudmark είναι ένα από τα αποτελεσματικότερα διαθέσιμα, αντι-spam προϊόντα στην αγορά. Το Cloudmark χρησιμοποιεί ένα φίλτρο προστασίας που του προσφέρει σχεδόν 98% επιτυχία αναγνώρισης ενός spam mail, ενώ το ποσοστό των false positives του, σύμφωνα με τους ερευνητές του, αγγίζει το μηδέν.

Το συγκεκριμένο προϊόν δεν απευθύνεται μόνο σε ιδιώτες τελικούς χρήστες, αλλά και σε μεγάλες επιχειρήσεις, οργανισμούς η ακόμα και υπουργεία που επιθυμούν να απαλλαχτούν μια και καλή από το spam.
Για αυτό τον λόγο παρουσιάζει και πολλές διαφορετικές εκδόσεις ανάλογα με την ανάγκη χρήσης κάθε φορά.

Η διεύθυνση του Cloudmark είναι:
www.cloudmark.com

Κεφάλαιο 7

Συστάσεις Συμπεριφοράς προς Αποφυγή και Άμυνα

1. Μέτρα πρόληψης

Στην συγκεκριμένη ενότητα αναλύονται μέτρα πρόληψης αλλά και τακτικές αντιμετώπισης του spam, βάσει των οποίων θα μπορέσουν οι ιδιώτες χρήστες του ηλεκτρονικού ταχυδρομείου, να αποφύγουν τις κακοτοπιές.

Πιο συγκεκριμένα:

i. Θα πρέπει να αποφεύγεται η εισαγωγή του προσωπικού e-mail σε δικτυακούς τόπους (web sites) εφόσον δεν είναι απόλυτα απαραίτητο. Αλλά ακόμη και αν είναι απαραίτητο, θα πρέπει να δημοσιεύεται με τις μεθόδους που αναλύουμε στη επόμενη ενότητα και οι οποίες το καθιστούν όπως θα δούμε «κρυφό».
Άλλωστε έχει παρατηρηθεί ότι τα δημοσιευμένα στο internet e-mails λαμβάνουν πολύ μεγαλύτερο ποσοστό spam έναντι των μη δημοσιευμένων.

ii. Ο ιδιώτης χρήστης θα πρέπει να μην απαντά σε μηνύματα spam καθώς μια ενδεχόμενη απάντηση, μπορεί είτε να εκληφθεί ως συναίνεση για την αποστολή ακόμα περισσότερων μη ζητηθέντων μηνυμάτων, αλλά και ώς ένδειξη ότι η προσωπική του email διεύθυνση είναι ενεργή.

iii. Για τους ίδιους λόγους θα πρέπει να αποφεύγεται και η αίτηση για διαγραφή (remove) (καθώς έτσι ενημερώνεται ο spammer ότι ή ηλεκτρονική διεύθυνση είναι ενεργή).

iv. Θα πρέπει να αποφεύγεται η εγγραφή του χρήστη σε λίστες αλληλογραφίας (mailing lists), εφόσον δεν είναι απόλυτα απαραίτητο.

v. Θα πρέπει να χρησιμοποιούνται αντιπροσωπευτικά θέματα (subjects) στα e-mail που στέλνονται. Έτσι, είναι σχετικά απίθανο για κάποιο κανονικό email, να θεωρηθεί ως spam από τους παραλήπτες του, ή από τα anti-spamming φίλτρα.

vi. Κρίνεται απαραίτητη η χρήση λογισμικού για το φιλτράρισμα των e-mails (Anti-Spam software). Αρκετά αξιόλογα λογισμικά που κυκλοφορούν στο εμπόριο, μπορούν να φιλτράρουν επιτυχώς τα spam, χρησιμοποιώντας διάφορες τεχνικές.

2. Προστασία της Email Διεύθυνσης

Για να προστατέψουμε το email μας κατά την δημοσίευση του, στο internet μπορούμε να χρησιμοποιήσουμε κάποια από τις ακόλουθες μεθόδους:

i. **Χρήση εικόνας αντί για κείμενο:** Αν χρησιμοποιήσουμε εικόνα αντί για κείμενο για την προβολή του email μας στο internet, επιτυγχάνουμε να μην είναι δυνατή η καταγραφή του από web robots, web crawlers και web spiders που χρησιμοποιούν οι spammers.

ii. **Αντικατάσταση του χαρακτήρα "@" με "@"**
Αντικαθιστώντας τον χαρακτήρα “@” με “@” που αποτελεί ειδικό χαρακτήρα παράστασης του “@”, καταφέρνουμε να κρύψουμε το email μας, από πολλά προγράμματα των spammers.

iii. **Αντικατάσταση όλων των χαρακτήρων με τις HTML οντότητες (entities).**

iv. **Χρησιμοποιώντας JavaScript.**

- Online εργαλείο για την προστασία της email διεύθυνσης ενός χρήστη «κρύβοντας το» μπορούμε να βρούμε στην ακόλουθη ηλεκτρονική διεύθυνση: http://www.no-spam.gr/mustknow.htm

3. Αναζήτηση του Header του μηνύματος προς αναζήτηση του αποστολέα

Σίγουρα έχει τύχει σε όλους μας να δεχτούμε, είτε κάποιο spam, είτε κάποιο ανώνυμο μήνυμα, που αποτελείται απο ύβρεις – απειλές, ανυπόστατες η μη ζητηθείσες πληροφορίες. Αυτές ακριβώς τις φορές είναι που κρίνεται επιτακτική η ανάγκη, να ανακαλύψουμε από που προέρχεται το συγκεκριμένο email.

Η προφανής και λογική για τον μη ειδικό χρήστη απάντηση, είναι πως μπορούμε να βρούμε την ταυτότητα του spammer «από την γραμμή διεύθυνσης του αποστολέα». Αυτό όμως κάθε άλλο παρά αλήθεια είναι, καθώς σχεδόν πάντα ο κακόβουλος αποστολέας – spammer, φροντίζει ώστε να μην χρησιμοποιεί την πραγματική του διεύθυνση, πόσο μάλλον το πραγματικό του όνομα.

Άρα θα πρέπει να βρούμε κάποιον άλλο τρόπο για να ανακαλύπτουμε τα ίχνη του αποστολέα. Η λύση λοιπόν, παρέχεται από τα Headers του Email μας.

Τα email headers είναι πληροφορίες που περιέχουν λεπτομέρειες σχετικά με τον αποστολέα,την δρομολόγηση και τον παραλήπτη και βρίσκονται μέσα σε κάθε email. Εξετάζοντας τα λοιπόν, μπορούμε να «ακολουθήσουμε» κατα κάποιο τρόπο την διαδρομή πίσω στο host, από το οποίο προήλθε, το συγκεκριμένο ανεπιθύμητο μήνυμα ηλεκτρονικής αλληλογραφίας.

Πώς όμως διαβάζουμε τα email headers ;

Ο τρόπος με τον οποίο μπορεί κάποιος χρήστης να διαβάσει τα email headers, εξαρτάται από το client που χρησιμοποιεί, για να διαβάζει τα email του. Παρακάτω θα παρουσιάσουμε την διαδικασία που πρέπει κάποιος να ακολουθήσει για να διαβάσει τα mail headers.

Εάν χρησιμοποιούμε το Outlook της Microsoft:

- Επιλέγουμε ένα ηλεκτρονικό μήνυμα.
- Κάνουμε δεξί κλικ και επιλέγουμε το πεδίο «Επιλογές» («Options…»).
- Κάνουμε κλικ στο πεδίο «Λεπτομέρειες» («Details»).

- Εν συνεχεία θα ανοίξει ένα μικρό παράθυρο «Επιλογές μηνύματος («Message Options»).

- Στο κάτω μέρος του παραθύρου μπορούμε να δούμε το πεδίο «Επικεφαλίδες» («Internet headers»).

- Ψάχνουμε στο συγκεκριμένο πεδίο για την τελευταία λέξη «Received», σαρώνοντας το κείμενο προς τα κάτω.

Το συγκεκριμένο κείμενο θα είναι κάπως έτσι :

Received: from [12.103.123.21] by web26505.mail.ukl.yahoo.com via HTTP

Εάν χρησιμοποιούμε το Yahoo:

- Ανοίγουμε έναν λογαριασμό Yahoo.
- Επιλέγουμε στο δεξί άνω μέρος της οθόνης το πεδίο «Επιλογές Mail» («Mail Options»).
- Στην συνέχεια επιλέγουμε το πεδίο «Γενικές προτιμήσεις» («General Preferences»).
- Επιλέγουμε το πεδίο «Μηνύματα» («Messages»).
- Επιλέγουμε το πεδίο «Προβολή όλα των headers των εισερχόμενων μηνυμάτων» («Show all headers on incoming messages»).
- Πηγαίνουμε στο τέλος της οθόνης και επιλέγουμε «Αποθήκευση» («Save») στο κάτω αριστερό μέρος της οθόνης.

Χρησιμοποιούμε στην συνέχεια το παρακάτω παράδειγμα για να αναλύσουμε, το τι πληροφορίες μπορούμε να συλλέξουμε απο το header, για τον αποστολέα.

Μήνυμα:

X-Message-Delivery:
Vj0xLjE7dXM9MDtsPTA7YT0xO0Q9MTtTQ0w9MA==
X-Message-Status: n:0
X-SID-PRA: Tedd Baker <spammer@hotmail.com>
X-SID-Result: Pass
X-Message-Info:
JGTYoYF78jGZZ3diV5RgIRSfKLV3rM8GKUbYkios1ubjgVqmMNA9dqnl8h
HavRVwZ5JBGeOoG3OGwK4FP1Sfy1RZzocr4a/t
Received: from bay0-omc2-s9.bay0.hotmail.com ([65.54.246.145]) by col0-
mc4-f16.Col0.hotmail.com with Microsoft SMTPSVC(6.0.3790.3959);
Sun, 19 Apr 2009 13:11:18 -0700
Received: from BAY140-W56 ([64.4.39.91]) by bay0-omc2-
s9.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.3959);
Sun, 19 Apr 2009 13:11:18 -0700
Message-ID: <BAY140-W565CBEDD001F72A65DEE34E4790@phx.gbl>
Return-Path: spammer@hotmail.com

Content-Type: multipart/mixed;
boundary="_49a30aee-aa10-48b7-b232-cbbdccaf278b_"
X-Originating-IP: [94.192.20.96]
From: Tedd Baker <spammer@hotmail.com>
To: <example1@hotmail.com>, <example2@hotmail.co.uk>,
<example3@hotmail.com, <example4@windowslive.com>
Subject: Spam Advertisment
Date: Sun, 19 Apr 2009 20:11:18 +0000
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 19 Apr 2009 20:11:18.0068 (UTC)
FILETIME=[FFC55740:01C9C12A]
X-Mailer: Internet Mail Service (5.5.2650.21)

Σημαντικές Πληροφορίες:

i. Σύμφωνα με το παραπάνω header το συγκεκριμένο email προέρχεται από κάποιον Tedd Baker, με email spammer@hotmail.com. (Οι συγκεκριμένες πληροφορίες μπορεί να είναι παραπλανητικές).

ii. Το header το οποίο περιέχει πληροφορίες σχετικά με την πραγματική προέλευση του μηνύματος, είναι το Received.

iii. Διαβάζοντας λοιπόν το πρώτο Received, αντιλαμβανόμαστε ότι το email προέρχεται από το bay0-omc2-s9.bay0.hotmail.com και έχει IP την 65.54.246.145.

iv. Στην ίδια σειρά το by μας δείχνει τον mail server που προώθησε το μήνυμα και ο οποίο το προώθησε στην διεύθυνση μας. (col0-mc4-f16.Col0.hotmail.com).

v. Το επόμενο Received header αφορά τον απομακρυσμένο email server (BAY140-W56) που δέχτηκε το μήνυμα και έχει IP την 64.4.39.91.

vi. Στην σειρά X-Originating-IP τις περισσότερες φορές μπορούμε να διαβάσουμε την πραγματική IP του αποστολέα. (Στην περίπτωση μας είναι η 94.192.20.96).

vii. Τέλος η σειρά X-Mailer, περιέχει το client που χρησιμοποιήσε ο spammer, για να στείλει το συγκεκριμένο email.

4. Βοηθητικά εργαλεία για την ανάλυση του Header

Πέρα από την ανάλυση του header με τους προαναφερόμενους τρόπους, υπάρχουν μια σειρά από εργαλεία, που μπορούν να φανούν εξαιρετικά χρήσιμα στους «παθόντες» από spam χρήστες του ηλεκτρονικού ταχυδρομείου.

Σημαντικά εργαλεία αποτελούν οι εντολές nslookup και whois, μέσω τον οποίων μπορούμε να επιβεβαιώσουμε από την γραμμή εντολών των windows, ότι κάποια IP αντιστοιχεί σε συγκεκριμένο mail server και το αντίστροφο.

Ένα άλλο εργαλείο είναι η εντολή traceroute, στην οποία χρησιμοποιούμε την IP που βρίσκεται στην σειρά X-Originating-IP του header. Με την εντολή αυτή μπορούμε να ανακαλύψουμε όλους τους ενδιάμεσους κόμβους από τους οποίους περνά ένα μήνυμα για να φτάσει από την συγκεκριμένη IP στον υπολογιστή μας.

Σε πολλές βέβαια περιπτώσεις spam, ο αποστολέας του φροντίζει ώστε να φαίνεται στην συγκεκριμένη γραμμή ένα ψεύτικο IP, άρα η συγκεκριμένη μέθοδος δεν αποτελεί μια εντελώς αξιόπιστη λύση, για την εύρεση της πραγματικής ταυτότητας του spammer.

5. Διαμαρτυρία στον υπεύθυνο του server

Σε ένα επόμενο στάδιο αυτό που πρέπει να κάνει ο παθών από την ανεπιθύμητη ηλεκτρονική αλληλογραφία, είναι να βρει σε ποιόν μπορεί να παραπονεθεί.

Για να το κάνει αυτό θα πρέπει αρχικά να ανατρέξει σε ένα από τα υπάρχοντα μητρώα σε όλο τον κόσμο (επονομαζόμενα ως «Regional Internet Registries» ή απλά RIR) όπου θα ψάξει την προέλευση του συγκεκριμένου μηνύματος.

Συνολικά τα RIR, είναι τα ακόλουθα πέντε (5):

i. Εάν το μήνυμα προέρχεται από την Βόρειο Αμερική, τότε υπεύθυνο μητρώο είναι το ARIN (American Registry of Internet Numbers) (www.arin.net).

ii. Εάν προέρχεται από την Λατινική Αμερική ή την Καραϊβική, τότε υπεύθυνο μητρώο είναι το LACNIC (Latin American and Caribbean Internet Address Registry) (www.lacnic.net).

iii. Εάν προέρχεται από την Ευρώπη, την Μέση Ανατολή ή την Ασία, τότε υπεύθυνο μητρώο είναι το RIPE NCC (www.ripe.net).

iv. Εάν προέρχεται από την Αφρική τότε υπεύθυνο μητρώο είναι το AFRINIC (African Internet Community) (www.afrinic.net).

v. Ενώ τέλος αν προέρχεται από χώρες της Ασίας ή του Ειρηνικού ωκεανού, τότε υπεύθυνο μητρώο είναι το APNIC (Asia Pacific Network Information Centre) (www.apnic.net).

Στην συνέχεια, ανεξάρτητα του σε ποια ιστοσελίδα φτάσει ο χρήστης, θα δει την επιλογή «whois». Μέσω αυτής της επιλογής, αφού ο χρήστης γράψει τον αριθμό που βρήκε στο αντίστοιχο πεδίο , μπορεί να αντιστοιχίσει την IP του spammer, με τον host ο οποίος τον φιλοξενεί.

Από την στιγμή που ο παθών θα έχει στα χέρια του την IP, αλλά και τα στοιχεία του host μέσω του οποίου έδρασε ο spammer το μόνο που απομένει, είναι να επικοινωνήσει με τον διαχειριστή (administrator) του συγκεκριμένου server - host, ενημερώνοντας τον για την παράνομη δράση του πελάτη – μέλους του.

Κατά την συγκεκριμένη επικοινωνία, οι «παθόντες» χρήστες ενθαρρύνονται να επισυνάπτουν και το spam μήνυμα που έλαβαν, στο email διαμαρτυρίας, προς τον διαχειριστή του εν λόγω server - host, ως απόδειξη των ισχυρισμών τους.

6. Ανάρτηση σε forums σχετικά με το SPAM αλλά και σε σχετικές blacklists

Πέρα από την διαμαρτυρία στον υπεύθυνο του server – host από τον οποίο κάποιος spammer, μας απέστειλε ένα μήνυμα ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, άλλη μια πρακτική η οποία προτείνεται στους παθόντες χρήστες, είναι η ανάρτηση του συγκεκριμένου μηνύματος σε forums σχετικά με το spam, αλλά και σε blacklists.

Όπως έχουμε αναλύσει και σε άλλα κεφάλαια, αν ένας χρήστης ενημερώνει τις σχετικές blacklists με κάθε μήνυμα spam που αυτός λαμβάνει, βοηθά χιλιάδες άλλους χρήστες που χρησιμοποιούν τις συγκεκριμένες λίστες, να μην λάβουν ποτέ το συγκεκριμένο μήνυμα.

Καταλαβαίνουμε λοιπόν πως αν αυτή η τακτική γίνει κοινή πρακτική, ο συνολικός «όγκος» του spam θα μειωθεί δραστικά.

Από την άλλη, η ανάρτηση ενός spam mail σε σχετικά με το spam forums, βοηθά με τους ακόλουθους 3 διαφορετικούς τρόπους:

i. Δημοσιεύει την spam δραστηριότητα συγκεκριμένων εταιριών και εντείνει την κοινωνική κατακραυγή εναντίον τους, επιφέροντας τους πλήγμα, σε επίπεδο δημοτικότητας.

   Οδηγεί με αυτόν τον τρόπο, εταιρείες που σκοπεύουν να προβούν σε spam καμπάνιες να το ξανασκεφτούν, οργανώνοντας τις κινήσεις τους στα πλαίσια του permission marketing.

ii. Συντονίζει την νομική δράση – απάντηση χρηστών, που πλήγησαν από το ίδιο spam mail και σκοπεύουν να προβούν σε ομαδική καταγγελία.

iii. Ενημερώνει τους χρήστες για spam διευθύνσεις, τις οποίες μπορούν να μπλοκάρουν “χειροκίνητα” από τα mailboxes τους.

Ελληνικά forums τα οποία φιλοξενούν καταγγελίες για spam μηνύματα και γνωστούς spammers είναι τα ακόλουθα:

i. http://www.freestuff.gr/forums/

ii. http://www.myphone.gr/forum/

iii. http://www.thelab.gr/

iv. http://www.adslgr.com/forum/

Κεφάλαιο 8

Πρωτοβουλίες Anti-Spam και permission marketing

1. Ομάδες εργασίας και πρωτοβουλίες για το πρόβλημα του Spam

Διάφορες ομάδες εργασίας αλλά και πρωτοβουλίες για την καταπολέμηση του spam, εμφανίζονται συνεχώς τόσο σε εθνικό όσο και σε διεθνές επίπεδο.
Οι ομάδες αυτές μπορούν να χωριστούν σε 2 κύριες κατηγορίες. Τις "επίσημες" που αφορούν ομάδες εντεταλμένων οργανισμών για την αντιμετώπιση του spam, αλλά και τις "ανεπίσημες" που αφορούν forums ή άλλες ομάδες χρηστών που κατα κάποιο τρόπο αυτοοργανώνονται και συναντιμετωπίζουν στην συγκεκριμένη μάστιγα.
Σε εθνικό επίπεδο, υπεύθυνη για την καταπολέμηση του spam είναι η «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» (www.dpa.gr), η οποία παρέχει χρήσιμες συμβουλές για το spam, ενημέρωση αλλά και νομική υποστήριξη για τυχόν νομικές διαμάχες.
Σε διεθνές επίπεδο η ομάδα CNSA της Ευρωπαϊκής Επιτροπής συγκροτήθηκε ως δίκτυο επαφής των αρμόδιων αρχών της Ευρώπης για το spam. Η «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» συμμετέχει στην συγκεκριμένη ομάδα ως ο αρμόδιος για το spam φορέας στην Ελλάδα, σύμφωνα με τον Ν. 3471/2006.
Η CNSA, μεταξύ άλλων, υιοθέτησε και το κείμενο συνεργασίας των αρμόδιων Αρχών της Ε.Ε. για την καταπολέμηση του spam. Η συνεργασία αυτή αφορά σε προσφυγές διασυνοριακού χαρακτήρα, δηλαδή αρκεί ο αποστολέας του μηνύματος ηλεκτρονικού ταχυδρομείου να φαίνεται πώς προέρχεται από άλλο κράτος μέλος.

Το πνεύμα του κειμένου συνεργασίας προβλέπει πως η Αρχή που λαμβάνει κάποια καταγγελία αφού διαπιστώσει από την έρευνα που διεξάγει ότι ο αποστολέας κάποιου spam μηνύματος, προέρχεται από άλλο κράτος μέλος, διαβιβάζει την προσφυγή, μαζί με όλα τα έγγραφα του φακέλου, στην Αρχή όπου έχει την κατοικία - έδρα του, ο αποστολέας.
Η ομάδα "London Action Plan" έχει ώς στόχο τη διεθνή συνεργασία μεταξύ των αρμόδιων φορέων, καταπολέμησης του spam. Σε αυτό το πλαίσιο έχει πραγματοποιήσει πληθώρα εκδηλώσεων και έχει εκδώσει τόσο εκθέσεις, όσο και στατιστικά για το spam και την αντιμετώπιση του.
(www.londonactionplan.com/)

Τέλος ο Οργανισμός Οικονομικής Ανάπτυξης και Συνεργασίας (ΟΟΣΑ) έχει συστήσει μια ειδική ομάδα για την καταπολέμηση του spam. Η συγκεκριμένη ομάδα έχει εκδώσει μία έκθεση αντιμετώπισης του προβλήματος, εξετάζοντας πολλές διαφορετικές πτυχές του, όπως την θεσμική, την οικονομική, την τεχνική, την διοικητική, κ.α. (www.oecd-antispam.org/)

2. Permission Marketing

Μέχρι πρόσφατα, η γνωστότερη και πιο διαδεδομένη μορφή επιχειρηματικής αξιοποίησης του email ήταν το spamming.

Καθημερινά, χιλιάδες επιχειρηματίες αποστέλλουν παράνομα διαφημιστικά μηνύματα σε όσο το δυνατόν περισσότερες email διευθύνσεις μπορούν, ελπίζοντας πως με αυτό τον τρόπο θα προσελκύσουν πελατεία.
Η συγκεκριμένη βέβαια πρακτική έχει δυσφημήσει το email, σε τέτοιο βαθμό, που ελάχιστοι πλέον τολμούν να το χρησιμοποιήσουν ως εργαλείο ουσιαστικού marketing.

Από την άλλη το χαμηλό κόστος και η μεγάλη διεισδυτική ικανότητα του το καθιστούν το πλέον δημοφιλές μέσο, απ' όλες τις υπηρεσίες του διαδικτύου. Έτσι, τον τελευταίο καιρό ολοένα και περισσότερες επιχειρήσεις αναγνωρίζουν τη σημασία του και υιοθετούν με αυξανόμενη συχνότητα τη χρήση λιστών opt-in (καταλόγους αποστολής διαφημιστικών-ενημερωτικών μηνυμάτων σε χρήστες του Internet που έχουν δηλώσει πως επιθυμούν την ενημέρωση τους για νέα προϊόντα).

Επίσης στις μέρες μας έχουν αρχίσει να χρησιμοποιούνται και διάφορες άλλες τεχνικές προώθησης πωλήσεων, μέσω ηλεκτρονικού ταχυδρομείου, όπως η αποστολή εκπτωτικών κουπονιών σε παλαιούς πελάτες, οι οποίοι δεν έχουν αγοράσει κάτι για μεγάλο χρονικό διάστημα και οι οποίοι έχουν δώσει την συγκατάθεση τους για την αποστολή των συγκεκριμένων μηνυμάτων.

Βέβαια οι τεχνικές του email marketing βρίσκονται ακόμη στα σπάργανα και ελάχιστοι διαθέτουν σημαντική εμπειρία στην αξιοποίηση του ηλεκτρονικού ταχυδρομείου, ως μέσου διαφημιστικής προβολής.

Άλλωστε, η μέχρι τώρα εμπειρία έχει δείξει πως στο χώρο αυτό τα όρια μεταξύ του αποδεκτού (permission marketing) και του μη αποδεκτού – ανήθικου - παράνομου (spamming) είναι εξαιρετικά δυσδιάκριτα.

Κεφάλαιο 9

Νομοθεσία για την αποστολή SPAM

a. Τρέχον νομικό πλαίσιο για την αποστολή ανεπιθύμητης αλληλογραφίας στην Ελλάδα

Η προστασία από την ανεπιθύμητη αλληλογραφία ρυθμίζεται στην Ελλάδα από ένα νομοθετικό πλαίσιο, το οποίο έχει εμπλουτιστεί από την ενσωμάτωση της ευρωπαϊκής νομοθεσίας.

Ο πρώτος άξονας, στον οποίο βασίζεται αυτό το πλαίσιο είναι η προστασία του καταναλωτή. Ο βασικός νόμος για την προστασία των καταναλωτών είναι ο 2251/1994, ο οποίος περιέχει ορισμούς των εννοιών του καταναλωτή, του προμηθευτή, και της σύμβασης από απόσταση. Αναφορικά με το spam εφαρμόζεται το άρθρο 9 και πιο συγκεκριμένα οι παράγραφοι 10, 11, 12 και 13.

«Άρθρο 9 (Διαφήμιση)

Παράγραφος 10.

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

Παράγραφος 11.

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

Παράγραφος 12.

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

Παράγραφος 13.

«Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή.»

Ο δεύτερος άξονας στον οποίο βασίζεται το ρυθμιστικό πλαίσιο για την ανεπιθύμητη αλληλογραφία είναι η προστασία των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα ισχύει ο νόμος 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Για το spam, εφαρμόζεται το άρθρο 11.

«Άρθρο 11 - Μη ζητηθείσα επικοινωνία

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

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

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

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

5. Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.»

Σύμφωνα με τα παραπάνω, οποιοσδήποτε λαμβάνει ανεπιθύμητη αλληλογραφία, μπορεί να απευθυνθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και να υποβάλλει καταγγελία.

ii. Νομοθεσία στην Ευρωπαϊκή Ένωση

Η Ευρωπαϊκή Ένωση έχει ανταποκριθεί στην ανάγκη αντιμετώπισης του συνεχώς διογκούμενου προβλήματος της ανεπιθύμητης αλληλογραφίας. Το κυριότερο νομοθέτημα είναι η οδηγία ΕΕ 2002/58/ΕΚ, η οποία ρυθμίζει την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Τα κράτη-μέλη οφείλουν να ενσωματώσουν στο εσωτερικό τους δίκαιο, το περιεχόμενο της οδηγίας. Η Ελλάδα, ενσωμάτωσε το κοινοτικό δίκαιο στο νόμο 3471/2006, όπως έχει αναφερθεί και στο προηγούμενο κεφάλαιο.

Περαιτέρω, η Ευρωπαϊκή Επιτροπή, συγκρότησε την ομάδα CNSA, ως δίκτυο επαφής των αρμόδιων αρχών της Ευρώπης για το spam. Ο αρμόδιος φορέας στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Το CNSA, μεταξύ άλλων, υιοθέτησε ένα κείμενο συνεργασίας των αρμόδιων Αρχών της Ε.Ε. για την καταπολέμηση του spam. Η συνεργασία αφορά κυρίως σε προσφυγές διασυνοριακού χαρακτήρα. Επίσης στο κείμενο της συνεργασίας ορίζεται ότι η Αρχή που λαμβάνει την καταγγελία εξετάζει εάν έχει αρμοδιότητα να επιληφθεί της προσφυγής σύμφωνα με το εθνικό δίκαιο και σε περίπτωση που διαπιστωθεί από την έρευνα ότι ο αποστολέας προέρχεται από άλλο κράτος μέλος, διαβιβάζει την προσφυγή μαζί με όλα τα έγγραφα του φακέλου στην Αρχή, όπου έχει την κατοικία - έδρα του ο αποστολέας.

Επίσης σημαντικό ρόλο στην καταπολέμηση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας έχει ο Ευρωπαϊκός Οργανισμός για την ασφάλεια **ENISA**, ο οποίος έχει εκδώσει δύο εκθέσεις για την ασφάλεια καθώς και μέτρα καταπολέμησης του spam που οφείλουν εφαρμόζουν οι Πάροχοι Υπηρεσιών Διαδικτύου στην Ευρώπη.

Τέλος, σημαντική είναι και η συμβολή της ομάδας **London Action Plan**, η οποία στοχεύει στη διεθνή συνεργασία μεταξύ των αρμόδιων φορέων καταπολέμησης του spam και άλλων συναφών προβλημάτων όπως η διαδικτυακή απάτη, το phising, οι ιοί. Σε αυτό το πλαίσιο έχει πραγματοποιήσει πολλές σχετικές εκδηλώσεις και έχει εκδώσει εκθέσεις και στατιστικά για το spam και την αντιμετώπιση του.

iii. Νομοθεσία στις ΗΠΑ

Οι ΗΠΑ είναι η χώρα όπου γεννήθηκε το διαδίκτυο ενώ ακόμα και σήμερα έχει τους περισσότερους κατ' αναλογία συνολικού πληθυσμού χρήστες. Επιπλέον εκεί έχει την έδρα της η πλειονότητα των εταιρειών που δραστηριοποιείται στον ευρύτερο τομέα των νέων τεχνολογιών. Συνεπώς το ζήτημα του spam έχει απασχολήσει - από τα αρχικά στάδια της ανάπτυξης του - τις αρχές.

Η ανάγκη άμεσης αντιμετώπισης και μείωσης του spam οδήγησε στην ψήφιση το 2003 του ομοσπονδιακού νόμου **CAN-SPAM Act** (15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th United States Congress).

Το **CAN-SPAM Act** υπογράφθηκε από τον Πρόεδρο George W. Bush 16 Δεκεμβρίου 2003, και εγκαθίδρυσε τις πρώτες εθνικές αρχές σχετικά με την αποστολή εμπορικών ηλεκτρονικών μηνυμάτων ενώ παράλληλα κατέστησε την Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) αρμόδια για την εφαρμογή τους. Το ακρωνύμιο **CAN-SPAM** προέρχεται από το πλήρες όνομα του νόμου: ***C*ontrolling the *A*ssault of *N*on-*S*olicited *P*ornography *A*nd *M*arketing Act of 2003**, το οποίο σημαίνει Νομοσχέδιο για τον έλεγχο της άνευ προηγούμενης συγκατάθεσης αποστολής ηλεκτρονικών αποστολών πορνογραφικού και εμπορικού περιεχομένου.

Το νομοσχέδιο κατέθεσαν στο κογκρέσο οι γερουσιαστές Conrad Burns και Ron Wyden. Ο νομός απαιτούσε επίσης, η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) να αναφέρει στο Κογκρέσο εντός 24 μηνών εάν τα μέτρα ήταν αποτελεσματικά. Πράγματι, το Δεκέμβριο του 2005 η Επιτροπή ανέφερε στο Κογκρέσο ότι ο όγκος του spam μειώθηκε.

Παρόλα αυτά το συγκεκριμένο νομοσχέδιο έχει δεχθεί έντονες κριτικές, αναφέρεται δε από πολλούς ως YOU-CAN-SPAM, δηλαδή μπορείς να κάνεις spam, διότι δεν απαιτεί οι αποστολείς να έχουν πάρει άδεια πριν στείλουν διαφημιστικά μηνύματα ταχυδρομείου.

Επίσης απαγορεύει στις Πολιτείες να ψηφίσουν αυστηρότερους πολιτειακούς νόμους από τον CAN-SPAM για την καταπολέμηση του spam. Τέλος απαγορεύει την άσκηση μηνύσεων από ιδιώτες που λαμβάνουν spam κατά των αποστολέων. Το μεγαλύτερο όμως πρόβλημα που προκύπτει είναι ότι το νομοσχέδιο έμεινε σχεδόν ανεφάρμοστο αφού μόνο το 1% των spammers συμμορφώθηκε με τις διατάξεις.

Το CAN-SPAM προβλέπει, ότι επιτρέπεται η μαζική αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων αρκεί να τηρούνται τρεις προϋποθέσεις.

i. Να υπάρχει πάνω στο ηλεκτρονικό μήνυμα ένας μηχανισμός που να επιτρέπει στον αποδεκτή να αφαιρέσει την ηλεκτρονική του διεύθυνση από την λίστα. Ο αποδέκτης έχει στη διάθεση του 10 μέρες για να δηλώσει ότι δεν επιθυμεί να λαμβάνει διαφημιστικά μηνύματα από τον αποστολέα. Οι λίστες με τα ονόματα αυτών που δήλωσαν ότι δεν επιθυμούν να λαμβάνουν μηνύματα μπορούν να χρησιμοποιηθούν μόνο για τη συμμόρφωση των παραβατών.

ii. Να υπάρχει επάνω στο ηλεκτρονικό μήνυμα η έγκυρη διεύθυνση του αποστολέα και του διαφημιστή. Σε περίπτωση που το περιεχόμενο του μηνύματος είναι ακατάλληλο για ανηλίκους να υπάρχει η αρμόζουσα ετικέτα.

iii. Το μήνυμα δεν πρέπει να σταλεί από open relay, δεν μπορεί να σταλεί σε ηλεκτρονική διεύθυνση που έχει αγοραστεί η υποκλαπεί και τέλος το μήνυμα δεν μπορεί να περιέχει ένα false header (Δηλαδή ψευδείς πληροφορίες για τον αποστολέα, τον παραλήπτη και την διαδρομή που ακολούθησε το email).

Συνεπώς όπως διαφαίνεται από τα παραπάνω, το CAN-SPAM δικαίως έχει δεχθεί κριτικές διότι δεν απαγορεύει ρητά το spam. Αντιθέτως απαριθμεί τις προϋποθέσεις κάτω από τις οποίες αυτό είναι παράνομο, αφήνοντας περιθώρια για την αποστολή «νόμιμου» spam το οποίο όμως συνεχίζει να είναι χρονοβόρο και πολυέξοδο για τους αποδέκτες του.

Κεφάλαιο 10

Λήψη μέτρων κατά του SPAM στο Α.Τ.Ε.Ι. Πάτρας

1. Ενημέρωση των φοιτητών του Α.Τ.Ε.Ι. Πατρών για τις επιπτώσεις αλλά και τους τρόπους προστασίας από το spam

Πρώτα απ' όλα θεωρούμε πως προτεραιότητα για την αντιμετώπιση του spam στο Α.Τ.Ε.Ι. Πατρών είναι να έχουν οι σπουδαστές του πλήρη ενημέρωση σχετικά με τους τρόπους αλλά και τις μεθόδους με τις οποίες θα κατορθώσουν, να το αποφύγουν.

Για αυτό τον λόγο λοιπόν καταλήξαμε και προτείνουμε μια σειρά από κοινές πρακτικές που θα βοηθήσουν τους συνσπουδαστές μας να κατανοήσουν αλλά και να αντιμετωπίσουν καλύτερα την συγκεκριμένη "απειλή". Οι συγκεκριμένες πρακτικές, απαριθμούνται στην ακόλουθη λίστα.

Κοινές πρακτικές αποφυγής του SPAM:

1. Να αποφεύγεται η δημοσίευση του πρωτεύοντος e-mail προσωπικής αλληλογραφίας, σε δημόσιους ιστότοπους.
2. Να χρησιμοποιούνται περισσότερες της μιας ηλεκτρονικές διευθύνσεις (e-mails), ώστε να μπορεί ο κάθε φοιτητής να έχει μια ηλεκτρονική διεύθυνση «αφιερωμένη» στην προσωπική του αλληλογραφία την οποία και δεν θα κοινοποιεί, ενώ τις υπόλοιπες διευθύνσεις θα μπορεί να τις χρησιμοποιεί για εγγραφές σε ομάδες και χώρους συζητήσεων (forums - chat rooms), εγγραφές σε λίστες αλληλογραφίας κ.α..
3. Να χρησιμοποιείται ως ηλεκτρονική διεύθυνση ένας συνδυασμός από το όνομα και το επίθετο σας αντί για απλά ονόματα. Είναι γνωστό άλλωστε ότι οι spammers χρησιμοποιούν συνδυασμούς ονομάτων, λέξεων και αριθμών για να δημιουργήσουν πιθανές διευθύνσεις.
4. Να αντιμετωπίζεται τα «κοινόχρηστα» e-mail σας (δηλαδή τα e-mail που χρησιμοποιείτε για τις εγγραφές, στις διάφορες υπηρεσίες), ως προσωρινά, καθώς η πιθανότητα να γίνουν γνωστά στους spammers είναι μεγάλη. Η συχνή αλλαγή τους λοιπόν είναι μια παρά πολύ καλή τακτική.

5. Όταν είναι απαραίτητο να κοινοποιήσετε το προσωπικό σας e-mail, σε κάποιον ιστότοπο, τότε θα πρέπει να το "καμουφλάρετε". Για παράδειγμα το nicolaou@spamming.gr, είναι εύκολο να βρεθεί από τις ειδικές μηχανές αναζήτησης e-mails. Μπορεί λοιπόν να γραφτεί ώς nicolaou-at-spamming-dot-gr, γραφή που το καθιστά "αόρατο" στους αποστολείς spam. Επίσης ένας άλλος τρόπος καμουφλαρίσματος, είναι να

δημοσιεύετε το email σας ως αρχείο γραφικών (εικόνα) και όχι ως σύνδεσμο (link).

6. Να αποφεύγεται ομάδες και χώρους συζητήσεων, οι οποίες σας έχουν δώσει την αφορμή ότι μπορεί να πωλούν διευθύνσεις σε spammers. (Αφορμή θεωρείται το να αρχίσετε να λαμβάνετε spam αμέσως μετά την εγγραφή σε κάποια ομάδα).
7. Να αποφεύγετε την οποιαδήποτε απάντηση σε μηνύματα spam, η καλύτερη λύση είναι το "μπλοκάρισμα" (επισύμανση του μηνύματος). Οι περισσότεροι spammers, χρησιμοποιούν την απάντηση σας για να επαληθεύουν την ύπαρξη της συγκεκριμένης e-mail διεύθυνσης. Για το ίδιο ακριβώς λόγο, προτείνεται να μην επισκέπτεστε συνδέσμους, με σκοπό την διαγραφή σας (unsubscribe) από μία λίστα, όταν η πηγή του μηνύματος είναι ύποπτη. Τέτοια μηνύματα αποστέλλονται από τους spammers με σκοπό να συλλέξουν ενεργές διευθύνσεις, στις οποίες μετέπειτα αυξάνεται ο αριθμός των ανεπιθύμητων e-mail που λαμβάνουν.
8. Προτείνεται ανεπιφύλακτα η εγκατάσταση ειδικού anti-spam λογισμικού στον υπολογιστή σας, καθώς και ειδικού φίλτρου στο πρόγραμμα ηλεκτρονικής αλληλογραφίας σας.

Απόκρυψη του E-MAIL από τους spammers

Θεωρούμε επίσης αρκετά σημαντικό για να το αναφέρουμε το εργαλείο το οποίο έχει αναπτύξει το Τ.Ε.Ι. Μεσολογγίου, για την απόκρυψη με μια σειρά «τεχνασμάτων» της ηλεκτρονικής διεύθυνσης των σπουδαστών του από τους spammers.

Το συγκεκριμένο εργαλείο βρίσκεται στην διεύθυνση: http://noc.teimes.gr/noc/wp-content/uploads/hide_mail_in-web.htm και βοηθά στην απόκρυψη της ηλεκτρονικής μας διεύθυνσης με 3 τρόπους:

i. Αντικατάσταση του χαρακτήρα "@" με "@"
ii. Αντικατάσταση όλων των χαρακτήρων με τις HTML οντότητες (entities)
iii. Χρησιμοποιώντας JavaScript

Ακολουθεί screenshot της συγκεκριμένης εφαρμογής:

2. Παρουσίαση προτεινόμενης μεθοδολογίας και εργαλείων αντιμετώπισης του spam για την περίπτωση του Α.Τ.Ε.Ι. Πατρών

Όταν έχουμε να κάνουμε με κεντρικούς εξυπηρετητές τότε το να ελέγχουμε το περιεχόμενο του κάθε μηνύματος ξεχωριστά απαιτεί σημαντική υπολογιστική ισχύ καθώς μπορεί να διακινούνται δεκάδες μηνύματα το δευτερόλεπτο. Αντ' αυτού ο εξυπηρετητής μπορεί να ελέγξει αν η ηλεκτρονική διεύθυνση IP του εξυπηρετητή που στέλνει το μήνυμα είναι καταγεγραμμένη, σε κάποια από τις μαύρες λίστες γνωστών πηγών spam στο Internet.

Αν λοιπόν ο υπό εξέταση εξυπηρετητής-αποστολέας είναι καταγεγραμμένος στις συγκεκριμένες λίστες, τότε το μήνυμα του απορρίπτεται προτού μεταφερθεί. Οι λίστες αυτές ονομάζονται DNS black lists (DNSBLs), καθώς όλες οι ερωταπαντήσεις γίνονται με βάση το πρωτόκολλο DNS. Η συγκεκριμένη μεθοδολογία μπορεί να μην είναι τόσο αποτελεσματική όσο η ένα προς ένα εξέταση των μηνυμάτων, παρουσιάζει όμως το σημαντικό πλεονέκτημα ότι τα μηνύματα spam δεν φεύγουν ποτέ από την πηγή – αποστολέα τους και δεν επιβαρύνουν ούτε το δίκτυο, αλλά ούτε και τους τελικούς χρήστες.

Το ΚΕΔ (Κέντρο Δικτύων) του Ε.Μ.Π. καθώς και το Κέντρο Διαχείρισης Δικτύου του Α.Τ.Ε.Ι. Μεσολογγίου, χρησιμοποιούν DNSBLs. Οι κεντρικοί εξυπηρετητές ηλεκτρονικής αλληλογραφίας από τους οποίους περνά κάθε μήνυμα με παραλήπτη κάποιο χρήστη εντός των εκπαιδευτικών ιδρυμάτων, ελέγχουν αν ο απομακρυσμένος εξυπηρετητής είναι καταγεγραμμένος στις λίστες DNSBL, προτού το αποδεχθούν. Με το τρόπο αυτό μειώνεται σημαντικά η ποσότητα ανεπιθύμητης αλληλογραφίας SPAM που καταλήγει στους τελικούς χρήστες.

Στην περίπτωση απόρριψης ο απομακρυσμένος εξυπηρετητής λαμβάνει ένα μήνυμα λάθους της μορφής:

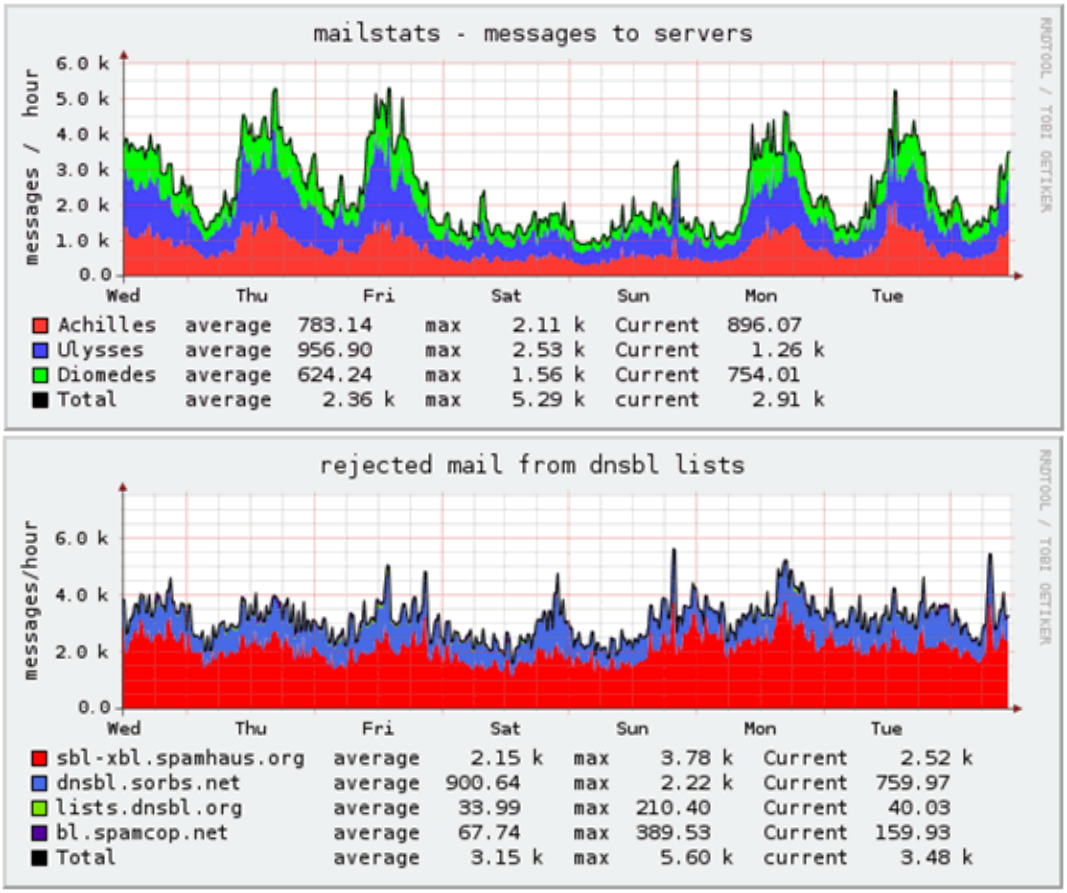
550 5.7.1 Rejected: 90.129.14.46 listed at sbl-xbl.spamhaus.org

Στην παραπάνω περίπτωση ο υπολογιστής με IP διεύθυνση 90.129.14.46 δοκίμασε να συνδεθεί σε έναν από τους κεντρικούς εξυπηρετητές του ιδρύματος και η σύνδεσή του απορρίφθηκε γιατί βρέθηκε καταχωρημένος στη λίστα sbl-xbl.spamhaus.org.

Συγκεκριμένα οι DNSBLs που χρησιμοποιούνται από τους κεντρικούς εξυπηρετητές των συγκεκριμένων ιδρυμάτων είναι οι:

i. sbl-xbl.spamhaus.org
ii. list.dsbl.org
iii. dnsbl.sorbs.net
iv. bl.spamcop.net.

Όπως φαίνεται και στα διαγράμματα, περίπου ένα στα δυο μηνύματα απορρίπτεται ως ανεπιθύμητο (spam):



[Τα συγκεκριμένα σχήματα προέρχονται από το ΚΕΔ του Ε.Μ.Π. **(noc.ntua.gr)**]

Από την άλλη ιδρύματα όπως το Πανεπιστήμιο Πατρών, το Πανεπιστήμιο Αιγαίου, το Πανεπιστήμιο Θεσσαλίας και το Γεωπονικό Πανεπιστήμιο Αθηνών, χρησιμοποιούν το λογισμικό ανοικτού κώδικα spamassassin, το οποίο χρησιμοποιεί μια σειρά από κανόνες ελέγχου για να υπολογίσει τη στατιστική πιθανότητα του κάθε μηνύματος να είναι "γενικά" ανεπιθύμητο, συλλέγοντας βαθμολογία από κάθε κανόνα.

Στη περίπτωση που η συνολική βαθμολογία ενός μηνύματος ξεπεράσει το πέντε (5), τότε το spamassassin εισαγάγει αυτόματα στο θέμα (subject) του μηνύματος το πρόθεμα ***** **SPAM***** .

Οι χρήστες – φοιτητές των συγκεκριμένων ιδρυμάτων μπορούν εφόσον το επιθυμούν να ρυθμίσουν το πρόγραμμα που χρησιμοποιούν για ηλεκτρονικό ταχυδρομείο (Outlook Express, Outlook, Mozilla thunderbird, Netscape mail, Eudora) ώστε να αφαιρεί τα μηνύματα αυτά και να τα βάζει σε ειδικό φάκελο για περαιτέρω έλεγχο ή ακόμη και να τα σβήνει. Όλα τα ιδρύματα παρέχουν επίσης πλήρεις οδηγίες για κάθε πρόγραμμα ηλεκτρονικού ταχυδρομείου

Πρόταση για το Α.Τ.Ε.Ι. Πάτρας

Λαμβάνοντας υπόψιν όλα τα παραπάνω καταλήγουμε στο συμπέρασμα, ότι η πιο επικερδής για την καταπολέμηση του spam μεθοδολογία θα ήταν η ταυτόχρονη χρήση DNSBLs και του spamassassin, ώστε οποιοδήποτε μήνυμα προέρχεται από άγνωστο spammer και καταφέρνει να ξεφύγει από τις black lists να ελέγχεται και από τους κανόνες του συγκεκριμένου προγράμματος αντιμετώπισης της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας.

Συμπεράσματα

Στην συγκεκριμένη εργασία αφού ασχοληθήκαμε με τις βασικές έννοιες του spam και του ηλεκτρονικού ταχυδρομείου, καταθέσαμε τον προβληματισμό που επικρατεί, σχετικά με το κόστος που προκαλεί το spam, σε ιδιώτες, επιχειρήσεις και ISPs.

Στην συνέχεια αναφερθήκαμε στα τεχνικά μέτρα τα οποία μπορούμε να λάβουμε για να περιορίσουμε το συγκεκριμένο φαινόμενο, καθώς και στο λογισμικό το οποίο μπορεί να σταθεί πολύτιμος σύντροφος δίπλα μας, στον αγώνα κατά του spam.

Στην συνέχεια εκθέσαμε μια σειρά από συστάσεις συμπεριφοράς τόσο για την αποφυγή, όσο και για άμυνα απέναντι στην ανεπιθύμητη αλληλογραφία.

Ακολούθως αναφερθήκαμε στις διάφορες Anti-Spam πρωτοβουλίες καθώς και στην έννοια αλλά και την σημασία του Permission Marketing. Στο 9^{ο} κεφάλαιο παρουσιάσαμε την νομοθεσία που διέπει την αποστολή spam μηνυμάτων, σε Ελλάδα, Ευρώπη και Αμερική, ενώ στο 10^{ο} κεφάλαιο απαριθμήσαμε μια σειρά από μέτρα που θα μπορούσε να λάβει το Α.Τ.Ε.Ι. Πατρών για την αντιμετώπιση αλλά και την πρόληψη της ανεπιθύμητης αλληλογραφίας.

Φτάνοντας στο τέλος της παρούσας εργασίας και αντιλαμβανόμενοι την σπουδαιότητα του θέματος αλλά και τις διαστάσεις που έχει λάβει το φαινόμενο του spam στις μέρες μας, αποφασίσαμε μετά το πέρας των βιβλιογραφικών αναφορών, να προσθέσουμε μια σειρά από χρήσιμα παραρτήματα.

Στο 1^{ο} (Α) παράρτημα προτείνουμε συγκεκριμένη πολιτική anti-spam για το Α.Τ.Ε.Ι. Πατρών προς ενημέρωση και συμμόρφωση των φοιτητών αλλά και των υπολοίπων μελών του.

Στο 2^{ο} (Β) παράρτημα καταθέτουμε μια σειρά από χαρακτηριστικές περιπτώσεις spam, ώστε να εξοικειωθεί ο αναγνώστης με τα διάφορα είδη.

Στο 3^{ο} (Γ) παράρτημα παραθέτουμε μια σειρά από πρόσφατα και ενδιαφέροντα στατιστικά στοιχεία για την «κίνηση» του spam, ενός τέλος στο 4^{ο} (Δ) παράρτημα, δίνουμε πληροφορίες σχετικά με τον διαδικτυακό οδηγό παρουσίασης της εργασίας μας, που ελπίζουμε να αποτελέσει άλλη μία anti-spam νησίδα στον απέραντο και απειλητικό ωκεανό του internet.

Πάτρα, Οκτώβριος 2009,

Γεωργία Νικολάου, Μαρίνος Ρουσελάτος

Βιβλιογραφία

“ No finite point has meaning without an infinite reference point “
~ Jean Paul Sartre

Βιβλιογραφία

i. McWilliams B. (2004), S*pam Kings: The Real Story Behind the High-Rolling Hucksters PUSHING PORN, PiLLS, and @*#?% Enlargements, 1st Edition. ISBN: 0-596-00732-9

ii. Spammer-X, Jeffrey Posluns (Editor), Stu Sjouwerman (Foreword) Inside the SPAM Cartel Syngress, 1 edition (November 1, 2004). ISBN: 1932266860

iii. Ken Feinstein, How to Do Everything to Fight Spam, Viruses, Pop-Ups, and Spyware (How to Do Everything), McGraw-Hill Osborne Media, 1 edition (July 30, 2004). ISBN: 0072256559

iv. Alan Schwartz, SpamAssassin, O'Reilly, 1 edition (July 2004). ISBN: 0596007078

v. Jonathan Land, The Spam Letters, No Starch Press, 1 edition (June 2004). ISBN: 1593270321

vi. Jeremy Poteet, Canning Spam: You've Got Mail (That You Don't Want), Sams; (May 13, 2004), ISBN: 0672326396

vii. Paul Wolfe, Charlie Scott, Mike Erwin, Anti-Spam Tool Kit Osborne/McGraw-Hill; (March 17, 2004), ISBN: 007223167X

viii. John R. Levine, Margaret Levine Young, Ray Everett-Church Fighting Spam for Dummies, For Dummies; (January 19, 2004) ISBN: 0764559656

ix. Shannon Kinnard, Marketing With Email: A Spam-Free Guide to Increasing Awareness, Building Loyalty, and Increasing Sales by Using the Internet's Most Powerful Tool Independent Pub Group; First edition (October 1, 1999), ASIN: 1885068409

x. Schwartz, A. & Garfinkel, S. (1998), Stopping Spam: Stamping Out Unwanted Email and News Postings, 1st Edition. O' Reilly. ISBN: 1-56592-388-X

xi. John Cho, Spam-Ku : Tranquil Reflections on Luncheon Loaf Perennial; 1st edition (October 1, 1998), ASIN: 0060952784

xii. Timothy D. Casey, ISP Liability Survival Guide: Strategies for Managing Copyright, Spam, Cache, and Privacy Regulations Wiley; 1 edition (May 8, 2000), ISBN: 0471377481

xiii. "Δίκτυα Υπολογιστών" – Andrew S. Tanenbaum

xiv. Οδηγός «Διαδικτύου» Πανεπιστημίου Μακεδονίας

xv. Το λεξικό του Internet - Οικονομικό Πανεπιστήμιο Αθηνών Τεχνολογικό Παρατήρητηριο - www.technowatch.aueb.gr

xvi. "As We May Think" – Vannevar Bush

xvii. "Αυτονομία και Κυβερνητική Ανυπακοή στον Κυβερνοχώρο" Γκρίτζαλης

xviii. "State of SPAM – A Monthly Report" October 2009, Report #34, Symantec

Παράρτημα Α

Πολιτική Anti-Spam Α.Τ.Ε.Ι. Πατρών

Προτεινόμενη πολιτική αντιμετώπισης spam του Α.Τ.Ε.Ι. Πάτρας

Θα πρέπει να καθίσταται σαφές στους σπουδαστές πώς το Spam, αποτελεί μη αποδεκτή χρήση του δικτύου του Α.Τ.Ε.Ι. Πάτρας. Ως spam ορίζεται οποιοσδήποτε τύπος ανεπιθύμητου εμπορικού e-mail.

Αναλυτικότερα απαγορεύονται οι ακόλουθες ενέργειες:

1. Η αποστολή ανεπιθύμητων μηνυμάτων ή άλλου διαφημιστικού περιεχομένου e-mail σε χρήστες οι οποίοι δεν έχουν αποδεχτεί τη λήψη τέτοιου είδους μηνυμάτων ηλεκτρονικού ταχυδρομείου.
2. Η αποστολή ανεπιθύμητων e-mail τα οποία δεν συμπεριλαμβάνουν τη δυνατότητα αυτόματης διαγραφής από τη συγκεκριμένη λίστα.
3. Η διανομή, διαφήμιση ή προώθηση λογισμικού ή υπηρεσίας που έχει ως αρχικό σκοπό την προτροπή ανεπιθύμητης χρήσης εμπορικού ηλεκτρονικού ταχυδρομείου ή spam.
4. Η παραποίηση των headers, δηλαδή των επικεφαλίδων που προσδιορίζουν / αναγνωρίζουν τον αποστολέα και το δίκτυο προέλευσης του μηνύματος.
5. Η δημιουργία ή προώθηση ηλεκτρονικού ταχυδρομείου με αιτήματα για φιλανθρωπίες, αιτήσεις για υπογραφές, ή οτιδήποτε έχει σχέση με chain mail (αλυσιδωτή αποστολή mail).
6. Η αποστολή πολυάριθμων μηνυμάτων στον ίδιο χρήστη (mail bombing).
7. Η χρήση προγραμμάτων (script) με σκοπό την αποστολή bulk (ογκώδη) ή ανεπιθύμητων μηνυμάτων (unsolicited mails).
8. Η διατήρηση open relay mail server.
9. Η αποστολή ιών Διαδικτύου, worms, trojan, καθώς επίσης και η διανομή πληροφοριών σχετικών με τη δημιουργία και την αποστολή αυτών.
10. Η εγγραφή οποιουδήποτε χρήστη σε mailing list χωρίς την άδειά του.

Παράρτημα Β

Χαρακτηριστικές Περιπτώσεις SPAM

1. SPAM από το ΤΕΙ Κρήτης

Αγαπητέ υποψήφιε,

στο πλαίσιο του ολοένα αυξανόμενου ανταγωνισμού που χαρακτηρίζει το σύνολο της επιχειρηματικής δραστηριότητας ανά τον κόσμο, το μάρκετινγκ αναδεικνύεται ως το πλέον ισχυρό εργαλείο για τη δημιουργία ανταγωνιστικού πλεονεκτήματος και την αποτελεσματική προώθηση προϊόντων ή/και υπηρεσιών. Η διαπίστωση αυτή αποτέλεσε και την αιτία για την ίδρυση του τμήματος Εμπορίας και Διαφήμισης του Τ.Ε.Ι. Κρήτης το 2003 στην Ιεράπετρα. Η αποστολή του τμήματος αφορά στην εκπαίδευση των φοιτητών σε όλο το φάσμα των λειτουργιών μάρκετινγκ (διαφήμιση, δημόσιες σχέσεις, B2B μάρκετινγκ, μάρκετινγκ λιανικού εμπορίου, κ.ά.), ενώ μέσω των αντιστοίχων κατευθύνσεων οι φοιτητές μπορούν να εξειδικευτούν στο ηλεκτρονικό εμπόριο, καθώς και στο τουριστικό και αγροτικό μάρκετινγκ.

……
……
……..

Η διαφοροποίηση του Τμήματός μας λοιπόν εδράζει στη φιλοσοφία οργάνωσης και λειτουργίας του, με επίκεντρο τον φοιτητή όσον αφορά στην παρεχόμενη εκπαίδευση και στη δημιουργία και διάχυση σύγχρονης γνώσης μέσω των ερευνητικών του δραστηριοτήτων, τη διοργάνωση πληθώρας σεμιναρίων, ημερίδων και διαλέξεων από επισκέπτες επιστήμονες και διακεκριμένους επιχειρηματίες, στα πλαίσια των σύγχρονων υποδομών του. Η φιλοσοφία αυτή είναι που καταξίωσε το τμήμα μας ως ένα από τα καλύτερα τμήματα μάρκετινγκ στην Ελλάδα, αναγνωρισμένο τόσο στην αγορά εργασίας, όσο και από τους υποψήφιους φοιτητές .

Με εκτίμηση,

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Δρ. Ιωάννης Κοπανάκης

Επίκουρος Καθηγητής

Προϊστάμενος, Τμήμα Εμπορίας & Διαφήμισης

Κ. Παλαμά & Ι. Κακριδή, Ιεράπετρα, 72200, Κρήτη
28420 89480-1 28420 89797
www.emark.teicrete.gr

Αυτό το e-mail δεν μπορεί να θεωρηθεί spam εφόσον αναγράφονται τα στοιχεία του

αποστολέα και διαδικασίες διαγραφής από την λίστα παραληπτών. Αν είστε σε αυτή τη λίστα κατά λάθος ή για οποιονδήποτε άλλο λόγο θέλετε να διαγραφεί το e-mail σας από αυτή τη λίστα παραληπτών e-mail απλά απαντήστε σε αυτό το e-mail με θέμα "UNSUBSCRIBE" στην ηλεκτρονική διεύθυνση info@emark.teicrete.gr Αυτό το μήνυμα πληροί τις προυποθέσεις της Ευρωπαικής νομοθεσίας περί διαφημιστικών μηνυμάτων. Κάθε μήνυμα θα πρέπει να φέρει τα πλήρη στοιχεία του αποστολέα ευκρινώς και θα πρέπει να δίνει στον δέκτη τη δυνατότητα διαγραφής. (Directiva 2002/31/CE του Ευρωπαικού Κοινοβουλίου Relative as A5-270/2001 του Ευρωπαικού Κοινοβουλίου).

Επειδή κάθε ηλεκτρονικό μήνυμα που αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση του παραλήπτη, είναι παράνομο (σύστημα γνωστό ώς «opt-in»), το συγκεκριμένο μήνυμα του Τ.Ε.Ι. Κρήτης, θα μπορούσε κάλλιστα να χαρακτηριστεί ώς spam, καθώς έφτασε σε χιλιάδες ηλεκτρονικές διευθύνσεις.

2. SPAM διαφήμιση για email marketing

1ο mail

ΟΙ ΚΑΙΡΟΙ ΕΙΝΑΙ ΔΥΣΚΟΛΟΙ

ΠΡΟΣΦΕΡΟΥΜΕ ΟΙΚΟΝΟΜΙΚΟ ΠΑΚΕΤΟ ΑΠΟΣΤΟΛΗΣ 40.000 E-MAILS ΓΙΑ ΝΑ ΕΞΑΣΦΑΛΙΣΕΤΕ ΑΠΡΟΣΜΕΝΕΣ ΧΡΙΣΤΟΥΓΕΝΝΙΑΤΙΚΕΣ ΠΩΛΗΣΕΙΣ ΜΕ ΑΣΗΜΑΝΤΗ ΔΑΠΑΝΗ 200 ΕΥΡΩ

Εμείς μπορούμε να στείλουμε 40.000 e-mails σε επιχειρήσεις – τράπεζες – οργανισμούς – δήμους – κοινότητες – γιατρούς – μηχανικούς – αρχιτέκτονες – δικηγόρους κλπ. Ετοιμάστε το οικονομικό πακέτο προϊόντων – υπηρεσιών και από 5/11 θα ξεκινήσουμε να το στέλνουμε μαζί, αν θέλετε, με το site σας σε προέδρους – δ/νοντες συμβούλους – επιχειρηματίες με βεβαιότητα ότι καθημερινά θα έχετε τηλεφωνήματα από διάφορα μέρη της Ελλάδας, Κύπρου, ακόμη και Ρωσίας!!! Δοκιμάστε το θα πετύχει 100%. Στείλτε e-mail infosarr@gmail.com <mailto:infosarr@gmail.com> – κιν. 6997 764122.

2ο mail

ΚΥΡΙΕΣ - ΚΥΡΙΟΙ, ΣΑΣ ΓΝΩΡΙΖΟΥΜΕ ΟΤΙ ΜΠΟΡΟΥΜΕ ΝΑ ΣΤΕΙΛΟΥΜΕ ΕΝΕΡΓΟ ΚΑΙ ΤΟ ΔΙΚΟ ΣΑΣ SITE με e-mail ΣΕ 60.000 ΕΠΙΧΕΙΡΗΣΕΙΣ – ΞΕΝΟΔΟΧΕΙΑ – ΤΡΑΠΕΖΕΣ – ΟΡΓΑΝΙΣΜΟΥΣ–ΓΙΑΤΡΟΥΣ ΜΗΧΑΝΙΚΟΥΣ- ΔΙΚΗΓΟΡΟΥΣ – ΑΡΧΙΤΕΚΤΟΝΕΣ κλπ. ΕΙΝΑΙ ΒΕΒΑΙΟ ΟΤΙ ΘΑ ΕΧΕΤΕ ΕΞΑΙΡΕΤΙΚΗ ΚΑΘΗΜΕΡΙΝΗ ΑΝΤΑΠΟΚΡΙΣΗ ΑΠΟ ΚΑΘΕ ΠΟΛΗ ΚΑΙ ΝΗΣΙ ΤΗΣ ΕΛΛΑΔΑΣ ΚΑΙ ΑΠΟ 1/1/09, ΑΝ ΣΑΣ ΕΝΔΙΑΦΕΡΕΙ, ΑΠΟ ΚΥΠΡΟ – ΒΑΛΚΑΝΙΚΕΣ ΧΩΡΕΣ. Επικοινωνήστε με κο Σαρρή κιν. 6997 764122 – boxsarr@gmail.com == ΔΕΙΤΕ ΤΟ SITE ΠΟΥ ΞΕΚΙΝΗΣΑΜΕ ΑΠΟΣΤΟΛΕΣ ΠΡΟΣΦΑΤΑ

3. SPAM απάτη (ευαισθητοποίησης για πρόβλημα υγείας)

ΕΙΜΑΣΤΕ Ο ΝΙΚΟΣ ΚΑΙ Η ΑΓΓΕΛΙΚΗ ΠΑΠΑΔΑΚΗ ΚΑΙ ΖΟΥΜΕ ΣΤΑ ΑΝΩ ΛΙΟΣΙΑ. ΕΧΟΥΜΕ 2 ΠΑΙΔΙΑ- ΤΗΝ ΕΛΕΝΗ Η ΟΠΟΙΑ ΕΙΝΑΙ 11 ΕΤΩΝ ΚΑΙ ΤΗ ΜΑΙΡΗ Η ΟΠΟΙΑ ΕΙΝΑΙ 2. Η ΜΑΙΡΗ ΓΕΝΝΗΘΗΚΕ Ε ΚΑΡΔΙΑΚΗ ΑΝΕΠΑΡΚΕΙΑ ΑΛΛΑ ΑΠΟ ΤΗ ΓΕΝΝΗΣΗ ΤΗΣ ΜΕΧΡΙ ΤΩΡΑ ΔΕΝ ΥΠΗΡΞ ΚΑΝΕΝΑ ΠΡΟΒΛΗΜΑ ΚΑΙ ΓΙ ΑΥΤΟ ΔΕΝ ΓΝΩΡΙΖΑΜΕ ΟΤΙ ΕΧΕΙ ΑΥΤΗ ΤΗΝ ΠΑΘΗΣΗ. ΤΩΡΑ ΟΜΩΣ ΠΑΡΟΥΣΙΑΖΕΙ ΑΡΚΕΤΑ ΠΡΟΒΛΗΜΑΤΑ. ΕΧΕΙ ΒΡΕΘΕΙ ΚΑΠΟΙΑ ΚΑΡΔΙΑ ΓΙΑ ΝΑ ΓΙΝΕΙ ΜΕΤΑΜΟΣΧΕΥΣΗ ΑΛΛΑ ΑΥΤΟ ΠΡΕΠΕΙ ΝΑ ΓΙΝΕΙ ΣΤΗ WASHINGTON ΤΩΝ Η.Π.Α ΚΑΙ ΕΜΕΙΣ ΕΙΜΑΣΤΕ ΜΙΑ ΜΕΣΗ ΟΙΚΟΓΕΝΕΙΑ ΧΩΡΙΣ ΤΗΝ ΟΙΚΟΝΟΜΙΚΗ ΑΝΕΣΗ ΝΑ ΠΑΜΕ ΤΟ ΚΟΡΙΤΣΑΚΙ ΜΑΣ ΕΚΕΙ. ΔΕΝ ΜΠΟΡΟΥΜΕ ΝΑ ΠΑΡΟΥΜΕ ΔΑΝΕΙΟ ΚΑΙ ΖΟΥΜΕ ΜΕ ΝΟΙΚΙ, ΟΠΟΤΕ ΔΕΝ ΕΧΟΥΜΕ ΑΚΙΝΗΤΑ ΝΑ ΠΟΥΛΙΣΟΥΜΕ.

Ο ΔΗΜΟΣ ΑΝΩ ΛΙΟΣΙΩΝ ΚΑΙ ΤΟ ΧΑΜΟΓΕΛΟ ΤΟΥ ΠΑΙΔΙΟΥ ΔΙΝΟΥΝ ΜΑΖΙ ΕΝΑ ΟΛΟΚΛΗΡΟ ΕΥΡΩ ΓΙΑ ΚΑΘΕ ΦΟΡΑ ΠΟΥ ΑΠΟΣΤΕΛΕΤΑΙ ΑΥΤΤΟ e-mail.

ΕΝΑ 2ΧΡΟΝΟ ΠΑΙΔΑΚΙ ΥΠΟΦΕΡΕΙ. ΣΑΣ ΠΑΡΑΚΑΛΟΥΜΕ, ΒΟΗΘΕΙΣΤΕ ΤΗΝ ΚΟΡΟΥΛΑ ΜΑΣ.

ΣΑΣ ΕΥΧΑΡΙΣΤΟΥΜΕ.

22/12/2008

Μετά την παραλαβή του συγκεκριμένου μηνύματος από κάποιο χρήστη ενός ελληνικού forum, ο συγκεκριμένος χρήστης απέστειλε διευκρινιστική ερώτηση στο «Χαμόγελο του Παιδιού» και έλαβε την ακόλουθη απάντηση.

Αγαπητέ κύριε Φισκίλη,

Θα θέλαμε καταρχάς να σας ευχαριστήσουμε για το ενδιαφέρον με το οποίο αντιμετωπίσατε το μήνυμα που μας προωθήσατε. Είναι πολύ σημαντικό ο καθένας μας να αντιμετωπίζει τέτοιου είδους μηνύματα με την απαραίτητη κρίση και υπευθυνότητα, καθώς αποτελεί έγκλημα τόσο σοβαρά ζητήματα να γίνονται αντικείμενο εκμετάλλευσης και κερδοσκοπίας από κάποιους και να μειώνουν την σοβαρότητα που έχουν τα πραγματικά τέτοια περιστατικά.

Διαψεύδουμε λοιπόν κατηγορηματικά την οποιαδήποτε ανάμιξη του Οργανισμού μας στο παρακάτω -υποτιθέμενο- ιατρικό πρόβλημα. Το Χαμόγελο του Παιδιού, πράγματι, στηρίζει ενεργά και ουσιαστικά, χιλιάδες παιδιά στην Ελλάδα που αντιμετωπίζουν σοβαρά προβλήματα (όπως μπορείτε να ενημερωθείτε αναλυτικότερα και στην ιστοσελίδα μας), αλλά ποτέ με τρόπο που να θίγει την

αξιοπρέπεια του παιδιού και της οικογένειας που αντιμετωπίζει το πρόβλημα. Ο σεβασμός προς την οικογένεια και το παιδί, αποτελούν έναν από τους βασικούς γνώμονες που ακολουθούμε σε κάθε δράση μας.

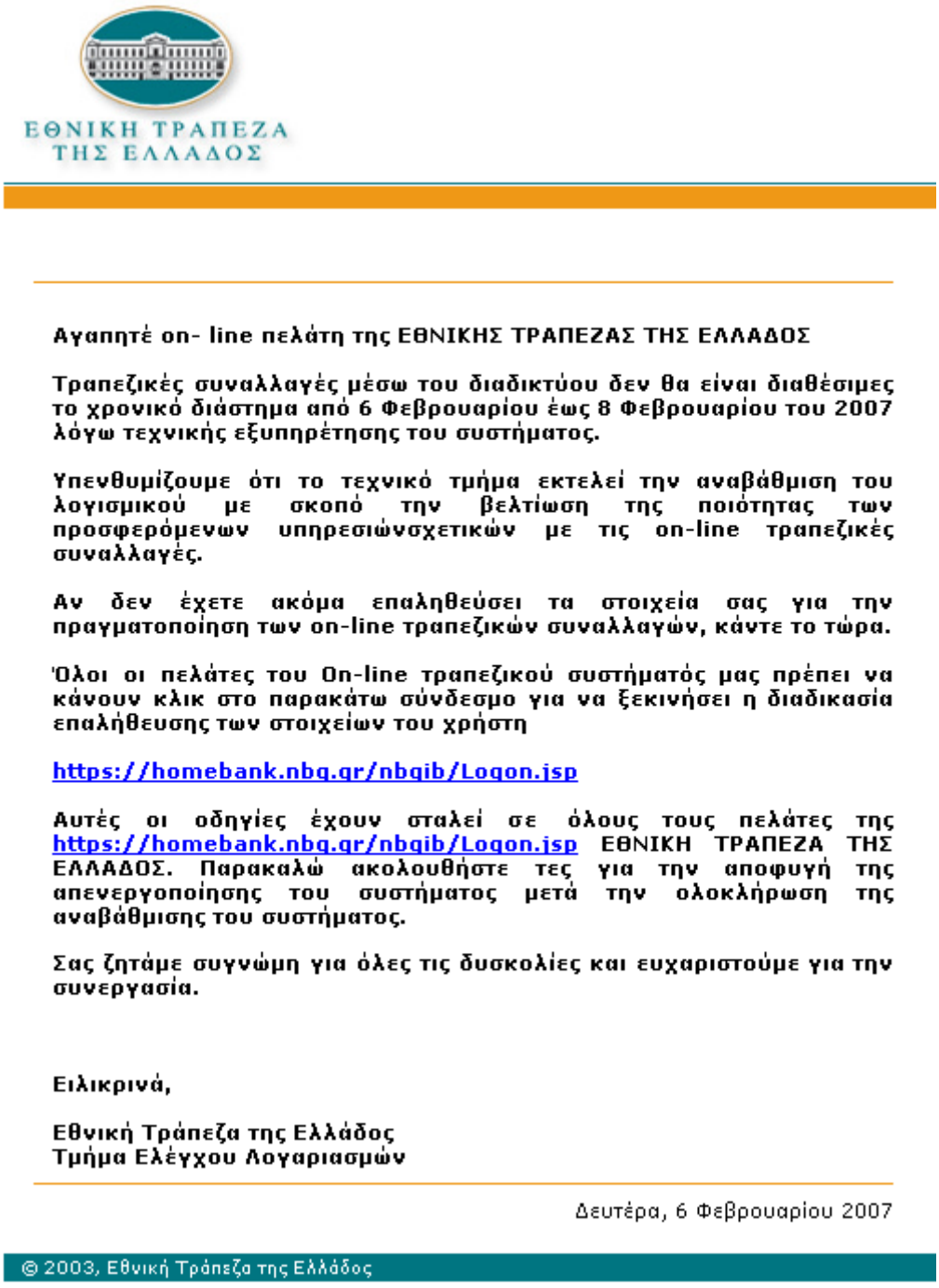
Είμαστε στη διάθεσή σας για οποιαδήποτε περαιτέρω πληροφορία αναφορικά με τον Οργανισμό και τη δράση μας.

Σας ευχαριστούμε θερμά.

Με εκτίμηση,
Για "το Χαμόγελο του Παιδιού"

Χρύσα Αργυρού
Κοινωνιολόγος
*210 330*****

4. SPAM απάτη (Τραπεζικών Λογαριασμών)



ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ
ΤΗΣ ΕΛΛΑΔΟΣ

Αγαπητέ on- line πελάτη της ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ

Τραπεζικές συναλλαγές μέσω του διαδικτύου δεν θα είναι διαθέσιμες το χρονικό διάστημα από 6 Φεβρουαρίου έως 8 Φεβρουαρίου του 2007 λόγω τεχνικής εξυπηρέτησης του συστήματος.

Υπενθυμίζουμε ότι το τεχνικό τμήμα εκτελεί την αναβάθμιση του λογισμικού με σκοπό την βελτίωση της ποιότητας των προσφερόμενων υπηρεσιώνσχετικών με τις on-line τραπεζικές συναλλαγές.

Αν δεν έχετε ακόμα επαληθεύσει τα στοιχεία σας για την πραγματοποίηση των on-line τραπεζικών συναλλαγών, κάντε το τώρα.

Όλοι οι πελάτες του On-line τραπεζικού συστήματός μας πρέπει να κάνουν κλικ στο παρακάτω σύνδεσμο για να ξεκινήσει η διαδικασία επαλήθευσης των στοιχείων του χρήστη

https://homebank.nbg.gr/nbgib/Logon.jsp

Αυτές οι οδηγίες έχουν σταλεί σε όλους τους πελάτες της https://homebank.nbg.gr/nbgib/Logon.jsp ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ. Παρακαλώ ακολουθήστε τες για την αποφυγή της απενεργοποίησης του συστήματος μετά την ολοκλήρωση της αναβάθμισης του συστήματος.

Σας ζητάμε συγνώμη για όλες τις δυσκολίες και ευχαριστούμε για την συνεργασία.

Ειλικρινά,

Εθνική Τράπεζα της Ελλάδος
Τμήμα Ελέγχου Λογαριασμών

Δευτέρα, 6 Φεβρουαρίου 2007

© 2003, Εθνική Τράπεζα της Ελλάδος

5. SPAM απάτη (Nigeria – Επιχειρηματική Πρόταση)

Ονομάζομαι Μομπάτε-Κόκο-Σούμα και είμαι γιός του ένδοξου Σομπάτε-Κάκο-Σούμα Βασιλιά του Ραμπούτου, ενός μικρού αλλά πλούσιου κρατίδιου στη Ζιμπάμπουε.

Το άδικο καθεστώς του σκληρού και αυταρχικού δικτάτορα Σεμαμπούτου έχει επιβάλλει ένα πρόστιμο 1.000 δολαρίων που απαγορεύει σε μένα και στην ένδοξη οικογένειά μου να διαχειριστούμε την αμύθητη περιουσία μας που αποτελείται από διαμάντια, πετρελαιοπηγές και χιλιάδες εκτάρια εύφορης γης.

Αναγκάζομαι, παρά την καταγωγή μου, να σας ζητήσω να μου στείλετε τα χρήματα με την υπόσχεση να σας τα επιστρέψω στο τετραπλάσιο μόλις ανακτήσω τα οικογενειακά μας πλούτη.

Μετά Τιμής

Μομπάτε-Κάκο-Σούμα

Πρωτότοκος υιός του Σομπάτε Βασιλιά του Ραμπούτο

6. SPAM malware

ΕΑΝ ΚΑΝΕΤΕ ΚΛΙΚ ΣΤΗΝ ΣΕΛΙΔΑ ΑΥΤΗ ΤΡΕΦΟΝΤΑΙ ΠΑΙΔΙΑ ΧΥΡΙΣ ΔΙΚΗ ΣΑΣ ΔΑΠΑΝΗ. 5 ΚΛΙΚ ΤΗ ΜΕΡΑ - 5 ΠΑΙΔΙΑ ΕΠΙΒΙΩΝΟΥΝ ΧΑΡΙ ΣΕ ΣΑΣ!!!!

http://www.fighthunger.org/en/node/2783

7. SPAM Hoax

Subject: FW: Epikundunos ios kukloforei!!

*Τις επόμενες ημέρες θα πρέπει να είστε προσεκτικοί και να μην ανοίξετε κανένα μήνυμα με τον τίτλο **'invitation',** ανεξάρτητα με το ποιος το στέλνει**,** πρόκειται για ένα ιό ο οποίος **'**ανάβει**'** μια ολυμπιακή δάδα που καίει το σκληρό δίσκο του **Pc.***

*Αυτός ο ιός θα σας σταλεί από ένα άτομο που έχετε ήδη στη λίστα επαφών σας**,** για αυτό θα πρέπει να ενημερώσετε όσο το δυνατό περισσότερους**.***

*Εάν λάβετε μήνυμα με τον τίτλο **'invitation'** μην το ανοίξετε και κλείστε αμέσως το **Pc.** Είναι ο χειρότερος ιός που ανακοινώθηκε από το **CNN** και αξιολογήθηκε από τη **Microsoft** ως ο πιο καταστροφικός ιός που έχει υπάρξει ποτέ**.** Ο συγκεκριμένος ιός*

*ανακαλύφθηκε χτές από το **MCAfee** και δεν υπάρχει ακόμα **'λύση'** για αυτόν**.** Απλά καταστρέφει τον Τομέα **Zero** του σκληρού δίσκου όπου βρίσκονται οι σημαντικότερες πληροφορίες**.***

*Αποστείλετε αυτό το **e-mail** σε όσους γνωρίζετε**,** στους φίλους και γνωστούς σας και θυμηθείτε πως αν το αποστείλετε σε όλους αυτούς**,** θα επωφεληθούμε όλοι**.***

8. SPAM Hoax

Ο** πλανήτης Άρης θα είναι ορατός στον ουρανό νύχτας αυτόν τον Αύγουστο**.

-** Θα φανεί τόσο μεγάλος όσο η Πανσέληνος στο γυμνό μάτι**.

-** Καλύτερη στιγμή να το παρατηρήσετε θα είναι στις **27** Αυγούστου στις **12.30** το βράδυ όταν ο Άρης θα έρθει σε απόσταση **34.65**Μ μίλια από τη γη**.

-** Να προσέξετε τον ουρανό στις **27** του Αυγούστου **12:30 AM.

-** Θα μοιάσει σαν να έχει η γη **2** φεγγάρια**.

-** ΜΗΝ ΤΟ ΧΑΣΕΤΕ ΑΥΤΟ**.....** Η επόμενη φορά που ο Αρης θα έρθει τόσο κοντά θα είναι το **2287.

-** ΣΗΜΕΙΩΣΗ**:** Μοιραστείτε το με τους φίλους σας δεδομένου ότι ΚΑΝΕΝΑΣ ΖΩΝΤΑΝΟΣ ΣΗΜΕΡΑ δέν θα ξαναδεί τέτοιο θέαμα**.

Παράρτημα Γ

Στατιστικά Στοιχεία για το SPAM

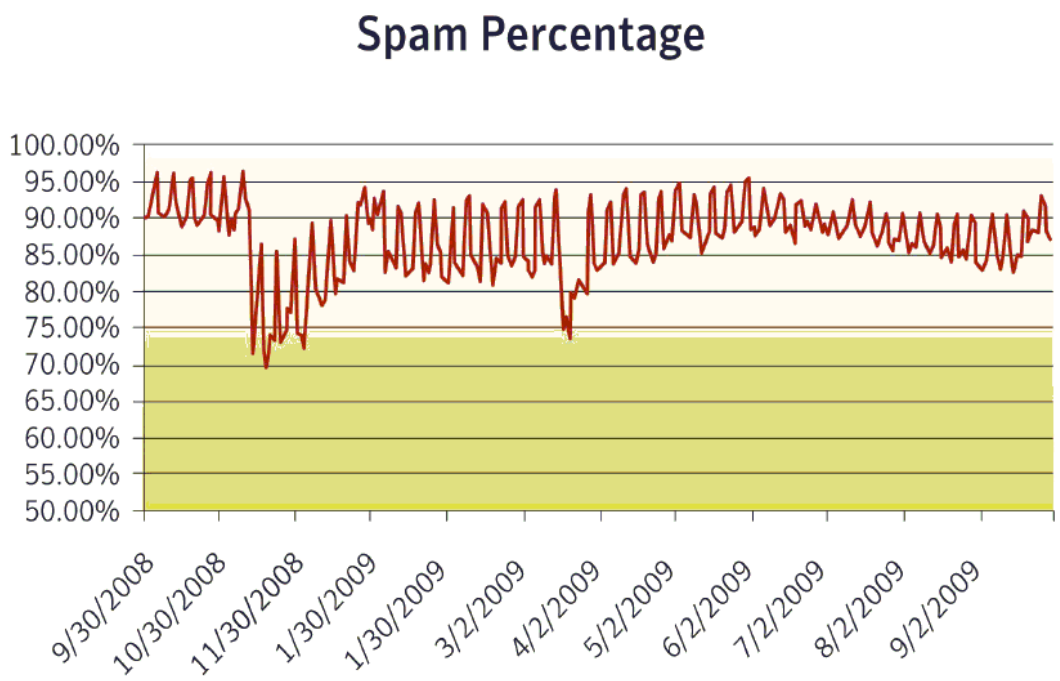
Έρευνα για το SPAM – Σεπτέμβριος 2009

Σύμφωνα με την έρευνα Οκτωβρίου (report #34), της παγκοσμίως γνωστής εταιρείας Symantec, κατά τον μήνα Σεπτέμβριο τα spam mails σε διεθνές επίπεδο, ξεπέρασαν κατα μέσο όρο το 86%, του συνόλου της ηλεκτρονικής αλληλογραφίας.

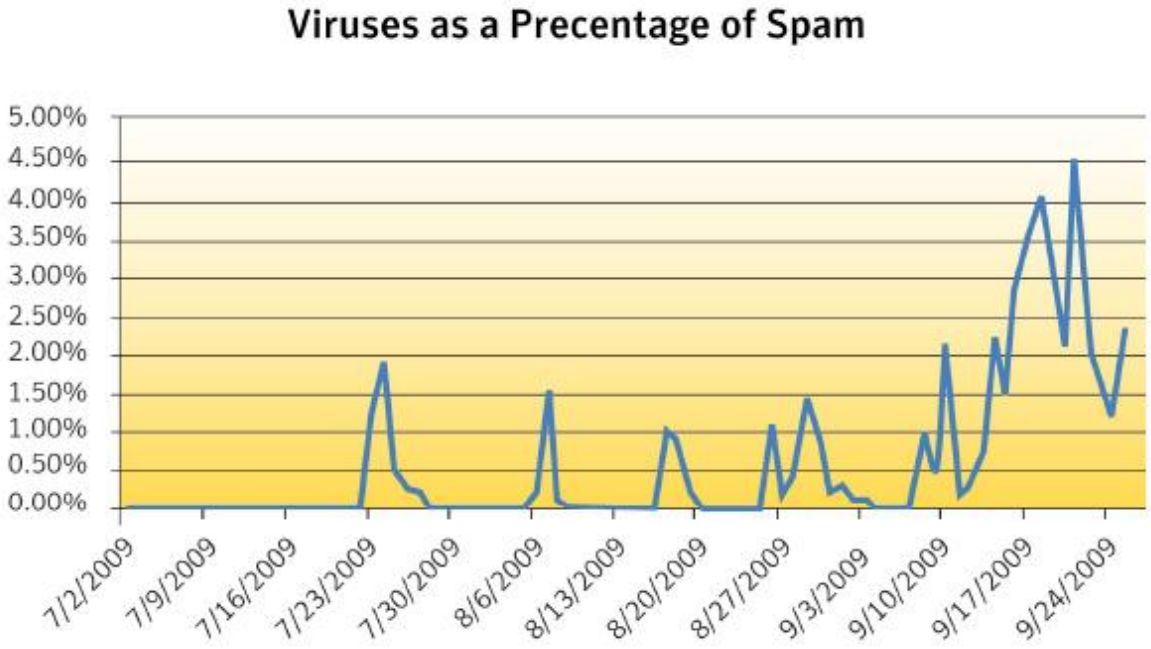
Επίσης ενδιαφέρον εύρημα της συγκεκριμένης έρευνας, είναι το γεγονός ότι φαίνεται να έχει αυξηθεί το ποσοστό των spam μηνυμάτων που περιείχαν κακόβουλο λογισμικό, σε 4.5%.

Ακολουθούν ενδιαφέροντα γραφήματα, της συγκεκριμένης έρευνας που αφορούν:

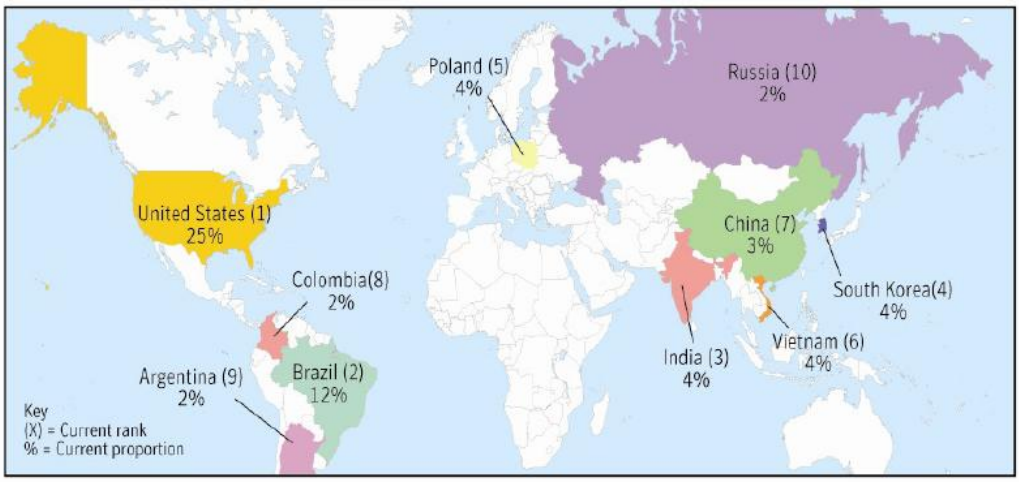
i. Την διακύμανση των ποσοστών εμφάνισης spam μηνυμάτων στο σύνολο της ηλεκτρονικής αλληλογραφίας.
ii. Την διακύμανση της "περιεκτικότητας" σε κακόβουλο λογισμικό, των spam μηνυμάτων.
iii. Το ποσοστό "συνεισφοράς" κάθε χώρας στο φαινόμενο του spam.
iv. τα subjects που χρησιμοποιήθηκαν περισσότερο τους συγκεκριμένους μήνες στην ανεπιθύμητη αλληλογραφία.
v. Τις κατηγορίες διαφημίσεων που αφορούσαν τα spam μηνύματα την συγκεκριμένη περίοδο.



[Στο συγκεκριμένο διάγραμμα παρουσιάζεται η διακύμανση του ποσοστού του SPAM, τους τελευταίους μήνες.]



[Στο συγκεκριμένο διάγραμμα παρουσιάζεται η διακύμανση της "περιεκτικότητας" σε κακόβουλο λογισμικό, των spam μηνυμάτων, τους τελυταίους μήνες.]



Country	September	August	Change
United States	25%	23%	2%
Brazil	12%	12%	0%
South Korea	4%	5%	-1%
India	4%	4%	0%
Colombia	2%	2%	0%
Poland	4%	4%	0%
China	3%	3%	0%
Vietnam	4%	3%	1%
Argentina	2%	2%	0%
Russia	2%	Not Listed	n/a

[Στο συγκεκριμένο διάγραμμα παρουσιάζεται η “συνεισφορά” κάθε χώρας στο φαινόμενο του spam, για τους μήνες, Αύγουστος & Σεπτέμβριος 2009.]

#	Total Spam: September 2009 Top Subject Lines	No of Days	Total Spam: August 2009 Top Subject Lines	No of Days
1	Notice of Underreported Income	20	Delivery Status Notification (Failure)	31
2	Delivery Status Notification (Failure)	30	Delivery Status Notification	31
3	failure notice	30	Re: Order status	31
4	Undelivered Mail Returned to Sender	30	Your order	31
5	Thank you for setting the order No.475456	17	RE: Message	31
6	Returned mail: see transcript for details	30	Return Mail	31
7	Gain 3Inches	27	no-reply	31
8	Delivery Status Notification	30	new mail	31
9	Your order	22	Return mail	31
10	RE: Message	20	Undelivered Mail Returned to Sender	31

[Στο συγκεκριμένο διάγραμμα παρουσιάζονται τα subjects που χρησιμοποιήθηκαν περισσότερο τους συγκεκριμένους μήνες στην ανεπιθύμητη αλληλογραφία.]

Category Name	September	August	Change
adult	1.50%	1.80%	0%
financial	17.10%	19.68%	-3%
fraud	6.60%	6.55%	0%
health	6.90%	6.73%	0%
internet	32.30%	29.30%	3%
leisure	3.10%	4.16%	-1%
419 spam	9.70%	9.23%	0%
political	<1%	<1%	No Change
products	19.60%	18.30%	1%
scams	2.70%	3.84%	-1%

[Στο συγκεκριμένο διάγραμμα παρουσιάζονται οι κατηγορίες διαφημίσεων, που αφορούσαν τα spam μηνύματα την συγκεκριμένη περίοδο.]

Παράρτημα Δ

Παρουσίαση υλοποίησης online οδηγού για το SPAM

"Twenty years from now you will be more disappointed by the things you didn't do than by the ones you did do. So throw off the bowlines. Sail away from the safe harbor. Catch the trade winds in your sails. Explore. Dream. Discover"

~ Mark Twain

Online Οδηγός Διαχείρισης Κινδύνων

Στα πλαίσια της συγκεκριμένης εργασίας αναπτύξαμε έναν online οδηγό σχετικό με το SPAM, ο οποίος παρουσιάζει τα ευρήματα της εργασίας μας, παραθέτοντας αυτούσιο το κείμενο της καθώς και διασυνδέσεις, με άλλους ενδιαφέροντες ιστότοπους.

Η διεύθυνση μέσα από την οποία μπορείτε να προσπελάσετε τον ιστότοπο μας είναι η ακόλουθη:

4. http://www.spamming.gr

Εργαλεία, τεχνικές και γλώσσες ανάπτυξης του ιστότοπου μας

Για την υλοποίηση του online αυτού χώρου, αρχικά μισθώθηκε χώρος στην εταιρεία DNHOST (www.dnhost.gr), στους servers της οποίας στήσαμε την σελίδα, ενώ στην συνέχεια αγοράστηκε το παραπάνω διακριτικό όνομα, με μεταπωλητή την ίδια εταιρεία.

Από λογισμικό ανοιχτού κώδικα (Open Source), χρησιμοποιήθηκε το δημοφιλές σύστημα διαχείρισης περιεχομένου (Content Management System – CMS) Joomla, (www.joomla.org, www.joomla.gr) το οποίο και εξατομικεύθηκε με γνώμονα τις ανάγκες μας (περιεχόμενα, γλώσσα επικοινωνίας, δημιουργία νέων banners, νέο στύλ μορφοποίησης (CSS-style) κ.α.).

Για την ανάπτυξη του ιστότοπου, χρησιμοποιήθηκαν εκτενώς, τεχνολογίες HTML, D-HTML, Ajax, Javascript, SQL, PHP, CSS.

Για την δημιουργία του εισαγωγικού banner, χρησιμοποιήθηκε το πρόγραμμα Adobe Flash CS3 Professional, ενώ για την συγγραφή σχεδόν του συνόλου των υπολοίπων αρχείων, το Notepad των Windows Vista Business Edition, στο οποίο σώζαμε τα αρχεία με κωδικοποίηση UTF-8, λόγω χρήσης της Ελληνικής γλώσσας στον κώδικα.

Ως ftp-client τέλος χρησιμοποιήθηκε το πρόγραμμα WinSCP (www.winscp.net), το οποίο μας φάνηκε πραγματικά πολύ χρήσιμο.

Ακολουθεί στην επόμενη σελίδα, πλήρης παρουσίαση μέσω εικόνων, του online οδηγού παρουσίασης.

Παρουσίαση Οδηγού

Ακολουθεί πλήρης παρουσίαση μέσω εικόνων, του online οδηγού παρουσίασης.

Εισαγωγικό banner

Κατα την προσπέλαση της διεύθυνσης http://www.spamming.gr αρχικά αντικρύζουμε ένα εισαγωγικό banner της διπλωματικής εργασίας.

[Τίτλος εργασίας και **ο**νόματα συγγραφέων και υπεύθυνου καθηγητή**]**

Κεντρική Σελίδα

Αμέσως μετά το τέλος του εισαγωγικού βίντεο, ανακατευθυνόμαστε στην διεύθυνση www.spamming.gr/main/ η οποία αποτελεί και την κεντρική μας σελίδα.

Στην δεξιά στήλη της κεντρική μας σελίδας, μπορούμε να διακρίνουμε ένα σύστημα παράθεσης ειδήσεων απο το spamnews.com, μέσω ειδικού rss feed.

Στην αριστερή στήλη, έχουμε το menu με τα περιεχόμενα όπου βρίσκουμε τις ακόλουθες επιλογές:

i. **Εισαγωγή:** Μας ανακατευθύνει σε νέα σελίδα, όπου μπορούμε να βρούμε κάποιες εισαγωγικές πληροφορίες σχετικές με την διπλωματική εργασία, όπως : **Εισαγωγή, Ευχαριστίες**

ii. **Εργασία:** Μας ανακατευθύνει στην σελίδα παρουσίασης του pdf αρχείου της διπλωματική εργασίας. (Με δεξί κλίκ και αποθήκευση ώς... μπορούμε να μεταφορτώσουμε το αρχείο στον σκληρό μας δίσκο).

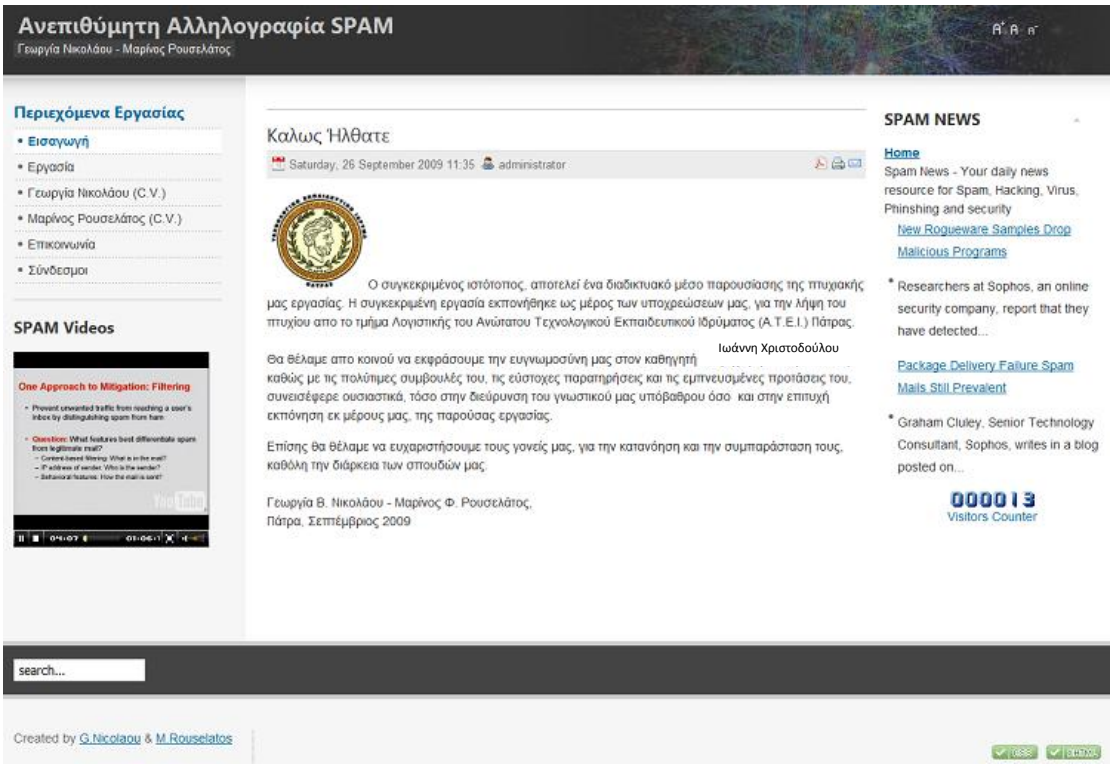
iii. **Γεωργία Νικολάου (C.V.):** Το βιογραφικό μας.

iv. **Μαρίνος Ρουσελάτος (C.V.):** Το βιογραφικό μας.

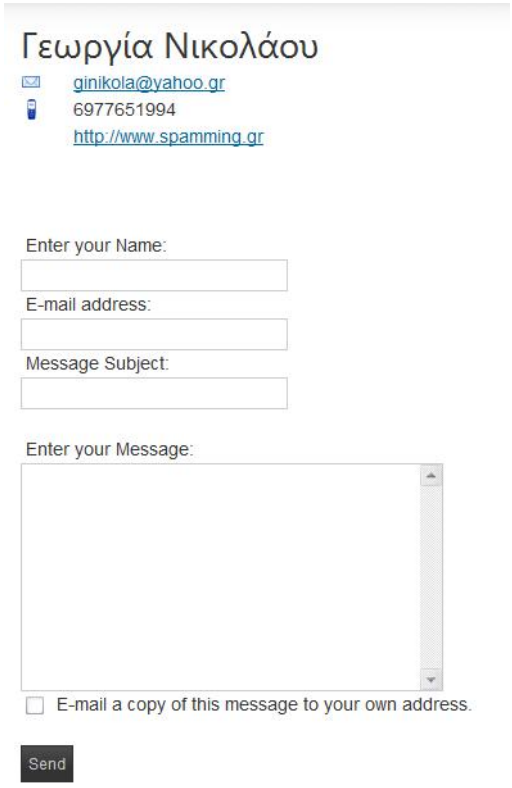
v. **Επικοινωνία:** Μας ανακατευθύνει στη σελίδα επικοινωνίας, όπου μπορούμε να δούμε τα στοιχεία επικοινωνίας, τόσο των συγγραφέων της εργασίας, όσο και του υπεύθυνου καθηγητή. (Κάθε επαφή οδηγεί σε μια φόρμα, εξατομικευμένης ώς προς τον παραλήπτη κάθε φορά, αποστολής email)

vi. **Σύνδεσμοι:** Μας ανακατευθύνει στη σελίδα των προτεινόμενων διασυνδέσεων.

Ακολουθεί screenshot της κεντρικής σελίδας...



[Κεντρική Σελίδα**:** **www.spamming.gr/main]**



[Παράδειγμα**:** φόρμα αποστολής **email]**

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

1. **ΑΤΟΜΙΚΑ ΣΤΟΙΧΕΙΑ :**
   - Ονοματεπώνυμο: Νικολάου Γεωργία
   - Τηλέφωνο : 6977651994
   - Διεύθυνση ηλεκτρονικού ταχυδρομείου: ginikola@yahoo.gr, nicolaou@spamming.gr
   - Ημερομηνία γέννησης : 5 Μαρτίου 1987
   - Τόπος γέννησης: Αθήνα
   - Οικογενειακή κατάσταση : Άγαμος

2. **ΕΚΠΑΙΔΕΥΣΗ:**
   - Απολυτήριο Λυκείου από το 4ο Ενιαίο Λύκειο Άρτας (Βαθμός Απολυτηρίου 14,9)
   - Πτυχιούχος του τμήματος Λογιστικής του Α.Τ.Ε.Ι. Πάτρας

3. **ΕΡΓΑΣΙΑΚΗ ΠΡΟΫΠΗΡΕΣΙΑ :**
   - Από 15/06/07 έως και 15/09/07: Ως βοηθός λογιστή στο λογιστικό γραφείο του Κ .Πούντου (Αντιδήμαρχος) στην Αίγινα (ως άμισθος υπάλληλος για εκμάθηση).
   - Από 01/10/08 έως και 31/03/09 Πρακτική άσκηση ως βοηθός λογιστή στην εταιρεία ΒΟΥΤΑΣ Α.Ε. .
   - Από 01/07/09 έως και σήμερα στο λογιστήριο της ΑΦΟΙ ΠΑΠΑΔΟΠΟΥΛΟΙ ΟΕ – Εισαγωγές και εμπορία χρωμάτων.

4. **ΞΕΝΕΣ ΓΛΩΣΣΕΣ:**
   - Αγγλικά

[Παράδειγμα**:** βιογραφικό σημείωμα**]**

#	Name	Position	Phone	Mobile Phone Number	Fax
1	**Γεωργία Νικολάου**	Συγγραφέας Εργασίας	-	6977651994	-
			-	-	-
3	**Μαρίνος Ρουσελάτος**	Συγγραφέας Εργασίας	-	-	-

[Σελίδα Επικοινωνίας **-** Επαφών**]**

links

Display # 20

#	Web Link	Hits
1	**www.no-spam.gr** Δικτυακός τόπος αφιερωμένος στην καταπολέμηση του spam... Ένα απο τα καλύτερα site στο είδος του και το καλύτερο ελληνικό στον τομέα...	0
2	**Α.Τ.Ε.Ι. Πάτρας** Το Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα της Πάτρας	0
3	**Λίστα με ενδιαφέροντες σύνδεσμους...** Σύνδεσμοι για το SPAM	3

• **links** (3)

[Σελίδα Συνδέσμων**]**