Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Μέθοδοι και Τεχνικές αντιμετώπισης Αυτόκλητων Μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam)

Γεωργία Βαρδάκη

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Αύγουστος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μέθοδοι και Τεχνικές αντιμετώπισης Αυτόκλητων Μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam)

Γεωργία Βαρδάκη

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος 2014

Περίληψη

Η εργασία αυτή έχει ως θέμα τα αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου και τις μεθόδους πρόληψης και αντιμετώπισής τους. Στις μέρες μας παρατηρείται τεράστια αύξηση στην αποστολή μηνυμάτων spam παγκοσμίως, για αυτό και η ανάγκη για μεθόδους και τεχνικές αντιμετώπισής τους είναι πλέον επιτακτική.

Αυτή η εργασία ως στόχο έχει να αναπτυχθεί πλήρως η έννοια των spam αλλά και να γίνει διεξοδική ανάλυση των βασικών τεχνικών για την πρόληψη, διαχείριση και αντιμετώπισή τους. Η εργασία αποτελείται από 6 κεφάλαια. Το πρώτο κεφάλαιο ορίζει την έννοια spam, αναφέρει την προέλευση του spamming, αλλά και ορίζει τις βασικές κατηγορίες στις οποίες χωρίζεται. Στο δεύτερο κεφάλαιο αναφέρεται στους λόγους που καθιστούν το spamming πρόβλημα, καθώς επίσης αναλύει την έκταση του προβλήματος. Το επόμενο κεφάλαιο πραγματεύεται την ανάλυση των βασικών αρχιτεκτονικών φιλτραρίσματος spam, παρουσιάζοντας τα βασικά χαρακτηριστικά τους. Στο τέταρτο κεφάλαιο διατυπώνεται μια συγκριτική μελέτη των μεθόδων πρόληψης και αντιμετώπισης spam, αναλύοντας τα βασικά πλεονεκτήματα και μειονεκτήματά τους. Στο πέμπτο κεφάλαιο γίνεται αναφορά στο νομοθετικό πλαίσιο σε σχέση με τα spam και παρουσιάζεται το ισχύον θεσμικό πλαίσιο της Ελλάδας, αλλά και οι ρυθμίσεις που ισχύουν για την Ευρώπη. Τέλος, στο έκτο και τελευταίο κεφάλαιο διατυπώνονται επιγραμματικά τα συμπεράσματα που προκύπτουν από τη μελέτη που έγινε.

Οι τεχνικές πρόληψης και αντιμετώπισης των spam μηνυμάτων έχουν αναπτυχθεί ραγδαία τα τελευταία χρόνια, καθώς ο όγκος της ανεπιθύμητης αλληλογραφίας αυξάνεται συνεχώς. Η παρούσα εργασία παρουσιάζει αναλυτικά το πρόβλημα των αυτόκλητων μηνυμάτων και παρέχει πολύπλευρες λύσεις για την προστασία των χρηστών, ενώ δίνει βάση στην αντιμετώπιση των spam από νομικής πλευράς.

Summary

This paper's subject is unsolicited e-mails and methods to prevent and deal with them. Nowadays there is a huge increase in sending spam messages worldwide, so the need for methods and techniques to deal with them is most urgent.

In this paper the aim is to fully develop the concept of spam but also to analyze thoroughly the key techniques for the prevention, management and deal with them. The thesis consists of six chapters. The first chapter defineσ the term spam, indicates the origin of spamming but also defines the main categories under which spam is separated. The second chapter discusses the reasons that make the spamming a problem and also analyzes the extent of the problem. The next chapter deals with the analysis of the main filtering spam methods, presenting the main characteristics of them. The fourth chapter sets out a comparative study of methods to prevent and deal with spam, analyzing the main advantages and disadvantages of each method. The fifth chapter is a reference to the legislative framework in relation to spam and presents the current institutional framework in Greece and the arrangements for Europe. Finally, the sixth and final chapter succinctly formulated the conclusions of the study conducted.

The techniques of prevention and treatment of spam messages have grown rapidly in recent years, as the volume of spam is increasing. This paper presents in detail the problem of spam and provides multiple solutions to protect users while emphases on addressing the spam problem from a legal standpoint.

Στόχοι εργασίας

Με την παρούσα εργασία θέλουμε πρώτα απ' όλα οι χρήστες να κατανοήσουν πλήρως την έννοια των spam, αλλά και να μάθουν απλές τεχνικές για να τα αναγνωρίζουν και να προφυλάσσονται από αυτά.

Έπειτα, θέλουμε να τονίσουμε την σημασία των spam filters για την προστασία από ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου και να αναδείξουμε τις βασικές κατηγορίες αυτών, παρέχοντας μία ολοκληρωμένη περιγραφή του τρόπου λειτουργίας τους. Ωστόσο, βασικός σκοπός της εργασίας είναι να παρέχει στους χρήστες μία ολοκληρωμένη συγκριτική ανάλυση των υπαρχόντων spam filters και όχι απλά μία παράθεση των κύριων χαρακτηριστικών τους. Έτσι, για να διαφοροποιηθεί η εργασία από παρόμοιες αναλύσεις που έχουν γίνει μέχρι σήμερα, παρουσιάζονται όχι μόνο τα πλεονεκτήματα και μειονεκτήματα της κάθε μεθόδου, αλλά και συνοψίζονται σε συγκεντρωτικό συγκριτικό πίνακα (ο οποίος προκύπτει μέσω διεξοδικής έρευνας και ανάλυσης), που καθιστά την σύγκριση μεταξύ τους ευκολότερη. Με τον τρόπο αυτόν διευκολύνεται η επιλογή του καταλληλότερου φίλτρου από τους χρήστες ή ακόμη και ο καταλληλότερος συνδυασμός αυτών, ανάλογα με τις ανάγκες τους.

Τέλος, σημαντικό είναι οι χρήστες να κατανοήσουν ότι τα μηνύματα spam δεν αποτελούν μόνο πρόβλημα, αλλά είναι και παράνομα και έτσι παρατίθεται ενότητα στην εργασία, όπου αναλύεται το ισχύον νομοθετικό πλαίσιο ενάντια στα spam, τόσο στην Ευρώπη, όσο και στην Ελλάδα.

Ευχαριστίες

Η παρούσα διατριβή πραγματοποιήθηκε υπό την επίβλεψη του Καθ. Στέφανου Γκρίτζαλη στον οποίο θα ήθελα να εκφράσω τις ευχαριστίες μου για την πολύτιμη και φιλική καθοδήγηση του, την ενθάρρυνση και υποστήριξή του καθ' όλη τη διάρκεια εκπόνησης της μεταπτυχιακής διατριβής μου , καθώς επίσης και για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Ιδιαίτερες ευχαριστίες θα ήθελα να εκφράσω στους γονείς μου για την ψυχολογική, ηθική και οικονομική τους υποστήριξη σε κάθε στάδιο των σπουδών μου.

Τέλος θα ήθελα να ευχαριστήσω θερμά τους φίλους μου που πίστεψαν σε μένα, με ενθάρρυναν, με στήριξαν ψυχολογικά και έδειξαν κατανόηση κατά το δύσκολο χρονικό διάστημα εκπόνησης της διατριβής μου.

Περιεχόμενα

1 Εισαγωγή 1
1.1 Ο ορισμός του spam 1
1.2 Η προέλευση του spamming 3
1.2.1 Η προέλευση του όρου spam 3
1.2.2 Η «ιστορία» του spam 4
1.3 Κατηγοριοποίηση Spamming 4
1.3.1 Κατηγορίες βάση περιεχομένου spam 4
Commercial Spam Forms 5
Phishing Spam 5
Scam 6
Adult Content Spam 6
Noncommercial Spam Forms 6
1.3.2 Κατηγορίες βάσει μέσου διάδοσης spam 7
E-mail spamming 7
Instant Messaging Spam 8
Mobile Phone Spam 9
Social Networking Spam 10
Blog, wiki Spam 10
Forum Spam 11
2 Το spam ως πρόβλημα 13
2.1 Γιατί το spam αποτελεί πρόβλημα 13
2.2 Η έκταση του προβλήματος σήμερα 16
3 Αρχιτεκτονικές Spam Filtering 19
3.1 Ορισμός Spam Filter 19
3.2 Απαιτήσεις Αρχιτεκτονικών Spam Filtering 20
3.3 Κατηγορίες Spam Filtering 23
3.3.1 End-user techniques 23
3.3.2 Αυτοματοποιημένες τεχνικές για email administrators 25
3.3.2.1 Origin-Based Filters 26
Blacklists 26
Whitelists 28

	Greylists	29
	Realtime Blackhole Lists	29
	DNS-based Blackhole List (DNSBL)	30
	Challenge-Response Filtering	30
3.3.2.2	Content – Based Filters	32
	Word – Based Filters	32
	Heuristic (rule-based) Filters	32
	Bayesian Filtering	33
	Signature-Based Filtering	35
	Clustering Techniques	36
3.3.2.3	Social Networks-Based Filters	37
3.3.2.4	Traffic Analysis Based Filters	38
	Mail-Volume Based Filters	38
3.3.2.5	Άλλοι τύποι φίλτρων	39
	Collaborative Filtering	39
	DNS Lookup Systems	40
	Payment-Based Approach	40
	Συνδυασμός Φίλτρων	41
3.3.3	Τεχνικές για ερευνητές και για όργανα επιβολής του νόμου	42
4	**Συγκριτική Μελέτη Anti-spam Methods**	44
4.1	Ανάλυση Συγκριτικών Αποτελεσμάτων	45
4.2	Email Services και Spam Filters	57
5	**Νομοθετικό Πλαίσιο για τα Spam**	63
5.1	Πως προκύπτουν οι Anti-spam Νόμοι	63
5.2	Νομοθετικό Πλαίσιο Anti-spam στην Ευρώπη	67
5.3	Νομοθετικό Πλαίσιο Anti-spam στην Ελλάδα	69
5.4	Η αποτελεσματικότητα των Anti-spam Νόμων	73
6	**Επίλογος**	76
	Πίνακας Ορολογίας (Ελληνική Απόδοση)	78
	Πίνακας Ορολογίας (Ξενόγλωσση Απόδοση)	79
	Συντμήσεις – Αρκτικόλεξα - Ακρωνύμια	80
	Βιβλιογραφία	81

Πίνακας Εικόνων

Εικόνα 2.1:	Το ποσοστό των spam σε σχέση με το συνολικό αριθμό e-mail το 2013	17
	Ανακτήθηκε από: http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf	
Εικόνα 2.2:	Η κατανομή των πηγών spam ανάλογα με την περιοχή το 2013	18
	Ανακτήθηκε από: http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf	
Εικόνα 3.1:	Η basic λειτουργία ενός spam filter	20
	Ανακτήθηκε από: http://rickconner.net/spamweb/filtering.html	
Εικόνα 3.2:	Παράδειγμα εισαγωγής διευθύνσεων σε μία blacklist	27
	Ανακτήθηκε από: http://www.rackspace.com/apps/support/portal/1709	
Εικόνα 3.3:	Παράδειγμα συστήματος πρόκλησης-απόκρισης CAPTCHA	31
	Ανακτήθηκε από: https://www.drupal.org/project/captcha	
Εικόνα 4.1:	Παράδειγμα επιλογής επιπέδου φίλτρων στο Outlook.com	59
	Ανακτήθηκε από: http://oregonstate.edu/helpdocs/safety-and-security/computer-viruses-fraud/blocking-e-mail-spam/email-filtering	
Εικόνα 4.2:	Αποτελέσματα έρευνας για την αποτελεσματικότητα στο φιλτράρισμα spam σε γνωστά email services	61
	Ανακτήθηκε από: http://www.cascadeinsights.com/wp-content/uploads/2012/02/Web_Mail_Provider_SPAM_Filtering_Effectiveness_Research.pdf	

Λίστα Πινάκων

Πίνακας 4.1:	Συγκεντρωτικός πίνακας παράθεσης πλεονεκτημάτων και μειονεκτημάτων μεθόδων spam filtering	52
Πίνακας 5.1:	Παραδείγματα νόμων ενάντια στα spam που εφαρμόζονται σήμερα παγκοσμίως	69

Κεφάλαιο 1
Εισαγωγή

Στο κεφάλαιο αυτό δίνεται ο ορισμός του spam, η προέλευσή του, αλλά και τα βασικά είδη στα οποία μπορούμε να κατηγοριοποιήσουμε το spamming. Το κεφάλαιο αυτό θα μας βοηθήσει να κατανοήσουμε βασικές έννοιες γύρω από τα ανεπιθύμητα μηνύματα αλλά και να διακρίνουμε τα είδη του spam ανάλογα τόσο με το περιεχόμενό τους, όσο και με το μέσο με το οποίο αυτά προωθούνται στους τελικούς χρήστες.

1.1 Ο ορισμός του spam

Ως spam ορίζεται η μαζική αποστολή ανεπιθύμητων μηνυμάτων μέσω της χρήσης ηλεκτρονικών συστημάτων, κυρίως για λόγους διαφήμισης και προώθησης προϊόντων. Τα spam κατακλύζουν το Διαδίκτυο στέλνοντας χιλιάδες αντίγραφα του ίδιου μηνύματος σε χρήστες, χωρίς απαραίτητα να έχουν επιλέξει οι ίδιοι να τα παραλάβουν. Ορισμένοι συνηθίζουν να χαρακτηρίζουν τα spam πιο γενικευμένα ως ανεπιθύμητα e-mail, ωστόσο είναι σημαντικό να αναφέρουμε ότι τα spam σχετίζονται με e-mail που στέλνονται σε λίστες ή ομάδες συζητήσεων διαφημίζοντας συνήθως ένα προϊόν και δεν πρόκειται για e-mail που απλά λαμβάνουμε από αποστολείς που δε γνωρίζουμε και εμείς χαρακτηρίζουμε ως «ανεπιθύμητα».

Η λέξη spam χρησιμοποιείται για να χαρακτηρίσει την αυτόκλητη και αζήτητη αποστολή ηλεκτρονικών μηνυμάτων. [1] Χρησιμοποιείται ο όρος "αυτόκλητη" καθώς για την αποστολή της αλληλογραφίας αυτής δεν έχει προηγηθεί η συγκατάβαση του παραλήπτη, αντίθετα για παράδειγμα με τα ηλεκτρονικά ενημερωτικά μηνύματα (e-newsletters). Συνήθως αποστολείς των μηνυμάτων αυτών είναι εταιρίες που αναζητούν ένα φθηνό τρόπο διαφήμισης, ενώ παραλήπτες είναι λογαριασμοί ηλεκτρονικής αλληλογραφίας (e-mail accounts) που έχουν κυκλοφορήσει στο Διαδίκτυο, όπως για παράδειγμα ανοιχτές λίστες αλληλογραφίας, διευθύνσεις καταγεγραμμένες σε διαδικτυακές σελίδες ή ακόμη και απλά συνηθισμένα ονόματα χρήστη που ανήκουν σε γνωστούς παρόχους ηλεκτρονικής αλληλογραφίας (π.χ. mary@hotmail.com).

Το spam συναντάται συχνά και με τους όρους Unsolicited Bulk E-mail (UBE) και Unsolicited Commercial E-mail (UCE), που εμφανίζουν ελάχιστες διαφορές μεταξύ τους αφού έχουν παρόμοιες συνέπειες για τους χρήστες του internet:

Unsolicited Bulk E-mail - UBE ("Αυτόκλητη Μαζική Ηλεκτρονική Αλληλογραφία"): χαρακτηρίζεται από e-mail με πανομοιότυπο περιεχόμενο που αποστέλλονται σε πολλούς παραλήπτες, χωρίς οι ίδιοι να έχουν ζητήσει να τα παραλάβουν. [2] Αυτή η μορφή spam θεωρούνταν η πιο κοινή μορφή κατάχρησης e-mail μέχρι που εμφανίστηκαν τα UCE που περιγράφονται παρακάτω.

Unsolicited Commercial E-mail - UCE ("Αυτόκλητη Εμπορική Ηλεκτρονική Αλληλογραφία"): αποτελεί ουσιαστικά υποσύνολο του UBE. [2] Περιλαμβάνει όλα τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, που διαφημίζουν ένα εμπορικό προϊόν, μία υπηρεσία ή μία εταιρεία. Με την αποστολή UCE, οι αποστολείς συνήθως στοχεύουν στην προσέλκυση καταναλωτών που θα δαπανήσουν χρήματα σε αυτούς. Εκτός του ότι τα UCE θεωρούνται ανεπιθύμητα μηνύματα, στέλνονται σε τεράστιες ποσότητες σε ηλεκτρονικές διευθύνσεις που συλλέγονται από το internet ή σε τυχαίες διευθύνσεις μεγάλων παρόχων ηλεκτρονικού ταχυδρομείου. Μάλιστα πολλές ανεπτυγμένες χώρες έχουν θεσπίσει νόμους που καθιστούν τα UCE e-mail παράνομα. Ο όρος UCE χρησιμοποιείται περισσότερο στις Ηνωμένες Πολιτείες, όπου η Ομοσπονδιακή Επιτροπή Εμπορίου στοχεύει στη ρύθμιση του εμπορίου.

Το spamming είναι ένα παγκόσμιο φαινόμενο που παραμένει οικονομικά βιώσιμο, λόγω του χαμηλού λειτουργικού κόστους που χρειάζεται εκ μέρους των διαφημιστών (κόστος μόνο για τη διαχείριση των λιστών τους), αλλά και του χαμηλού κόστους αποστολής των μηνυμάτων. Έτσι

ολοένα και αυξάνονται τόσο οι spammers [1], όσο και ο όγκος των ανεπιθύμητων μηνυμάτων που είναι πλέον τεράστιος, με εκτιμήσεις μάλιστα που υπολογίζουν τα spam να καταλαμβάνουν ποσοστό μέχρι και 70% των παγκοσμίως διακινούμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Επίσημα το 1998 το λεξικό New Oxford Dictionary of English κατέγραψε τον όρο spam με την έννοια «άσχετα ή αυτόκλητα μηνύματα που στέλνονται μέσω του διαδικτύου σε μεγάλο αριθμό χρηστών». [3]

1.2 Η προέλευση του spamming

Καθημερινά λαμβάνουμε διαφημιστικά e-mail από αποστολείς που μας είναι άγνωστοι και ουδέποτε ζητήσαμε πληροφορίες για τα προϊόντα τους. Η αύξηση των spam κατά την τελευταία δεκαετία έχει κλιμακωθεί, με το ποσοστό των spam πολλές φορές να υπερβαίνει τον αριθμό των νόμιμων e-mail. Από πού προέρχεται όμως το spam και ποια ήταν η πρώτη εφαρμογή του;

1.2.1 Η προέλευση του όρου spam

Ο όρος spam προέρχεται από ένα αμερικανικό γεύμα σε κονσέρβα με βάση το κρέας (Shoulder Pork and hAM) που δημιουργήθηκε από την εταιρεία Hormel το 1937. [4] Παρόλο που κυκλοφόρησε το Β΄ Παγκόσμιο Πόλεμο το spam εδραίωσε τη φήμη του στις Ηνωμένες Πολιτείες και γρήγορα εισήχθη στις αγορές όλου του κόσμου.

Η σύνδεση ωστόσο του spam με τα ανεπιθύμητα μηνύματα βασίζεται σε ένα σκετς της βρετανικής τηλεοπτικής σειράς Monty Python's Flying Circus το 1970, στο οποίο ένα εστιατόριο περιλαμβάνει στο μενού του το spam σε κάθε πιάτο. [4] Η σερβιτόρα επαναλαμβάνει πολλές φορές τη λέξη spam περιγράφοντας τα φαγητά και τότε μία ομάδα Vikings στη γωνία ξεκινάει το τραγούδι "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam". Όπως και το τραγούδι, έτσι και το spam είναι μία ατέλειωτη επανάληψη άχρηστου ουσιαστικά κειμένου που πολλές φορές ίσως προκαλεί ενόχληση.

[1] spammer: αυτός που στέλνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (spam)

1.2.2 Η «ιστορία» του spam

Σύμφωνα με τον Brad Templeton, το πρώτο e-mail spam εστάλη από τον Gary Thuerk το 1978 σε αρκετές εκατοντάδες χρήστες (400 από τους 2600 χρήστες του ARPANET [2]) στις Ηνωμένες Πολιτείες και επρόκειτο για διαφήμιση μιας παρουσίασης της Digital Equipment Corporation. [4] Ωστόσο η πρώτη τεκμηριωμένη περίπτωση είναι στις 31 Μαρτίου 1993, όταν ο Richard Depew προσπαθούσε να δοκιμάσει ένα καινούργιο λογισμικό και κατά λάθος δημοσίευσε περίπου 200 διπλά μηνύματα. Λέγεται ότι ο πρώτος που είδε το μήνυμα αυτό ήταν ο Joel Furr. Όταν ο Depew απολογήθηκε για την αποστολή των μηνυμάτων, αναφέρθηκε σε αυτά με τον όρο spam.

Τον Απρίλιο του 1994 το spamming εφαρμόστηκε για πρώτη φορά ως πρακτική διαφήμισης και επιχειρηματικότητας, όταν δύο δικηγόροι, ο Canter και ο Siegel, προσέλαβαν έναν προγραμματιστή για να δημοσιεύσει το μήνυμα "Green Card Lottery - Final One?" (που παρείχε πληροφορίες για τη συμπλήρωση εντύπων αδειών εργασίας στις ΗΠΑ) σε όσο περισσότερες ομάδες συζήτησης ήταν δυνατόν. Μάλιστα δε δίστασαν να κρύψουν το γεγονός ότι ήταν spammers, αλλά αντιθέτως ήταν περήφανοι γι' αυτό, θεωρώντας το ως μια διαφήμιση που θα μπορούσε να προσεγγίσει πολύ κόσμο.

1.3 Κατηγοριοποίηση Spamming

Όπως προαναφέρθηκε τα μηνύματα spam στοχεύουν κατά κύριο λόγο στη διαφήμιση. Ωστόσο, κατά καιρούς έχει γίνει λόγος για τις κατηγορίες spam και πώς αυτές προκύπτουν ανάλογα με το περιεχόμενο ή το μέσο διάδοσης των μηνυμάτων. Παρακάτω διαχωρίζονται και περιγράφονται οι κατηγορίες αυτές διεξοδικά.

1.3.1 Κατηγορίες βάσει περιεχομένου spam

Οι spammers επεκτείνουν συνεχώς το φάσμα του περιεχομένου των μηνυμάτων τους και αναζητούν συνεχώς τρόπους να προσελκύσουν περισσότερα ανυποψίαστα θύματα, με αποτέλεσμα ο κατάλογος των κατηγοριών spam συνεχώς να αυξάνεται. Συνήθως τα spam προωθούν προϊόντα που δε δύναται να γίνουν γνωστά στο ευρύ κοινό με άλλο μέσο, όπως παράνομο λογισμικό, φάρμακα των οποίων η κυκλοφορία έχει απαγορευτεί, ή ακόμη και παράνομα αποκτηθείσες πληροφορίες από βάσεις δεδομένων.

[2] ARPANET: πρόδρομος του παγκόσμιου διαδικτύου. Αποτέλεσε το πρώτο δίκτυο μεταγωγής πακέτου ανά τον κόσμο.

Ως spam θεωρούνται τα μηνύματα -ανεξαρτήτως περιεχομένου- που διαβιβάζονται σε μεγάλο αριθμό παραληπτών και ορισμένοι ή όλοι οι παραλήπτες δεν έχουν δώσει την άδειά τους για την παραλαβή τους. Το περιεχόμενο ενός e-mail spam μπορεί να είναι μία διαφήμιση, μία απάτη, μία προσφορά, πορνογραφικό υλικό, ή οτιδήποτε άλλο. Παρακάτω αναλύονται ορισμένες από τις κατηγορίες spamming που συναντάμε συχνότερα στη σύγχρονη εποχή.

Commercial Spam

Στις περισσότερες των περιπτώσεων τα μηνύματα spam εξυπηρετούν εμπορικούς σκοπούς διαφήμισης. Πολλές επιχειρήσεις μάλιστα βλέπουν τη διαφήμιση μέσω spam ως ένα εύκολο και γρήγορο μέσο για να προσεγγίσουν δυνητικούς πελάτες και να έρθουν σε επαφή μαζί τους. Τα spam που προορίζονται για διαφήμιση αποτελούν το πιο κοινό είδος spam. [5] Οι εταιρείες που επιλέγουν να διαφημίσουν τα προϊόντα ή τις υπηρεσίες τους με τον τρόπο αυτό, διενεργούν είτε με δικό τους newsletter, είτε προσλαμβάνουν άτομα που εξειδικεύονται στα spam για την προώθησή τους.

Phishing Spam

Το phishing αποτελεί μία προσπάθεια εξαπάτησης του παραλήπτη αποσπώντας του αριθμούς ή κωδικούς πρόσβασης για σύνδεση με την πιστωτική του κάρτα ή άλλα συστήματα πληρωμών. [5] Η επιστολή αυτή, συνήθως συγκαλύπτεται ως επίσημη ανακοίνωση της διοίκησης της τράπεζας. Αναφέρεται ότι ο δικαιούχος πρέπει να επιβεβαιώσει κάποια λεπτομέρεια για την ταυτότητά του, αλλιώς ο λογαριασμός του θα μπλοκαριστεί και στη συνέχεια τον παραπέμπει στη διεύθυνση spam με τα πεδία που πρέπει να συμπληρώσει. Ανάμεσα στα πεδία αυτά βρίσκονται και τα στοιχεία τα οποία οι δράστες προσπαθούν να αποσπάσουν. Για να εξασφαλιστεί ότι το θύμα δε θα συσχετίσει το μήνυμα αυτό με απάτη, τις περισσότερες φορές ο σχεδιασμός της ιστοσελίδας προσομοιώνει το σχεδιασμό της επίσημης ιστοσελίδας της τράπεζας.

Scam

Τα scam μηνύματα στοχεύουν στην εξαπάτηση ενός ατόμου ή μίας ομάδας ατόμων, αφού πρώτα κερδίσουν την εμπιστοσύνη των παραληπτών. Μέσω της συγκεκριμένης κατηγορίας spam, παρουσιάζονται ψευδείς πληροφορίες στους αποδέκτες της επιστολής, οι οποίες στοχεύουν στην απόσπαση κάποιου χρηματικού ποσού. [5]

Λόγω του ότι ένας μεγάλος αριθμός τέτοιων επιστολών αρχικά προήλθε από τη Νιγηρία, η πιο κοινή μέθοδος ονομάζεται Nigerian Letter (νιγηριανή επιστολή). Η νιγηριανή επιστολή περιέχει ένα μήνυμα σύμφωνα με το οποίο ο παραλήπτης ενημερώνεται ότι μπορεί να κερδίσει ένα μεγάλο χρηματικό ποσό με τη βοήθεια του αποστολέα. Αφού ο αποστολέας κερδίσει την εμπιστοσύνη του παραλήπτη, του ζητά τη μεταφορά κάποιου χρηματικού ποσού με κάποιο πρόσχημα (για παράδειγμα το άνοιγμα λογαριασμού). Η απόσπαση του ποσού αυτού, αποτελεί και το αντικείμενο της απάτης αυτής.

Σε αυτή την κατηγορία εντάσσεται επίσης, η απάτη με τις λαχειοφόρους αγορές. Σε αυτή την περίπτωση, ο παραλήπτης λαμβάνει ένα μήνυμα μέσω τηλεφώνου ή e-mail ότι έχει κερδίσει το λαχείο και ενημερώνεται ότι προκειμένου να λάβει το χρηματικό έπαθλο πρέπει να υποβάλλει ένα μικρό διαδικαστικό ποσό. Μετά την κατάθεση των χρημάτων, ο αποστολέας εξαφανίζεται με τα χρήματα του παραλήπτη.

Adult Content Spam

Αυτή η κατηγορία spam περιλαμβάνει στοιχεία πορνογραφικού χαρακτήρα, όπως απροκάλυπτες εικόνες και λεκτικές περιγραφές, προσφορές για προϊόντα που έχουν σχεδιαστεί για να αυξάνουν ή να ενισχύσουν τη σεξουαλική ικανότητα, συνδέσμους σε ιστοσελίδες πορνό ή διαφημίσεις για πορνογραφία κλπ. [52] Κατά τη διάρκεια των τελευταίων χρόνων η επικράτηση της κατηγορίας αυτής έχει υποχωρήσει και έχει αντικατασταθεί από άλλες αποστολές. Πιο συγκεκριμένα, η ποσότητα αυτού του τύπου αλληλογραφίας στις δυτικές χώρες φαίνεται διαρκώς να μειώνεται, ενώ αντιθέτως σε χώρες όπως η Ρωσία συνεχώς αυξάνεται, με ολοένα και περισσότερα spam να στέλνονται στη ρωσική γλώσσα και να παραπέμπουν σε υπηρεσίες γνωριμιών και διαφημίσεις για πορνογραφικές ιστοσελίδες.

Noncommercial Spam Forms

Τόσο το e-mail όσο και οι άλλες μορφές spamming, έχουν χρησιμοποιηθεί κατά καιρούς και για άλλους σκοπούς εκτός από τη διαφήμιση. Τα μηνύματα που προωθούνται πέρα από εμπορικά, μπορούν ακόμη να είναι πολιτιστικά, φιλανθρωπικά, θρησκευτικά ή πολιτικά εξυπηρετώντας ποικίλους μη εμπορικούς σκοπούς και συμφέροντα. Για παράδειγμα υπάρχουν περιπτώσεις προώθησης κάποιας πολιτικής ή θρησκευτικής πεποίθησης ή ακόμα πιο ακραία περιπτώσεις κατά τις οποίες εγκληματίες καταφέρνουν να εξαπατήσουν ανθρώπους, να τους απαγάγουν ή ακόμα και να τους σκοτώσουν.

Επιπλέον, οι spammers φαίνεται να προωθούν συγκεκριμένα αγαθά και υπηρεσίες που πολλές φορές προέρχονται από τη μαύρη αγορά. Έτσι, τα spam μπορούν να θεωρηθούν παράνομα, όχι μόνο λόγω των μέσων που χρησιμοποιούν για να διαφημίσουν αγαθά, αλλά και επειδή τα ίδια αγαθά και οι υπηρεσίες που προσφέρονται είναι παράνομα.

1.3.2 Κατηγορίες βάσει μέσου διάδοσης spam

Παρά το γεγονός ότι η πιο ευρέως διαδεδομένη μορφή διάδοσης του κακόβουλου αυτού λογισμικού είναι το e-mail, υπάρχουν και άλλες κατηγορίες spam, που παίρνουν το όνομά τους ανάλογα με το κανάλι μέσω του οποίου διανέμονται, όπως για παράδειγμα instant messaging spam, mobile phone spam, social networking spam, blog spam, wiki spam, Internet forum spam, spam σε μηχανές αναζήτησης και πολλά ακόμα είδη. Παρακάτω παρουσιάζονται αναλυτικά οι πιο διαδεδομένοι τύποι ανεπιθύμητων μηνυμάτων βασισμένοι στα μέσα διάδοσής τους.

E-mail spamming

Τα spam e-mail, που είναι επίσης γνωστά ως junk e-mail (ανεπιθύμητη αλληλογραφία), unsolicited bulk e-mail (UBE) ή unsolicited commercial e-mail (UCE), είναι ένα υποσύνολο της κατηγορίας ηλεκτρονικών spam που αφορούν σχεδόν πανομοιότυπα μηνύματα που αποστέλλονται σε πολλαπλούς παραλήπτες μέσω e-mail. [2] Κάνοντας κλικ σε συνδέσμους των spam e-mail ο χρήστης παραπέμπεται συνήθως σε ιστοσελίδες phishing [3], ιστοσελίδες με κακόβουλο λογισμικό ή ακόμη και πέφτει θύμα scripts [4] και άλλων εκτελέσιμων συνημμένων αρχείων που προκαλούν ιούς. Το spam άρχισε να αποτελεί πρόβλημα όταν το Διαδίκτυο άνοιξε για το ευρύ κοινό στα μέσα της δεκαετίας του 1990.

Εξ ορισμού, e-mail spam θεωρείται οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου πληροί τα ακόλουθα κριτήρια:

- Ανωνυμία: η διεύθυνση και η ταυτότητα του αποστολέα κρύβονται

[3] phishing: ενέργεια εξαπάτησης με σκοπό την απόκτηση προσωπικών δεδομένων (συνήθως οικονομικών), όπως ιδιωτικά στοιχεία τραπεζικών λογαριασμών, πιστωτικών καρτών, κωδικούς κ.α. Συνήθως οι θύτες χρησιμοποιούν ένα αξιόπιστο όνομα για να προσελκύσουν τα ανυποψίαστα θύματά τους. Περιγράφεται αναλυτικά στην ενότητα 1.3.1

[4] script: πρόγραμμα γραμμένο σε ειδικό περιβάλλον που εκτελεί αυτόματα καθήκοντα που θα μπορούσαν εναλλακτικά να εκτελεστούν ένα προς ένα από έναν χειριστή. Ένα μεγάλο ποσοστό ιών βασίζεται σε scripts που ενσωματώνουν οι spammers στα μηνύματά τους

- Μαζική αποστολή αλληλογραφίας: Τα e-mail αποστέλλονται ως μέρος μίας ευρύτερης συλλογής μηνυμάτων σε μεγάλες ομάδες χρηστών και τυπικά (όχι πάντα) περιέχουν κακόβουλο περιεχόμενο

- Μη ζητηθέντα μηνύματα (unsolicited): Αν και ο χρήστης δεν έχει ζητήσει το συγκεκριμένο e-mail, τελικά το παραλαμβάνει

Το e-mail spamming στοχεύει σε μεμονωμένους χρήστες με άμεσα ηλεκτρονικά μηνύματα. [6] Οι λίστες e-mail spam δημιουργούνται τις περισσότερες φορές από τη σάρωση Usenet [5] δημοσιεύσεων, κλέβοντας λίστες με e-mail, ή από την αναζήτηση στο Διαδίκτυο για διευθύνσεις. Οι spammers επίσης συλλέγουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από chatrooms, ιστοσελίδες, καταλόγους πελατών, newsgroups και ιούς που βλέπουν τις λίστες διευθύνσεων των χρηστών, οι οποίες μάλιστα μεταπωλούνται σε άλλους spammers. [2] Χρησιμοποιούν επίσης μια πρακτική που είναι γνωστή ως "e-mail appending» ή «epending» κατά την οποία χρησιμοποιούν γνωστές πληροφορίες σχετικά με το στόχο τους (όπως για παράδειγμα την ταχυδρομική του διεύθυνση) για να αναζητήσουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου του. Μεγάλο μέρος των spam μηνυμάτων αποστέλλονται σε διευθύνσεις που δεν υφίστανται. Μάλιστα σύμφωνα με έρευνα του Message Anti-Abuse Working Group, το πρώτο εξάμηνο του 2010 το ποσοστό των spam e-mail ήταν μεταξύ 88-92% των συνολικά απεσταλμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Instant Messaging Spam

Συχνά το συναντάμε και με τον όρο spim, που προέρχεται από τα spam που στέλνονται διαμέσου IM [6], αντί μέσω ηλεκτρονικού ταχυδρομείου. Τα συστήματα ανταλλαγής άμεσων μηνυμάτων (instant messaging systems), όπως το Windows Live Messenger, το Yahoo, το Messenger, το AIM, το Skype, το ICQ, το XMPP και το Myspace chat rooms, αποτελούν όλα στόχο για τους spammers. [3] Πολλά από αυτά τα συστήματα προσφέρουν έναν κατάλογο των χρηστών, που περιλαμβάνει δημογραφικά στοιχεία όπως την ηλικία και το φύλο τους. Οι διαφημιστές – spammers μπορούν να συγκεντρώσουν τις πληροφορίες αυτές, αφού συνδεθούν στο σύστημα και να στείλουν

[5] Usenet: ένα από τα παλαιότερα συστήματα επικοινωνίας δικτύων υπολογιστών, που συναντάται ακόμα και σήμερα σε ευρεία χρήση.
[6] IM: ακρωνύμιο για το instant message, δηλαδή άμεσο μήνυμα. Αποτελεί είδος online chat που προσφέρει μετάδοση κειμένου σε πραγματικό χρόνο μέσω internet.

ανεπιθύμητα μηνύματα, τα οποία ίσως περιλαμβάνουν εμπορικές απάτες, ιούς και συνδέσμους σε κακόβουλες σελίδες. Μάλιστα η Microsoft ανακοίνωσε ότι το επερχόμενο Windows Live Messenger 9.0 θα υποστηρίζει εξειδικευμένες δυνατότητες για την καταπολέμηση μηνυμάτων spam. Στα περισσότερα συστήματα οι χρήστες μπορούν να μπλοκάρουν τη συντριπτική πλειοψηφία των spam μέσω της χρήσης ενός whitelist[7]. Έχει διαπιστωθεί ότι μέσω της αμεσότητας που προσφέρει το IM, οι χρήστες είναι πιο ευπαθείς και κάνουν κλικ σε συνδέσμους αντανακλαστικά. Εκτός αυτού, επειδή παρακάμπτει το λογισμικό antivirus και τα firewalls, αποτελεί εύκολο μέσο διάδοσης όχι μόνο εμπορικών μηνυμάτων, αλλά και ιών και κακόβουλων προγραμμάτων.

Mobile Phone Spam

Το συναντάμε αλλιώς με τους όρους spamming, SMS spam, text spam, m-spam, mspam. Το mobile phone spam είναι μία μορφή spam που απευθύνεται στην ανταλλαγή μηνυμάτων κειμένου ή άλλων υπηρεσιών επικοινωνίας μέσω κινητών τηλεφώνων. [3] Τα μηνύματα αυτά μπορεί να αφορούν διαφημίσεις ή μπορεί ακόμη και να επιδιώκουν να εξαπατήσουν τον παραλήπτη. Δεδομένου ότι η δημοτικότητα των κινητών τηλεφώνων αυξήθηκε ήδη από τις αρχές της δεκαετίας του 2000, οι συχνοί χρήστες των text messages (μηνυμάτων κειμένου) άρχισαν να βλέπουν μια αύξηση του αριθμού των αυτόκλητων (και γενικά ανεπιθύμητων) εμπορικών διαφημίσεων που αποστέλλονταν στα τηλέφωνα τους μέσω sms. Σήμερα, οι περισσότεροι άνθρωποι που κατέχουν ένα κινητό τηλέφωνο είναι ήδη αρκετά εξοικειωμένοι με τα μηνύματα αυτού του είδους. Τα mobile spam messages μπορεί να είναι ιδιαίτερα ενοχλητικά για τους παραλήπτες, αφού σε αντίθεση με το ηλεκτρονικό ταχυδρομείο, ορισμένοι παραλήπτες μπορεί να χρεώνονται για κάθε μήνυμα που λαμβάνουν.

Το mobile spam είναι γενικά λιγότερο διαδεδομένο από το e-mail spam και ο αριθμός των spam συνήθως διαφέρει ανάλογα με την περιοχή. [7] Για παράδειγμα στην Ασία το 2012 , περίπου το 30% των μηνυμάτων κειμένου ήταν spam. Για τη συμμόρφωση με τους κανονισμούς CAN-SPAM, τα μηνύματα sms πρέπει πλέον να παρέχουν τις επιλογές HELP και STOP (τερματισμός παραλαβής μηνυμάτων από τον συγκεκριμένο αριθμό).

[7] whitelist: Πρόκειται για έναν κατάλογο με ηλεκτρονικές διευθύνσεις από τις οποίες ορίζουμε ότι επιθυμούμε να λαμβάνουμε μηνύματα. Όσοι βρίσκονται στη λίστα γίνονται αποδεκτοί. Οι whitelists είναι το αντίθετο των blacklists, που περιέχουν διευθύνσεις αυτών των οποίων τα μηνύματα θέλουμε να απορρίψουμε.

Social Networking Spam

Το social spam αποτελεί ανεπιθύμητο περιεχόμενο που εμφανίζεται στις υπηρεσίες κοινωνικής δικτύωσης (social networks[8]) και σε οποιαδήποτε ιστοσελίδα περιέχει περιεχόμενο που εισάγεται από τους χρήστες (σχόλια, συνομιλίες κ.α.). Ακόμη και ορισμένα από τα δημοφιλέστερα social media, όπως το Facebook και το Twitter έχουν πέσει θύματα των spam. [3] Οι ειδικοί μάλιστα εκτιμούν ότι περίπου το 40% των λογαριασμών που δημιουργούνται στα social media χρησιμοποιούνται για την αποστολή spam. Για παράδειγμα στο Twitter οι spammers κερδίζουν την αξιοπιστία των χρηστών κάνοντας follow έγκυρους λογαριασμούς διάσημων, που όταν κάνουν με τη σειρά τους follow τον spammer, τον νομιμοποιούν έμμεσα και του επιτρέπουν να πολλαπλασιάζεται. Οι spammers χακάρουν λογαριασμούς χρηστών και στέλνουν συνδέσμους spam σε επαφές του χρήστη, όπως στους φίλους και την οικογένειά του. Το social spamming εκδηλώνεται με πολλούς τρόπους, όπως χυδαία μηνύματα, βωμολοχίες, κακόβουλες συνδέσεις, δόλια σχόλια κ.α. Για την προστασία των χρηστών πολλά κοινωνικά δίκτυα έχουν συμπεριλάβει το πλήκτρο «αναφορά spam» ή δίνουν στον χρήστη τη δυνατότητα να αναφέρει τη διεύθυνση αυτού που νομίζουν ότι δημοσιεύει spam.

Blog, wiki Spam

Το blog spamming αποτελεί μια μορφή spamdexing[9]. [3] Αυτό γίνεται με την ταχυδρόμηση (συνήθως αυτοματοποιημένη) τυχαίων παρατηρήσεων, με την αντιγραφή υλικού που δεν είναι πρωτότυπο από άλλες διευθύνσεις, ή με την προώθηση εμπορικών υπηρεσιών σε blogs, wikis, βιβλία επισκεπτών, ή άλλων δημόσια προσβάσιμων πινάκων συζητήσεων. Κάθε διαδικτυακή εφαρμογή που δέχεται και εμφανίζει υπερσυνδέσεις (hyperlinks) που κοινοποιούν οι επισκέπτες μπορεί να είναι στόχος για αυτό το είδος spamming. Ο σκοπός του blog spam είναι συνήθως να αυξηθεί το PageRank[10], αφού η προσθήκη συνδέσμων που οδηγούν στη σελίδα του αποστολέα αυξάνουν τεχνητά την ταξινόμηση της συγκεκριμένης σελίδας στις μηχανές αναζήτησης. Τα blogs αυτά συνήθως περιέχουν ένα μεγάλο αριθμό συνδέσεων σε ιστοσελίδες που σχετίζονται με τους δημιουργούς των spam και οδηγούν σε κακόφημες ή άχρηστες ιστοσελίδες. Η αυξημένη

[8] social network: δίκτυα που βασίζονται σε μία δομή που επιτρέπει στους ανθρώπους να εκφράζουν την προσωπικότητά τους και να συναντούν ανθρώπους με παρόμοια ενδιαφέροντα με αυτούς. Η δομή αυτή συνήθως περιλαμβάνει τη δημιουργία προφίλ, την δυνατότητα απόκτησης φίλων, τα widgets κ.α. Ορισμένα από τα πιο γνωστά τέτοια δίκτυα είναι το Facebook, το Pinterest, το Google+, το LinkedIn και το Twitter.
[9] spamdexing: χαρακτηρίζεται από την οποιαδήποτε σκόπιμη χειραγώγηση των ευρετηρίων των μηχανών αναζήτησης.
[10] PageRank: αλγόριθμος που χρησιμοποιείται από το Google Search για την ταξινόμηση των ιστοτόπων στους καταλόγους αποτελεσμάτων των μηχανών αναζήτησης. Αποτελεί ουσιαστικά έναν τρόπο μέτρησης της σημαντικότητας των ιστοσελίδων

κατάταξη έχει σαν αποτέλεσμα το εμπορικό site του spammer να κατατάσσεται υψηλότερα στη λίστα έναντι άλλων σε συγκεκριμένες αναζητήσεις, αυξάνοντας έτσι τον αριθμό των δυνητικών επισκεπτών και των πελατών που θα κάνουν αγορές.

Forum Spam

Τα forum spam αποτελούν δημοσιεύσεις σε forum του Διαδικτύου που μπορεί να περιέχουν διαφημίσεις, συνδέσμους που παραπέμπουν σε κακόβουλες ιστοσελίδες και καταχρηστικές ή ανεπιθύμητες πληροφορίες. [8] Τα spam αυτά, είναι συνήθως αναρτημένα σε πίνακες μηνυμάτων από αυτοματοποιημένα συστήματα ή χειροκίνητα από ασυνείδητους, που θέλουν να προβάλλουν το spam σε τέτοιο σημείο που ένας χρήστης διαφορετικά δε θα το πρόσεχε. Τα forum spambots [11] σερφάρουν στο Διαδίκτυο και ψάχνουν για wikis, blogs, forums και άλλες μορφές web για να υποβάλουν τα spam links τους εκεί. Μερικά από αυτά τα spam μηνύματα μπορεί να εξυπηρετούν σκοπούς marketing ή ακόμη και phishing, ενώ τις περισσότερες φορές τα αυτοματοποιημένα αυτά μηνύματα μπορεί να είναι τόσο καλά σχεδιασμένα ώστε να μην είναι αναγνωρίσιμο αν αποτελούν πραγματικές διαφημίσεις ή spam.

Τα περισσότερα forum spam αποτελούνται από συνδέσμους προς εξωτερικούς δικτυακούς τόπους με στόχο τόσο να αυξήσουν την προβολή συγκεκριμένων domains με διαφημίσεις, όπως προϊόντα απώλειας βάρους, φαρμακευτικά προϊόντα, τυχερά παιχνίδια, πορνογραφία, αγορά ακινήτων ή δάνεια, όσο και για να παράγουν περισσότερη κίνηση σε αυτές τις εμπορικές ιστοσελίδες. Μερικές από αυτές τις συνδέσεις ενδέχεται να περιέχουν κώδικα για να παρακολουθούν και την ταυτότητα του spambot, έτσι ώστε αν μια πώληση περνά ένα συγκεκριμένο όριο, τότε ο spammer πίσω από το spambot να μπορεί να συλλέγει μια προμήθεια.

Η πρόληψη από τα spam και η διαγραφή τους σίγουρα αυξάνει το φόρτο εργασίας για τους διαχειριστές των forum και για τους συντονιστές. Το ποσό του χρόνου και των πόρων που δαπανώνται για να κρατηθεί ένα forum ελεύθερο από τα spam, συμβάλλει σημαντικά στο συνολικό κόστος εργασίας και την όλη λειτουργία ενός δημόσιου forum. Μάλιστα κάποια οριακά κερδοφόρα ή μικρότερα forum μπορεί να κλείσουν και οριστικά από τους διαχειριστές τους, όταν δεν μπορούν να ανταποκριθούν στις απαιτήσεις αυτές.

[11] spambot: αυτοματοποιημένο πρόγραμμα υπολογιστή σχεδιασμένο για να βοηθάει στην αποστολή spam

Spamdexing

Στην επιστήμη των υπολογιστών, το spamdexing (αλλιώς γνωστό ως search engine spam, search engine poisoning, Black-Hat SEO, search spam ή web spam) είναι η σκόπιμη χειραγώγηση των ευρετηρίων των μηχανών αναζήτησης. [9] Περιλαμβάνει μια σειρά από μεθόδους, όπως η επανάληψη άσχετων φράσεων, προκειμένου να χειραγωγηθεί η σημασία και η προβολή ενός συστήματος κατά τρόπο που δε συνάδει με το σκοπό του συστήματος ευρετηρίασης.

Οι μηχανές αναζήτησης χρησιμοποιούν μια ποικιλία αλγορίθμων για να βελτιώσουν το ranking τους. Ορισμένες από αυτές περιλαμβάνουν τον προσδιορισμό, αν ο όρος που αναζητά ο χρήστης εμφανίζεται στο σώμα του κειμένου ή τη διεύθυνση URL μιας ιστοσελίδας. Οι spammers ωστόσο, χρησιμοποιούν ανήθικες μεθόδους για να κάνουν τις ιστοσελίδες τους να κατατάσσονται σε υψηλότερη θέση στα αποτελέσματα των μηχανών αναζήτησης, από ότι θα ήταν διαφορετικά με βάση τη βιομηχανία του SEO (Search Engine Optimization). Πολλές μηχανές αναζήτησης ελέγχουν για περιπτώσεις spamdexing και αφαιρούν τις ύποπτες σελίδες από τα αποτελέσματά τους. Επίσης, οι άνθρωποι που εργάζονται για οργανώσεις search engine μπορούν να εμποδίσουν γρήγορα την εμφάνιση αποτελεσμάτων ακόμη και από ολόκληρες ιστοσελίδες που χρησιμοποιούν spamdexing, αν ειδοποιηθούν από καταγγελίες χρηστών. Η άνοδος του Spamdexing στα μέσα της δεκαετίας του 1990, έκανε τις τότε κορυφαίες μηχανές αναζήτησης να είναι λιγότερο χρήσιμες για τους χρήστες.

Κεφάλαιο 2
Το spam ως πρόβλημα

Αρχικά τα spam δε δημιουργήθηκαν με σκοπό να ενοχλήσουν ή να εξαπατήσουν τους τελικούς χρήστες, αλλά χρησιμοποιούνταν ως ένα μέσο γρήγορης μετάδοσης μηνυμάτων σε πολλούς αποδέκτες. Ωστόσο, ήδη από το τα τέλη δεκαετίας του '90 λόγω της αύξησης της δημοτικότητας του ηλεκτρονικού ταχυδρομείου, το spam άρχισε να αποτελεί πρόβλημα. Στη σημερινή εποχή με τις φθηνές και υψηλών ταχυτήτων συνδέσεις στο internet, πολλοί spammers χρησιμοποιούν τα spam τόσο για διαφημιστικούς σκοπούς, όσο και για να διανείμουν κακόβουλο περιεχόμενο. Οι χρήστες εκείνοι που δεν είναι εξοικειωμένοι με τα spam e-mails, δυσκολεύονται να φιλτράρουν μεταξύ των μηνυμάτων τους τα έγκυρα νόμιμα μηνύματα, έναντι των spam. Τα spam μηνύματα εκτός από ενοχλητικά μπορεί πολλές φορές να είναι και επικίνδυνα για τους χρήστες, αφού είναι πιθανό να περιέχουν μολυσμένα αρχεία (viruses) ή συνδέσμους σε ιστοσελίδες με κακόβουλο λογισμικό. Στο κεφάλαιο αυτό αναλύονται οι λόγοι που καθιστούν το spam πρόβλημα, αλλά και η έκταση που έχει λάβει το πρόβλημα spamming παγκοσμίως.

2.1 Γιατί το spam αποτελεί πρόβλημα

Το φαινόμενο spam δημιουργεί προκλήσεις τόσο για τους χρήστες του Internet, όσο και για τους ρυθμιστικούς οργανισμούς που προσπαθούν να ελέγξουν το πρόβλημα. Παρακάτω, εκτίθενται

ορισμένοι από τους βασικότερους λόγους για τους οποίους το spam θεωρείται πρόβλημα στις μέρες μας.

Παραβίαση Ιδιωτικής Ζωής: Γύρω από τα spam τίθενται σημαντικά ζητήματα προστασίας της ιδιωτικής ζωής όσον αφορά τον τρόπο με τον οποίο οι διευθύνσεις ηλεκτρονικού ταχυδρομείου και τα προσωπικά δεδομένα συλλέγονται και χρησιμοποιούνται. [53] Δεν είναι ασυνήθιστο για τους spammers να μαζεύουν συγκεκαλυμμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου χρηστών Internet, και στη συνέχεια να τις αγοράζουν ή να τις πωλούν μαζικά, χωρίς την έγκρισή των χρηστών.

Ζημία στην αγορά: Για τις περισσότερες μορφές διαφήμισης, το κόστος αποστολής κάθε μηνύματος παίζει πρωταγωνιστικό ρόλο, ειδικά όταν συγκρίνεται με το κόστος του αντικειμένου που πωλείται και το μέγεθος της αγοράς. Το χαμηλό κόστος των spam μηνυμάτων ενθαρρύνει τους spammers να στέλνουν καθημερινά τεράστιο αριθμό μηνυμάτων. Οι επιχειρήσεις που διαφημίζουν χρησιμοποιώντας τα παραδοσιακά μέσα ενημέρωσης συνήθως κάνουν κάποια προσπάθεια για να αποστείλουν τα μηνύματά τους σε στοχευμένους πελάτες, που έχουν περισσότερες πιθανότητες να αγοράσουν το προϊόν, έτσι ώστε να ελαχιστοποιήσουν τα έξοδα. Για παράδειγμα, δεν υπάρχει κανένας λόγος να δαπανήσουν χρήματα για να στείλουν μια διαφήμιση τροφής σκύλων σε ιδιοκτήτες γατών. Ωστόσο, οι spammers δεν έχουν κανένα κίνητρο να στείλουν μηνύματα σε στοχευμένους πελάτες, αφού το κόστος για την αποστολή ηλεκτρονικών μηνυμάτων είναι πολύ χαμηλό. Αυτό το εξαιρετικά χαμηλό κόστος της αποστολής spam, είναι ο μεγαλύτερος μεμονωμένος παράγοντας που οδηγεί στην συνεχή ανάπτυξη του φαινομένου. Σύμφωνα με τις εκτιμήσεις του Alexander Ivanov, Πρόεδρο της Ρωσικής Ένωσης δικτύων και υπηρεσιών, πριν από τρία χρόνια οι επιχειρήσεις του Διαδικτύου έχασαν $ 55 εκατομμύρια από τις ζημίες που προκλήθηκαν από το spam. [10] Το ποσό αυτό αντιπροσωπεύει μόνο τα έξοδα κίνησης. Επιπλέον, υπάρχουν διακομιστές ηλεκτρονικού ταχυδρομείου που λαμβάνουν και επεξεργάζονται τα spam και αυτοί οι διακομιστές πρέπει να συντηρούνται από υψηλόμισθους ειδικούς. Ως εκ τούτου, υπάρχουν επίσης σημαντικά λειτουργικά κόστη.

Υπερφόρτωση Επικοινωνιακών μέσων: Τα spam καταλαμβάνουν ένα τεράστιο εύρος ζώνης δικτύου παγκοσμίως δεσμεύοντας, αποθηκευτικούς και υπολογιστικούς πόρους τόσο στα e-mail servers (εξυπηρετητές ηλεκτρονικού ταχυδρομείου), όσο και στα αντίστοιχα συστήματα των χρηστών. Εκτός αυτού, μπλοκάρουν τους διαύλους επικοινωνίας και αυξάνουν την κυκλοφορία, γεγονός το οποίο δημιουργεί κόστος για τον πάροχο, το χρήστη ή τον εργοδότη σε περίπτωση εταιρείας.

Απειλή: Το περιεχόμενο των μηνυμάτων spam πολλές φορές κρύβει καλά οργανωμένες απάτες. Οι νέες τεχνολογίες επιτρέπουν στους spammers να στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου, που περιέχουν αναληθές περιεχόμενο, πλαστές διευθύνσεις αποστολέα και μολυσμένους μηχανισμούς. Όπως είναι αναμενόμενο, η χρήση του spam που στόχευε στην παραπλάνηση των χρηστών, καθώς και η ικανότητα να κρυφτεί κάποιος πίσω από μία τέτοια δραστηριότητα, προσέλκυσε και προσελκύει καθημερινά εγκληματίες και απατεώνες του κυβερνοχώρου όλων των τύπων. Η ανωνυμία των spam, δηλαδή η αδυναμία να εντοπίσει κανείς εύκολα το από που ξεκινά η μαζική αλληλογραφία, σημαίνει ότι οι εγκληματίες μπορούν να δρουν με ατιμωρησία, συμβάλλοντας περαιτέρω στην ποινικοποίηση των spam.

Ακατάλληλο Περιεχόμενο: Υπάρχουν προφανείς ανησυχίες από τους ρυθμιστικούς και κοινοτικούς οργανισμούς σχετικά με το παράνομο περιεχόμενο που προωθείται μέσω των spam παγκοσμίως, όπως η πορνογραφία, οι παράνομες online υπηρεσίες τυχερών παιχνιδιών, τα γρήγορα συστήματα πλουτισμού και οι παραπλανητικές επιχειρηματικές πρακτικές. [11] Η αδιάκριτη μέθοδος διανομής των μηνυμάτων είναι αυτή που προκαλεί τη μεγαλύτερη ανησυχία, δεδομένου ότι θεωρείται κοινό για τους ανηλίκους να λαμβάνουν spam με προσβλητικό, πορνογραφικό ή παράνομο περιεχόμενο.

Μετάδοση επικίνδυνων Ιών: Τα spam αποτελούν πρωταρχικό μέσο για τη μεταφορά ηλεκτρονικών ιών και malware λοιμώξεων, είτε σκόπιμα, είτε ως το άμεσο αποτέλεσμα της δημιουργίας μαζικών e-mail από και προς ένα μεγάλο αριθμό παραληπτών. Το λογισμικό malware είναι σχεδιασμένο για να διεισδύει και να βλάπτει το σύστημα του υπολογιστή των χρηστών. Συχνά αποστέλλεται ως ανυποψίαστο συνημμένο αρχείο στα e-mail των χρηστών, το οποίο όταν ανοιχτεί, εγκαθίσταται στο σύστημα.

Μείωση δεικτών παραγωγικότητας: Η αυξανόμενη ποσότητα spam έχει όλο και μεγαλύτερο αντίκτυπο στον τελικό χρήστη, αφού εκείνος καταναλώνει εύκολα πολύτιμο χρόνο του, αν δεν υπάρξει η σωστή διαχείρισή των μηνυμάτων spam από μέρους του. [12] Ως αποτέλεσμα, πολλές οργανώσεις αλλά και άτομα μεμονωμένα, έχουν προσπαθήσει να βρουν τεχνικές για την καλύτερη αντιμετώπισή των μηνυμάτων spam. Η διαφάνεια του Διαδικτύου είναι ένας βασικός παράγοντας που επιτρέπει στα spam να πολλαπλασιάζονται. Αυτή η έμφυτη ελευθερία επιτρέπει στους spammers να δημοσιεύουν διαφημιστικά σχόλια σχεδόν οπουδήποτε χωρίς κανένα ενδοιασμό. Τόσο οι ιδιωτικοί χρήστες, όσο και οι διαχειριστές σε συστήματα επιχειρήσεων, αναγκάζονται να διαγράφουν άπειρα μεμονωμένα ανεπιθύμητα μηνύματα, δαπανώντας καθημερινά πολύτιμο χρόνο. Αυτή η χαμένη προσπάθεια και ο χρόνος, οδηγούν

αναπόφευκτα σε έλλειψη παραγωγικότητας, καθώς οι πόροι διατίθενται αναποτελεσματικά σε μη κερδοφόρες διαδικασίες. Σε έρευνα που διεξήχθη σε 76 διαφορετικές αμερικάνικες εταιρείες για να αποδοθεί η ζημία που προκαλούν τα spam, βρέθηκε ότι ο μέσος εργαζόμενος παραλαμβάνει 13,3 spam μηνύματα τη μέρα, ενώ ο χρόνος που δαπανάται για τη διαχείρισή τους κυμαίνονταν από 1 μέχρι 90 λεπτά, με μέσο όρο τα 6,5 λεπτά τη μέρα.

Ενόχληση - Δυσαρέσκεια Χρηστών: Ίσως το σημαντικότερο πρόβλημα σε σχέση με τα spam να είναι ο παράγοντας της ενόχλησης. Τα ανεπιθύμητα μηνύματα κατακλύζουν τους λογαριασμούς e-mail ιδιωτικών χρηστών με διαφημίσεις προϊόντων που δε χρειάζονται, απάτες στις οποίες μπορεί να πέσουν θύματα, ή ακόμη και ακατάλληλο περιεχόμενο. Για κάποιο χρήστη η διαδικασία του να διαγράψει από την κατοχή του τα spam e-mail χειροκίνητα, πολλές φορές τον ενοχλεί και του δημιουργεί ανεπιθύμητα αρνητικά συναισθήματα. [10]

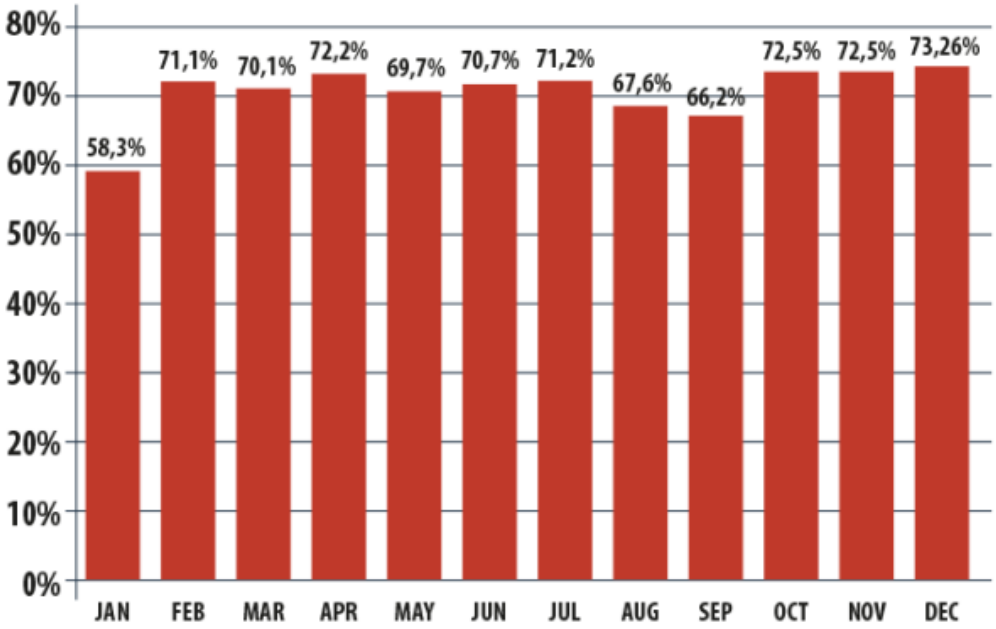
Εκτός όλων των παραπάνω υπάρχουν φυσικά και άλλες αρνητικές συνέπειες των spam, όπως η μείωση της αποτελεσματικότητας των νόμιμων διαφημίσεων, η αυξημένη πιθανότητα διαγραφής ενός χρήσιμου e-mail μαζί με τα spam, αλλά και η συνολική αύξηση του κόστους χρήσης του internet.

2.2 Η έκταση του προβλήματος σήμερα

Τα αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου αναγνωρίζονται ευρύτερα ως ένα από τα σημαντικότερα θέματα που αντιμετωπίζει σήμερα το Internet. [13] Το φαινόμενο spam έχει λάβει ανησυχητικές διαστάσεις, απειλώντας την ίδια τη χρησιμότητα του ηλεκτρονικού ταχυδρομείου ως μορφή επικοινωνίας.

Ακόμη και αν οι χρήστες λαμβάνουν διαφορετικές ποσότητες spam ανάλογα με τη διαθεσιμότητα των ηλεκτρονικών διευθύνσεών τους, τη χρήση του Διαδικτύου και την ευαισθητοποίηση τους σε θέματα ασφάλειας, υπάρχουν στοιχεία που δείχνουν ότι ο μέσος όρος συχνότητας εμφάνισης μηνυμάτων spam, αυξάνεται παγκοσμίως με ταχείς ρυθμούς. [13] Για να κατανοήσουμε καλύτερα την έκταση του προβλήματος spam στις μέρες μας, παρακάτω παραθέτουμε σχετική έρευνα που διεξήχθη από το Kaspersky Lab (από τις κορυφαίες εταιρείες ασφάλειας του πλανήτη), για τον όγκο των ανεπιθύμητων μηνυμάτων το 2013.

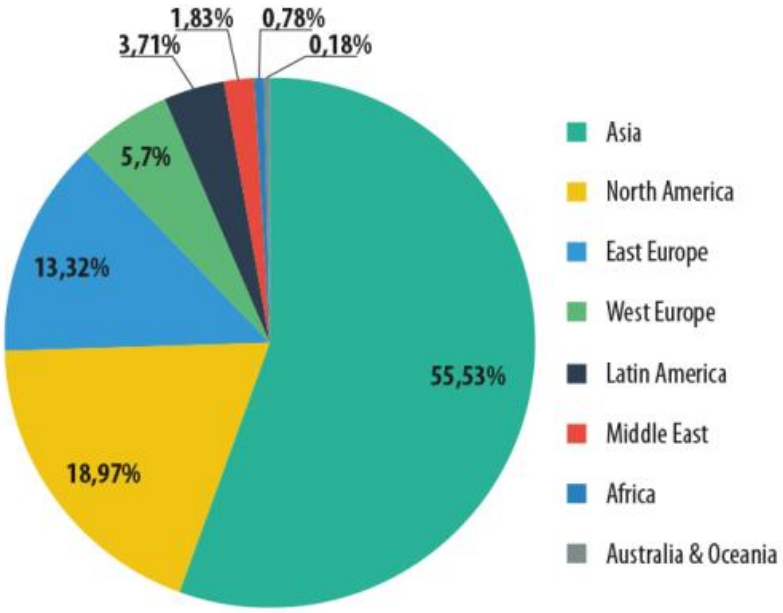
Το ποσοστό των spam έναντι της συνολικής κίνησης e-mail μειώθηκε κατά 2,5 ποσοστιαίες μονάδες σε σύγκριση με το προηγούμενο έτος και διαμορφώθηκε στο ποσοστό 69,6%. [14] Για πρώτη φορά μετά από πολλά χρόνια, το μέσο ετήσιο ποσοστό spam είναι μικρότερο από 70%. Κατά τη διάρκεια του έτους 2013, το ποσοστό των spam παρέμεινε σχετικά σταθερό από μήνα σε μήνα (με εξαίρεση το ασυνήθιστα χαμηλό ποσοστό για το μήνα Ιανουάριο).



Εικόνα 2.1: Το ποσοστό των spam σε σχέση με το συνολικό αριθμό e-mail το 2013.

Οι χώρες που αποτελούν τις κορυφαίες πηγές spam παγκοσμίως παρέμειναν οι ίδιες με την προηγούμενη χρονιά: η Κίνα (+3,5 ποσοστιαίες μονάδες) και οι ΗΠΑ (+2 μονάδες) ήταν η πηγή του 40,6% του συνόλου του παγκόσμιου spam. [14] Οι χώρες αυτές ήρθαν πρώτη και δεύτερη θέση στον πίνακα διανομής spam και ταίριαξαν με τις αντίστοιχες θέσεις τους στις λίστες των χωρών ανάλογα με τον αριθμό χρηστών στο Διαδίκτυο.

Όσον αφορά τα αποτελέσματα για τις κορυφαίες πηγές spam ανά περιοχή, η Ασία (+5,3 ποσοστιαίες μονάδες) και η Βόρεια Αμερική (+3,2 Ποσοστιαίες μονάδες) ήταν και πάλι μπροστά. Η Ανατολική Ευρώπη ανέβηκε στην τρίτη θέση, το μερίδιο της Δυτικής Ευρώπης μειώθηκε κατά 2,4 ποσοστιαίες μονάδες και παρέμεινε στην 4η θέση ενώ η Λατινική Αμερική ήρθε 5η.



Εικόνα 2.2: Η κατανομή των πηγών spam ανάλογα με την περιοχή το 2013.

Το Kaspersky Lab ανακοίνωσε επίσης κάποια στατιστικά στοιχεία για το πρώτο τρίμηνο του 2014 κατά το οποίο το ποσοστό των spam e-mail σε σχέση με το σύνολο των διακινούμενων e-mail ανήλθε σε 66,34% (έπεσε 6,42 ποσοστιαίες μονάδες από το προηγούμενο τρίμηνο). [14] Ωστόσο, σε σύγκριση με την ίδια περίοδο του 2013, το ποσοστό των spam στο τρίμηνο του 2014, δεν άλλαξε σχεδόν καθόλου, αφού σημείωσε πτώση μόνο 0,16 ποσοστιαίες μονάδες.

Το φαινόμενο spam αλλάζει συνεχώς και ακόμη και αν η συγκεκριμένη έρευνα έδειξε την παραδοσιακή διαφήμιση μέσω spam να μειώνεται, παρατηρήθηκαν πολύ περισσότερα περιστατικά απάτης, malware και phishing. Ως εκ τούτου, ακόμη και οι πιο έμπειροι χρήστες του διαδικτύου θα πρέπει να είναι πιο προσεκτικοί από ποτέ για να αποφύγουν παγίδες που κρύβουν τα μηνύματα αυτά.

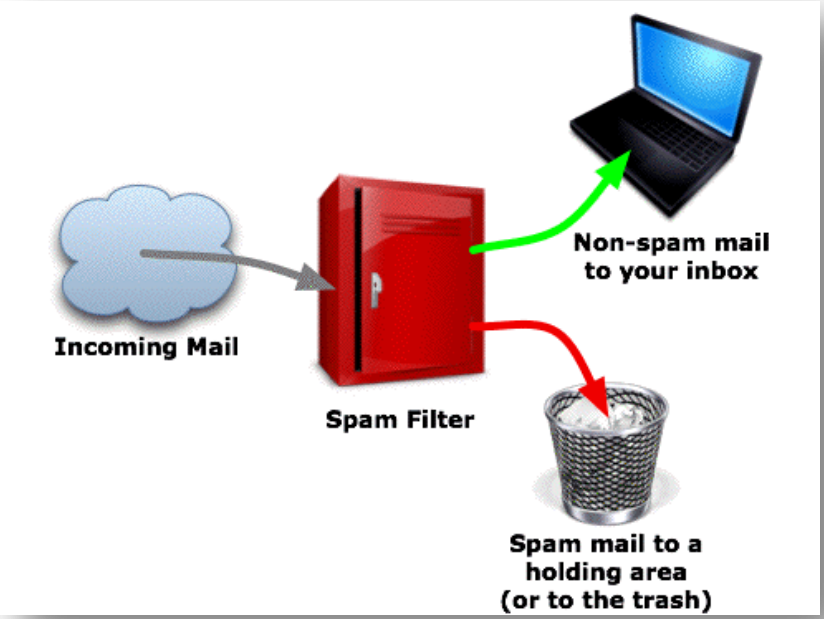
Κεφάλαιο 3
Αρχιτεκτονικές Spam Filtering

Ακριβώς επειδή το Διαδίκτυο είναι δημόσιο, είναι αδύνατο να αποφευχθεί η αποστολή spam μηνυμάτων. Ωστόσο με την εφαρμογή κατάλληλων μεθόδων πρόληψης και αντιμετώπισης, τα μηνύματα spam μπορούν να περιοριστούν σημαντικά. Για τον περιορισμό αυτό, τόσο οι τελικοί χρήστες, όσο και οι διαχειριστές συστημάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιούν διάφορες τεχνικές (anti-spam τεχνικές). [15] Μερικές από αυτές τις τεχνικές συχνά ενσωματώνονται σε προϊόντα, υπηρεσίες και λογισμικό, έτσι ώστε το βάρος για τους χρήστες και τους διαχειριστές όσο γίνεται να μειώνεται. Ωστόσο, καμία τεχνική από μόνη της δεν αποτελεί μια ολοκληρωμένη λύση για το πρόβλημα των αυτόκλητων μηνυμάτων, με καθεμία από αυτές να παρουσιάζει διαφορές με τις υπόλοιπες ως προς την αποτελεσματικότητα, το σχετικό κόστος σε χρόνο και προσπάθεια, καθώς και τα κοινωνικά θέματα που θίγει.

3.1 Ορισμός Spam Filter

Ένα spam filter είναι ένα πρόγραμμα που ταξινομεί την εισερχόμενη αλληλογραφία με σκοπό τον εντοπισμό και την επισήμανση της ανεπιθύμητης αλληλογραφίας. [16] Μπορεί να εγκατασταθεί σε έναν Internet mail server, σε έναν ιδιωτικό network server ή σε έναν προσωπικό υπολογιστή.

Λόγω του ότι τα μηνύματα spam δεν είναι μόνο ενοχλητικά, αλλά συχνά χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού και ιών, ή ακόμη και για απάτες phishing, τα φίλτρα spam αποτελούν έναν πολύ καλό τρόπο για να προστατέψουν οι χρήστες τον υπολογιστή ή το δίκτυό τους, αλλά και για να απαλλαχθούν από τα junk mail. Η παρακάτω εικόνα (εικόνα 3.1) αναπαριστά τη λειτουργία την οποία είναι υπεύθυνα να επιτελέσουν τα spam filters. [42]



Εικόνα 3.1: Η basic λειτουργία ενός spam filter

Τα φίλτρα, προκειμένου να ανιχνεύσουν τα spam, συγκρίνουν διάφορες παραμέτρους στα εισερχόμενα μηνύματα χρησιμοποιώντας καταλόγους που περιέχουν διαμορφωμένους κανόνες. Για παράδειγμα, τα φίλτρα, μπορούν να ρυθμιστούν για να ελέγχουν το θέμα της κεφαλίδας του μηνύματος για όρους που σχετίζονται με κοινά προϊόντα που διαφημίζονται μέσω spam, όπως πορνογραφία ή παράνομα φαρμακευτικά προϊόντα. Επίσης τα spam filters εξετάζουν συχνά το πεδίο με τη διεύθυνση του αποστολέα, ώστε να διαπιστωθεί αν το μήνυμα προέρχεται από κάποιο γνωστό spammer.

3.2 Απαιτήσεις Αρχιτεκτονικών Spam-Filtering

Τα φίλτρα που προορίζονται για χρήστες e-mail πρέπει να είναι ακριβή, να προσαρμόζονται εύκολα στις ανάγκες του χρήστη και φυσικά να είναι εύκολα στη χρήση. [17] Ωστόσο, τα

απαιτούμενα χαρακτηριστικά ενός φίλτρου ανεπιθύμητης αλληλογραφίας για e-mail servers είναι ελαφρώς διαφορετικά. Σε γενικές γραμμές υπάρχουν πολλά κριτήρια που αξιολογούν την αποτελεσματικότητα των anti-spam μεθόδων. Ορισμένα από τα βασικά χαρακτηριστικά που πρέπει να διακρίνουν ένα αποτελεσματικό φίλτρο είναι τα παρακάτω:

Ευκολία συντήρησης: Οι περισσότερες από τις παραδοσιακές μεθόδους φιλτραρίσματος spam απαιτούν ενημέρωση της βάσης δεδομένων τους, έτσι ώστε να μπορούν να χειριστούν νέους τύπους spam. [17] Δυστυχώς, οι spammers έχουν την τάση να είναι πολύ παραγωγικοί και πάντα να δημιουργούν νέους τύπους spam. Αυτό καθιστά τη διαδικασία της συντήρησης δύσκολη, ειδικά για τους e-mail servers.

Ευρωστία: Το κριτήριο αυτό χρησιμοποιείται για να αξιολογήσει πόσο δύσκολο είναι για τους spammers να βρουν ελαττώματα στο φίλτρο spam και να τα εκμεταλλευτούν για την αποστολή ανεπιθύμητων μηνυμάτων. [18] Η μέθοδος φιλτραρίσματος θεωρείται αξιόπιστη μόνο αν υπάρχει ένας ισχυρός μηχανισμός για την ανίχνευση πλαστών e-mail. Στις σημερινές υπηρεσίες e-mail, τόσο οι κεφαλίδες του e-mail, όσο και άλλα μέρη του, μπορούν να τροποποιηθούν εύκολα. Ως εκ τούτου, υπάρχει μια σημαντική πιθανότητα ο αποστολέας να έχει παραποιήσει τα στοιχεία της κεφαλίδας, ή ακόμη και τα πεδία ονομάτων DNS και τη διεύθυνση e-mail αποστολέα, προκειμένου να προσποιηθεί ότι το e-mail προέρχεται από μια νόμιμη πηγή. Επιπλέον, σε ένα ελεγχόμενο περιβάλλον, όπως είναι μία επιχείρηση, οι spammers είναι σχετικά εύκολο να δεσμεύσουν τις πραγματικές ταυτότητες των χρηστών και των λογαριασμών e-mail τους, αφού ο κάθε χρήστης έχει ήδη μια πραγματική ταυτότητα καταχωρημένη στη βάση δεδομένων της εταιρείας. Ωστόσο, σε δημόσια συστήματα, όπως το Yahoo! ή το AOL, οι spammers μπορούν να δημιουργήσουν πολλούς πλαστούς λογαριασμούς, καθώς αυτοί δε συνδέονται με μια πραγματική ταυτότητα. Μια πολιτική θα μπορούσε να αναγκάσει τους χρήστες να κάνουν εγγραφή με τις πραγματικές ταυτότητές τους, ακόμη και σε δημόσια συστήματα, αλλά αυτό θα μπορούσε να έρχεται σε σύγκρουση με ζητήματα προστασίας της ιδιωτικής ζωής, διότι τα ανώνυμα μηνύματα θα πρέπει να παρεμποδίζονται. Σε γενικές γραμμές, ένα αποτελεσματικό anti-spam σύστημα θα πρέπει να έχει σχεδιαστεί στο πνεύμα μίας λύσης ασφάλειας, υποθέτοντας πάντα για το χειρότερο σενάριο και την ικανότητα των spammers να αναλύουν τις μεθόδους φιλτραρίσματος και να παίρνουν μέτρα για να τις προσπερνούν. [19]

Υψηλή ταχύτητα επεξεργασίας: Οι μεγάλοι ISP e-mail servers πρέπει να χειρίζονται δισεκατομμύρια e-mail ανά ημέρα. [17] Αυτό σημαίνει ότι τα φίλτρα spam πρέπει να χειρίζονται περισσότερα από 1000 e-mails ανά δευτερόλεπτο. Δεδομένου ότι πιο γνωστό πρόγραμμα

φιλτραρίσματος spam απαιτεί 10 έως 100 χιλιοστά του δευτερολέπτου για να ασχοληθεί με κάθε e-mail, η βελτίωση των επιδόσεων των φίλτρων καθίσταται απαραίτητη.

Απουσία false positives: Η απόρριψη της αυτόκλητης ανεπιθύμητης αλληλογραφίας δεν πρέπει να αποτελεί εμπόδιο για τη διάδοση των νόμιμων e-mail. [19] Τα false positives είναι νόμιμα μηνύματα που λανθασμένα χαρακτηρίζονται ως spam. Για τους περισσότερους χρήστες, το να χάσουν ένα νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου είναι πολύ χειρότερο απ' ότι να λάβουν ένα spam. Έτσι, ένα φίλτρο που δίνει false positives θεωρείται μη αποδεκτό.

Ευκολία χρήσης: Το κριτήριο αυτό αναφέρεται στο πόσο εύκολα μπορούν να χρησιμοποιηθούν οι anti-spam προσεγγίσεις από τους τελικούς χρήστες. [18] Για παράδειγμα, υπάρχουν συστήματα τα οποία ενσωματώνουν τη διατήρηση whitelist, τη ρύθμιση ψευδωνύμου για κάθε διεύθυνση και τη διαδικασία πρόκλησης – απόκρισης, που είναι σχετικά πολύπλοκα για το χρήστη σε σύγκριση με άλλες μεθόδους.

Υψηλή ακρίβεια: Παρά το γεγονός ότι η ακρίβεια είναι σημαντική για τα φίλτρα ανεπιθύμητης αλληλογραφίας που χρησιμοποιούν οι χρήστες, είναι επίσης σημαντικό ένα φίλτρο spam να είναι ακριβές σε έναν e-mail server. [17] Κατά την εξέταση των spam φίλτρων, οι απαιτήσεις για ακρίβεια είναι πολύ διαφορετικές για τους απλούς χρήστες και για τους διακομιστές. Ένας server απαιτεί η λανθασμένη πιθανότητα ενός κανονικού e-mail να σημειωθεί ως spam να είναι μηδενική, ενώ η αυστηρή αυτή απαίτηση δεν είναι απαραίτητη για τους χρήστες. Με άλλα λόγια, μία μέθοδος anti-spam που επιτυγχάνει την ανωτέρω απαίτηση υλοποιείται μόνο μέσα σε ένα περιβάλλον server.

Συμβατότητα με την τρέχουσα υποδομή ηλεκτρονικού ταχυδρομείου: Η ευθύτητα και η ευελιξία των συστημάτων διανομής ηλεκτρονικού ταχυδρομείου είναι οι δύο βασικοί παράγοντες επιτυχίας του ηλεκτρονικού ταχυδρομείου ως κανάλι ανταλλαγής πληροφοριών. [19] Ως εκ τούτου, μία αποτελεσματική λύση anti-spam δε θα πρέπει να δημιουργεί πολλά εμπόδια στα υπάρχοντα πρωτόκολλα και αρχιτεκτονικές e-mail.

Προστασία της ιδιωτικής ζωής: Για να τεθεί ένα φίλτρο σε εφαρμογή σε ένα διακομιστή e-mail ή σε ένα δίκτυο, είναι επιθυμητό η μέθοδος αυτή και οι συναφείς λειτουργίες της να μην αποκαλύπτουν άμεσα το περιεχόμενο του e-mail (π.χ. κατά τη σύγκριση μηνυμάτων ή λέξεων κλειδιών). [17]

3.3 Κατηγορίες Spam Filtering

Η ενασχόληση με τα spam μηνύματα αποτελεί χάσιμο χρόνου, αλλά και πόρων. Το φιλτράρισμα των έγκυρων μηνυμάτων έναντι των spam, απαιτεί να δαπανήσουμε μεγάλο χρονικό διάστημα της καθημερινότητάς μας σε βάθος χρόνου, και ως εκ τούτου χρημάτων. Η εγκατάσταση ενός φίλτρου spam παρέχει τα απαραίτητα στοιχεία που απαιτούνται για να εξασφαλιστεί ότι θα σπαταλάμε τον ελάχιστο χρόνο στο «κοσκίνισμα» των έγκυρων μηνυμάτων έναντι των spam. Ενώ κανένα anti-spam λογισμικό δεν μπορεί να εγγυηθεί την κατάργηση όλων των ανεπιθύμητων μηνυμάτων αυτόματα, υπάρχουν συστήματα που μπορούν να κάνουν μια πολύ καλή δουλειά.

Οι τεχνικές anti-spam μπορούν να χωριστούν σε τρεις μεγάλες κατηγορίες: αυτές που απαιτούν ενέργειες από τους χρήστες, αυτές που μπορούν να αυτοματοποιηθούν από τους διαχειριστές e-mail και εκείνες που χρησιμοποιούνται από τους ερευνητές και τα όργανα επιβολής του νόμου.

3.3.1 End-user techniques

Υπάρχει μια σειρά από τεχνικές που μπορούν να χρησιμοποιήσουν οι τελικοί χρήστες προκειμένου να προλάβουν ή να περιορίσουν την παραλαβή μηνυμάτων spam.

Αποφυγή απάντησης σε spam: Όταν οι spammers δέχονται απαντήσεις στα μηνύματα που στέλνουν, ακόμη και αν λαμβάνουν απαντήσεις όπως, «Μη μου ξαναστείλετε spam", επιβεβαιώνουν την εγκυρότητα μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου. [15] Επίσης, πολλά μηνύματα spam περιέχουν υπερσυνδέσμους ή διευθύνσεις που προτρέπουν το χρήστη να τους ακολουθήσει προκειμένου αυτός να αφαιρεθεί από τη λίστα του αποστολέα. Σε αρκετές από αυτές τις περιπτώσεις, οι σύνδεσμοι αυτοί δεν οδηγούν στην εν λόγω αφαίρεση από τη λίστα αλλά αν μη τι άλλο, σε περισσότερα spam.

Διακριτικότητα: Η γνωστοποίηση της προσωπικής διεύθυνσης ηλεκτρονικού ταχυδρομείου ορισμένων ατόμων, μόνο ανάμεσα σε μια περιορισμένη ομάδα χρηστών είναι ένας τρόπος για να περιοριστεί ο αριθμός των spam. [15] Η μέθοδος αυτή στηρίζεται στη διακριτική ευχέρεια όλων των μελών μιας ομάδας, καθώς η αποκάλυψη διευθύνσεων ηλεκτρονικού ταχυδρομείου εκτός της ομάδας παρακάμπτει τη σχέση εμπιστοσύνης τους. Για το λόγο αυτό, θα πρέπει να αποφεύγεται η αποστολή μηνυμάτων σε παραλήπτες που δε γνωρίζουν ο ένας τον άλλο. Όταν είναι απολύτως απαραίτητο να προωθηθούν μηνύματα σε παραλήπτες που δεν γνωρίζουν ο ένας τον άλλο, είναι καλή πρακτική να προσθέτουμε τις διευθύνσεις των παραληπτών στο πεδίο «bcc:» [12] έναντι του πεδίου «to:». Η πρακτική αυτή αποκλείει το σενάριο κατά το οποίο αδίστακτοι παραλήπτες «κλέβουν» μια λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου και τη χρησιμοποιούν για σκοπούς spamming. Η πρακτική αυτή μειώνει επίσης τον κίνδυνο η διεύθυνση του χρήστη να διανεμηθεί από υπολογιστές που έχουν προσβληθεί από malware συγκομιδής διευθύνσεων ηλεκτρονικού ταχυδρομείου. Ωστόσο, αν κάποια διεύθυνση ηλεκτρονικού ταχυδρομείου αποκαλυφθεί, η αρχική μυστικότητα δεν μπορεί να ανακτηθεί.

Φόρμες επικοινωνίας (contact forms): Οι φόρμες επικοινωνίας επιτρέπουν στους χρήστες να στέλνουν e-mail συμπληρώνοντας φόρμες με τα στοιχεία τους σε ένα πρόγραμμα περιήγησης στο web. [15] Ο web server λαμβάνει τα δεδομένα της φόρμας, διαβιβάζοντάς τα σε μια διεύθυνση e-mail. Οι χρήστες δε βλέπουν ποτέ τη διεύθυνση αυτή ηλεκτρονικού ταχυδρομείου στην οποία διαβιβάζονται τα προσωπικά στοιχεία τους. Τέτοιες μορφές είναι μερικές φορές ενοχλητικές για τους χρήστες, δεδομένου ότι δεν είναι σε θέση να χρησιμοποιήσουν τον δικό τους e-mail client, κινδυνεύοντας να εισάγουν τη διεύθυνσή τους λάθος και συνήθως δεν τους κοινοποιούνται πιθανά προβλήματα παράδοσης. Τέλος, εάν το λογισμικό που χρησιμοποιείται για να τρέξει τις contact forms έχει κακό σχεδιασμό, μπορεί να γίνει ένα εργαλείο spam από μόνο του. Μάλιστα, μερικοί spammers έχουν αρχίσει να στέλνουν spam, χρησιμοποιώντας τις φόρμες επικοινωνίας.

Απόκρυψη ηλεκτρονικής διεύθυνσης: Η χρήση ανωνυμίας ή εναλλακτικά η χρήση ψεύτικου ονόματος και διεύθυνσης είναι ένας τρόπος για να αποφευχθεί η «συγκομιδή» της διεύθυνσης ηλεκτρονικού ταχυδρομείου του χρήστη. [15] Ωστόσο, οι χρήστες θα πρέπει να διασφαλίζουν ότι η πλαστή διεύθυνση που χρησιμοποιούν δεν είναι έγκυρη, διαφορετικά κάποιος άλλος

[12] bcc: είναι παρόμοιο με το Cc, που χρησιμοποιείται για να στείλουμε αντίτυπα του e-mail και σε άλλους χρήστες, αλλά οι παραλήπτες του μηνύματος που καθορίζονται στο Bcc είναι "αόρατοι" στους υπόλοιπους παραλήπτες.

διακομιστής θα λαμβάνει πλέον τα spam. Οι χρήστες που θέλουν να λαμβάνουν έγκυρη αλληλογραφία, σχετικά με δημοσιεύσεις τους ή κάποιες ιστοσελίδες μπορούν να αλλάξουν τις διευθύνσεις τους, έτσι ώστε να είναι κατανοητές από τους ανθρώπους, αλλά όχι από τους spammers. Για παράδειγμα, ο χρήστης με τη διεύθυνση joe@example.com θα μπορούσε να τη χρησιμοποιήσει ως joeNOS@PAM.example.com. Υπάρχουν και άλλοι τρόποι βέβαια, στους οποίους η διεύθυνση που χρησιμοποιείται, επιτρέπει ναι μεν στους χρήστες να τη δουν, αλλά τη «θολώνει» στις αυτόματες μηχανές αναζήτησης e-mail, με μεθόδους όπως η εμφάνιση του συνόλου ή μέρους της διεύθυνσης ηλεκτρονικού ταχυδρομείου ως μια εικόνα, ένα λογότυπο κειμένου συρρικνωμένο σε κανονικό μέγεθος ή μπερδεμένο κείμενο με τη σειρά των χαρακτήρων να έχει αποκατασταθεί χρησιμοποιώντας CSS (π.χ. contact@thatsjournal@com).

Απενεργοποίηση HTML στα e-mail: Πολλά προγράμματα σύγχρονου ηλεκτρονικού ταχυδρομείου ενσωματώνουν τη λειτουργικότητα των προγραμμάτων περιήγησης στο Διαδίκτυο, όπως η απεικόνιση HTML, URLs, και εικόνων. [15] Αυτό μπορεί εύκολα να εκθέσει το χρήστη σε προσβλητικό περιεχόμενο που περιέχεται στο spam. Επιπλέον, τα spam που είναι γραμμένα σε HTML μπορεί να περιέχουν συστήματα τέτοια που επιτρέπουν στους spammers να ελέγχουν αν μία διεύθυνση ηλεκτρονικού ταχυδρομείου είναι έγκυρη και ότι το μήνυμα δεν έχει πιαστεί σε φίλτρα spam. Επίσης με τη χρήστη Javascript οι spammers συχνά κατευθύνουν το χρήστη σε σελίδες με διαφημιστικό περιεχόμενο ή καθιστούν το κλείσιμο ή τη διαγραφή του μηνύματος δύσκολη. Τα spam μηνύματα με το περιεχόμενο αυτό συχνά έχουν αναφερθεί και για εγκατάσταση λογισμικού υποκλοπής spyware στα συστήματα των χρηστών, με αποτέλεσμα η ασφάλεια του τελικού χρήστη να τίθεται σε κίνδυνο. Οι χρήστες ηλεκτρονικού ταχυδρομείου που δεν κατεβάζουν και εμφανίζουν αυτόματα την HTML, εικόνες ή συνημμένα αρχεία, έχουν λιγότερους κινδύνους, ακριβώς όπως και οι λογαριασμοί που έχουν ρυθμίσει ως προεπιλογή να μην εμφανίζεται το περιεχόμενο αυτό.

3.3.2 Αυτοματοποιημένες τεχνικές για e-mail administrators

Οι διαχειριστές ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιήσουν μια σειρά από συσκευές, υπηρεσίες και συστήματα λογισμικού, για να μειώσουν τον αριθμό των spam στα συστήματα και τα γραμματοκιβώτιά τους. [15] Μερικά από τα συστήματα αυτά βασίζονται στην απόρριψη e-mail από ιστοσελίδες του Διαδικτύου που είναι γνωστές ή έχουν μεγάλες

πιθανότητες να στέλνουν spam. Άλλες πιο προηγμένες τεχνικές αναλύουν μοτίβα μηνυμάτων σε πραγματικό χρόνο για να ανιχνεύουν τα spam ως συμπεριφορά και στη συνέχεια να τα συγκρίνουν με παγκόσμιες βάσεις δεδομένων spam. Αυτές οι μέθοδοι μπορούν να ανιχνεύουν spam σε πραγματικό χρόνο, ακόμη και όταν δεν υπάρχει περιεχόμενο (spam που περιέχουν συνημμένες εικόνες) και σε οποιαδήποτε γλώσσα. Μια άλλη μέθοδος βασίζεται στην αυτόματη ανάλυση του περιεχομένου των μηνυμάτων ηλεκτρονικού ταχυδρομείου και στη διαγραφή εκείνων που μοιάζουν με spam. Αυτές οι τρεις προσεγγίσεις συχνά αναφέρονται ως blocking (κλείδωμα), pattern detection (ανίχνευση μοτίβου), και το filtering (φιλτράρισμα).

Πολλά συστήματα φιλτραρίσματος επωφελούνται από τις τεχνικές μηχανικής μάθησης, οι οποίες βελτιώνουν την ακρίβειά τους πάνω στις χειροκίνητες μεθόδους. Ωστόσο, μερικοί άνθρωποι βρίσκουν το filtering παρεμβατικό για την ιδιωτική ζωή και πολλοί διαχειριστές e-mail προτιμούν το blocking για να σταματήσουν την πρόσβαση στα συστήματά τους από γνωστές ιστοσελίδες δράσης των spammers.

3.3.2.1 Origin - Based Filters

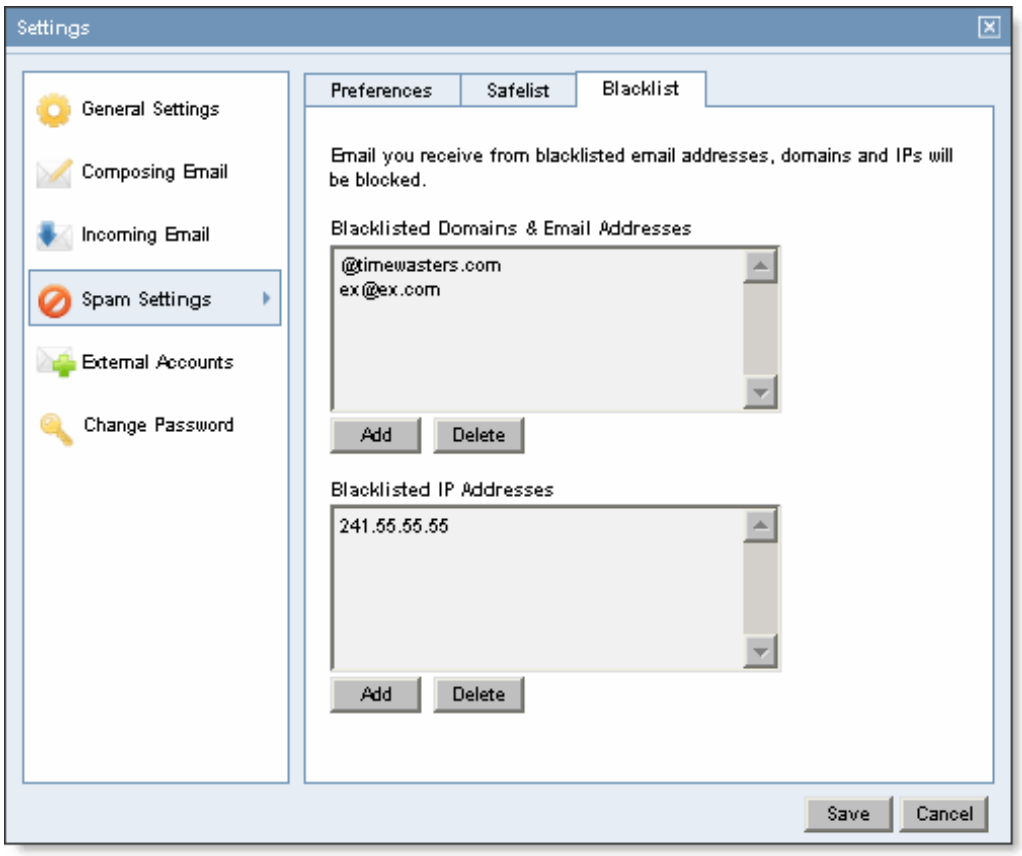
Τα φίλτρα αυτά προσπαθούν να μειώσουν τα spam, χαρακτηρίζοντας τους αποστολείς μηνυμάτων ως έμπιστους ή ως spammers επιτρέποντας ή μπλοκάροντας τα μηνύματα από αυτούς αντίστοιχα.

Blacklists

Η δημοφιλής αυτή μέθοδος φιλτραρίσματος spam, προσπαθεί να σταματήσει τα ανεπιθύμητα e-mail με το κλείδωμα των μηνυμάτων από έναν προκαθορισμένο κατάλογο αποστολέων που ο χρήστης ή ο διαχειριστής του συστήματος δημιουργεί. Επομένως, η Blacklist αποτελεί μία λίστα με διευθύνσεις αποστολέων, domain names ή IP διευθύνσεις, που θεωρούνται ως πηγές spam (δίνεται παράδειγμα εισαγωγής διευθύνσεων στην blacklist στην εικόνα 3.2 [44]). [20] Όταν φθάνει ένα νέο εισερχόμενο μήνυμα, το φίλτρο spam ελέγχει να δει εάν η διεύθυνση IP ή η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα είναι στη μαύρη λίστα και αν είναι, το μήνυμα θεωρείται spam και απορρίπτεται. Αν και οι blacklists εξασφαλίζουν ότι δεν μπορούν να φτάσουν μηνύματα από γνωστούς spammers στα εισερχόμενα των χρηστών, μπορούν επίσης

να αναγνωρίσουν λάθος νόμιμους αποστολείς ως spammers. Αυτά είναι τα λεγόμενα false positives και μπορούν να προκύψουν αν ένας spammer τυχαίνει να στέλνει ανεπιθύμητη αλληλογραφία από μια διεύθυνση IP που χρησιμοποιείται επίσης από έναν νόμιμο χρήστη ηλεκτρονικού ταχυδρομείου. Επίσης, δεδομένου ότι πολλοί έξυπνοι spammers αλλάζουν συνήθως διευθύνσεις IP και διευθύνσεις ηλεκτρονικού ταχυδρομείου για να καλύψουν τα ίχνη τους, μια blacklist δεν μπορεί να εντοπίσει αμέσως τις νέες εστίες τους.

Σε αντίθεση με μια λίστα που χρησιμοποιείται σε συνδυασμό με άλλα φίλτρα, μια blacklist δρα ως φίλτρο από μόνη της. Ωστόσο, ένας χρήστης δεν μπορεί να δημιουργήσει μία αρκετά μεγάλη λίστα πιθανών αποστολέων ανεπιθύμητης αλληλογραφίας για μια προσωπική blacklist που να είναι χρήσιμη ως γενικό φίλτρο spam. Αντ' αυτού, υπάρχουν οργανώσεις που συγκεντρώνουν μεγάλες βάσεις δεδομένων με διευθύνσεις IP ή domain names που είναι γνωστά ή πιθανολογούνται να στέλνουν spam και τα φίλτρα spam μπορούν να «ρωτούν» τις βάσεις αυτές σε πραγματικό χρόνο.



Εικόνα 3.2: Παράδειγμα εισαγωγής διευθύνσεων σε μία blacklist

Η διατήρηση μίας πλήρους, ακριβής μαύρης λίστας παραμένει σημαντική πρόκληση. Τα spam στέλνονται από έναν τεράστιο αριθμό πηγών και έτσι η αποτελεσματικότητα της blacklist εξαρτάται από τη δυνατότητά της να προσδιορίσει την πηγή των περισσότερων μηνυμάτων. Μια προσέγγιση είναι η χρήση honeypots [13] και η θεώρηση ότι όσα e-mail στέλνονται από αυτές τις διευθύνσεις είναι spam. Η αποτελεσματικότητα μιας blacklist εξαρτάται από την πληρότητα της και την ακρίβειά της .

Whitelists

Η whitelist μπλοκάρει τα spam χρησιμοποιώντας ένα σύστημα σχεδόν ακριβώς αντίθετο από εκείνο των blacklists. Αντί να δίνει στο χρήστη τη δυνατότητα να καθορίσει από ποιους αποστολείς να εμποδίζονται τα e-mail, του δίνει τη δυνατότητα να καθορίσει από ποιους αποστολείς να επιτρέπονται τα e-mail, οι διευθύνσεις των οποίων τοποθετούνται σε έναν κατάλογο με τους αξιόπιστους χρήστες. [54] Τα περισσότερα φίλτρα spam επιτρέπουν τη χρήση περισσότερων από μία whitelists, στην προσπάθειά τους να μειώσουν τον αριθμό των νόμιμων μηνυμάτων που κατά λάθος χαρακτηρίζονται ως spam. Με ένα πολύ αυστηρό φίλτρο που χρησιμοποιεί μόνο μία λίστα, είναι πολύ πιθανό, όποιο μήνυμα δεν εγκρίνεται (βάσει αυτής της whitelist), να απορρίπτεται αυτόματα.

Το βιβλίο διευθύνσεων του παραλήπτη χρησιμοποιείται συνήθως ως μια whitelist, με την παραδοχή ότι είναι απίθανο να παραλάβουμε μηνύματα spam από αυτές τις διευθύνσεις ηλεκτρονικού ταχυδρομείου. [20] Η whitelist δεν αποτελείται απαραίτητα από μία λίστα ηλεκτρονικών διευθύνσεων, αλλά μπορεί να περιέχει domain names ή διευθύνσεις IP. Αυτές οι λίστες μπορεί να αποτελέσουν κίνδυνο, στην περίπτωση που ο spammer μαντέψει μία διεύθυνση της λίστας και προσθέσει τη διεύθυνση αυτή ψευδώς ως αποστολέα του spam μηνύματος. Ένας τρόπος να μαντέψει ο spammer τις διευθύνσεις είναι απλά να χρησιμοποιήσει πραγματικές διευθύνσεις ηλεκτρονικού ταχυδρομείου που βρήκε στο Διαδίκτυο ή οπουδήποτε αλλού. Μάλιστα, κάποιες πιο εξελιγμένες τεχνικές εξόρυξης δεδομένων, ταξινομούν τις ηλεκτρονικές διευθύνσεις ανάλογα με τον τομέα τους ή ανάλογα με την ιστοσελίδα στην οποία εμφανίζονταν. Για παράδειγμα, ένας συγγραφέας θα λαμβάνει ένα δυσανάλογα μεγάλο αριθμό

[13] honeypot: είναι μία παγίδα για την ανίχνευση ή την αντιμετώπιση απόπειρας μη εξουσιοδοτημένης χρήσης συστημάτων πληροφοριών. Μοιάζει με τη διαδικασία κατά την οποία η αστυνομία βάζει ένα δόλωμα και στη συνέχεια διεξάγει μυστική παρακολούθηση

πλαστογραφημένων spam μηνυμάτων, που θα φαίνονται ότι αποστέλλονται από τους συντάκτες του για διάφορες δημοσιευμένες δουλειές του.

Greylists

Αποτελεί μια σχετικά νέα τεχνική φιλτραρίσματος spam που επωφελείται από το γεγονός ότι πολλοί spammers προσπαθούν να στείλουν μια παρτίδα ανεπιθύμητης αλληλογραφίας μόνο μία φορά. Το greylisting είναι μία μορφή πρόκλησης - απόκρισης (challenge - response) που εμπλέκει το λογισμικό παράδοσης αλληλογραφίας του αποστολέα και όχι τον ίδιο τον αποστολέα. [20] Στο σύστημα greylist, ο διακομιστής παραλαβής αλληλογραφίας απορρίπτει αρχικά μηνύματα από άγνωστους χρήστες και στέλνει ένα μήνυμα σφάλματος στο διακομιστή προέλευσης του μηνύματος. Εάν ο διακομιστής αλληλογραφίας προσπαθήσει να στείλει το μήνυμα για δεύτερη φορά - ένα βήμα που θα κάνουν οι περισσότεροι νόμιμοι servers- το greylist υποθέτει ότι το μήνυμα δεν είναι spam και του δίνει τη δυνατότητα να προχωρήσει στα εισερχόμενα του παραλήπτη. Επίσης, σε αυτό το σημείο, το φίλτρο greylist προσθέτει τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή τη διεύθυνση IP του παραλήπτη σε μια λίστα επιτρεπόμενων αποστολέων. Το φίλτρο λοιπόν αυτό δρα με την παραδοχή ότι τα νόμιμα μηνύματα είναι πιο πιθανό να σταλούν για δεύτερη φορά, απ' ότι τα spam μηνύματα.

Αν και τα greylist φίλτρα απαιτούν λιγότερους πόρους συστήματος από ό, τι κάποια άλλα φίλτρα spam, μπορεί επίσης να καθυστερήσουν την παράδοση της αλληλογραφίας, γεγονός που θα μπορούσε να είναι ενοχλητικό, πόσο μάλλον όταν περιμένουμε μηνύματα ευαίσθητα στον παράγοντα χρόνο. Εκτός από την καθυστέρηση, το greylisting μπορεί να οδηγήσει και στο να χαθούν νόμιμα μηνύματα, δεδομένου ότι εξαρτάται από τον αποστολέα να κάνει την αναμετάδοση και από την ικανότητα του φίλτρου να αναγνωρίσει την αναμετάδοση αυτή. Επιπλέον, τα χαμένα μηνύματα είναι σχεδόν αδύνατο να εντοπιστούν ή να ανακτηθούν.

Realtime Blackhole Lists

Αποτελεί μία μέθοδο φιλτραρίσματος spam. που λειτουργεί σχεδόν με τον ίδιο τρόπο όπως μια παραδοσιακή blacklist, με τη διαφορά ότι απαιτεί λιγότερα «χέρια» για τη συντήρηση. [21] Αυτό συμβαίνει γιατί οι περισσότερες realtime blackhole lists συντηρούνται από τρίτους οι οποίοι

αναπτύσσουν ολοκληρωμένες blacklists για λογαριασμό των συνδρομητών τους. Το φίλτρο αυτό απλά συνδέεται με το σύστημα των τρίτων κάθε φορά που ένα νέο e-mail έρχεται και συγκρίνει τη διεύθυνση IP του αποστολέα με βάση τη λίστα αυτή.

Καθώς οι blackhole λίστες είναι μεγάλες και ενημερώνονται συχνά, το προσωπικό μίας εταιρείας ή οι χρήστες δε χρειάζεται να δαπανούν χρόνο για να προσθέτουν χειροκίνητα νέες διευθύνσεις IP στη λίστα. Όμως, ακριβώς όπως και οι blacklists, έτσι και οι realtime blackhole lists μπορούν επίσης να δημιουργήσουν false positives, αν τύχει οι spammers να χρησιμοποιήσουν μια νόμιμη διεύθυνση IP για την αποστολή junk mail. Επίσης, δεδομένου ότι η λίστα διατηρείται συνήθως από τρίτους, οι χρήστες έχουν μικρότερο έλεγχο ως προς τις διευθύνσεις που βρίσκονται ή όχι στη λίστα.

DNS-based Blackhole List (DNSBL)

Αποτελεί μια λίστα με τις διευθύνσεις IP που χρησιμοποιούνται πιο συχνά, για να δημοσιεύουν διευθύνσεις υπολογιστών ή δίκτυα που συνδέονται με το spamming. [22] Οι περισσότεροι διακομιστές ηλεκτρονικής αλληλογραφίας μπορούν να ρυθμιστούν ώστε να απορρίπτουν ή να επισημαίνουν μηνύματα που έχουν αποσταλεί από ένα site που αναφέρεται σε έναν ή περισσότερους τέτοιους καταλόγους. Ο όρος "Blackhole List" μερικές αναφέρεται απλά και με τους όρους " blacklist" και "blocklist". Η DNSBL αποτελεί περισσότερο έναν μηχανισμό λογισμικού, παρά μία απλή λίστα. Αυτή τη στιγμή, υπάρχουν δεκάδες DNSBLs, οι οποίες χρησιμοποιούν ένα ευρύ φάσμα κριτηρίων για την εγγραφή και διαγραφή διευθύνσεων. Οι λίστες αυτές μπορεί να περιλαμβάνουν την καταχώριση διευθύνσεων υπολογιστών ή άλλων μηχανημάτων που χρησιμοποιούνται μόνο για την αποστολή spam, τους ISP που φιλοξενούν πρόθυμα spammers ή εκείνους που έχουν στείλει spam σε ένα σύστημα honeypot. Αν η διεύθυνση του αποστολέα είναι καταγεγραμμένη στις λίστες αυτές, τότε απορρίπτεται πριν ακόμη μεταφερθεί.

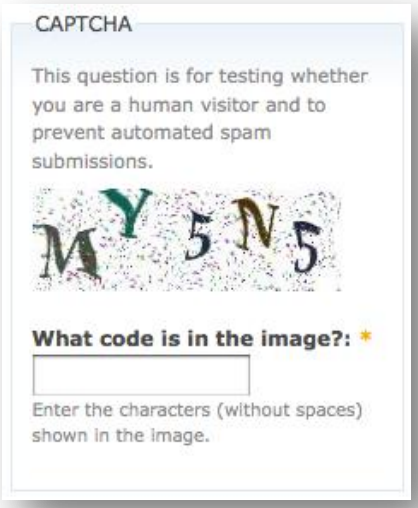
Challenge - Response Filtering

Το σύστημα πρόκλησης – απόκρισης (challenge - response) αποτελεί ένα είδος φίλτρου spam που στέλνει αυτόματα μια απάντηση με μια πρόκληση (για απόκριση) στον αποστολέα ενός εισερχόμενου e-mail. [23] Στην απάντηση αυτή, ο αποστολέας καλείται να εκτελέσει κάποια

δράση που να εξασφαλίζει την παράδοση του αρχικού μηνύματος, το οποίο διαφορετικά δε θα παραδοθεί. Η δράση που πρέπει να εκτελεστεί είναι συνήθως κάτι που μπορεί να εκτελεστεί σχετικά αβίαστα, αλλά χρειάζεται μεγάλη προσπάθεια, εάν αυτή πραγματοποιηθεί σε μεγάλους αριθμούς, δρώντας έτσι αποτελεσματικά ενάντια στους spammers. Η απόκριση αυτή του αποστολέα μπορεί να είναι τόσο ένα απλό κλικ σε ένα σύνδεσμο ή η επαναποστολή του μηνύματος, όσο η παροχή διαπιστευτηρίων, η επίλυση ενός παζλ, η πραγματοποίηση μιας υποτιθέμενης πληρωμής ή η εκτέλεση ενός χρονοβόρου υπολογισμού. [20] Αντιλαμβανόμαστε λοιπόν γιατί η εργασία αυτή είναι εύκολη για έναν νόμιμο αποστολέα, αλλά ακριβή και χρονοβόρα για έναν spammer που στέλνει χιλιάδες ή εκατομμύρια μηνύματα.

Τα συστήματα challenge - response χρειάζεται να στέλνουν προκλήσεις μόνο σε άγνωστους αποστολείς. Οι αποστολείς που έχουν ήδη απαντήσει στην προκλητική ενέργεια, ή στους οποίους έχουμε στείλει εμείς e-mail, μπαίνουν στη λίστα επιτρεπόμενων αποστολέων αυτόματα.

Υπάρχουν διάφορα συστήματα πρόκλησης-απόκρισης που διαφέρουν ως προς τους μηχανισμούς που χρησιμοποιούν για την εξακρίβωση του αποστολέα. Από τα πιο γνωστά τέτοια συστήματα είναι τα pre-challenge, που ενσωματώνουν τη διαδικασία πρόκλησης – απόκρισης στη διασύνδεση του αποστολέα και συνήθως εμφανίζονται στο μήνυμα με ξεχωριστό interface. Το πιο γνωστό σύστημα pre-challenge είναι η ανθρώπινη διαδραστική απόδειξη, όπως για παράδειγμα το CAPTCHA [14]. [43]



Εικόνα 3.3: Παράδειγμα συστήματος πρόκλησης-απόκρισης CAPTCHA

Τα φίλτρα αυτά φαίνεται να μη γίνονται ευρέως αποδεκτά, αφού σε πολλές των περιπτώσεων απορρίπτουν μηνύματα από νόμιμους αποστολείς. [20] Για παράδειγμα, υπάρχει νόμιμη ηλεκτρονική αλληλογραφία, όπως οι απαντήσεις σε συναλλαγές του web ή τα ενημερωτικά newsletters, που αποστέλλεται από αυτοματοποιημένους servers που φυσικά αδυνατούν να ανταποκριθούν στις προκλήσεις και κατά συνέπεια τα μηνύματα δε φθάνουν ποτέ στον παραλήπτη. Εκτός αυτού, υπάρχει πάντα η μικρή πιθανότητα εάν ο αποστολέας και ο

[14] CAPTCHA: χρησιμοποιείται για να διαπιστωθεί αν ο χρήστης ενός συστήματος που κάνει μία ενέργεια είναι άνθρωπος και όχι μία αυτοματοποιημένη μηχανή

παραλήπτης χρησιμοποιούν και οι δύο συστήματα challenge - response, οι εφαρμογές τους να προκαλούν κατ' επανάληψη η μία την άλλη, με αποτέλεσμα να θέτουν το μήνυμα σε μη παραδοτέο βρόχο (loop).

3.3.2.2 Content - Based Filters

Αντί να επιβάλουν την ίδια πολιτική σε όλα τα μηνύματα από ένα συγκεκριμένο e-mail ή μία IP διεύθυνση, τα content-based filters, αξιολογούν τις λέξεις και τις φράσεις μέσα σε ένα μήνυμα για να καθορίσουν εάν αυτό είναι spam ή όχι.

Word – Based Filters

Τα φίλτρα αυτά, αποτελούν την πιο απλή μορφή content-based filters. Σε γενικές γραμμές, τα word-based filters, απλά μπλοκάρουν κάθε μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει ορισμένες λέξεις ή όρους. Δεδομένου ότι πολλά μηνύματα spam περιέχουν όρους που δε συναντώνται συχνά σε προσωπικές ή επαγγελματικές επικοινωνίες, τα φίλτρα αυτά μπορεί να αποτελούν μια απλή αλλά ικανή τεχνική για την καταπολέμηση της ανεπιθύμητης αλληλογραφίας. Ωστόσο, εάν ρυθμιστούν να μπλοκάρουν μηνύματα που περιέχουν περισσότερο κοινές λέξεις, αυτοί οι τύποι των φίλτρων μπορεί να δημιουργήσουν false positives. Για παράδειγμα, εάν το φίλτρο έχει ρυθμιστεί να σταματάει όλα τα μηνύματα που περιέχουν τη λέξη «έκπτωση», ακόμη και τα μηνύματα από νόμιμους αποστολείς που προσφέρουν μη κερδοσκοπικό υλικό ή λογισμικό σε μειωμένη τιμή, δεν θα μπορούν να φθάσουν στον προορισμό τους. Επίσης, δεδομένου ότι οι spammers συχνά κάνουν αναγραμματισμούς στις λέξεις-κλειδιά σκοπίμως, για να αποφύγουν τα keyword filters, οι χρήστες θα πρέπει να αφιερώνουν χρόνο για να ενημερώνουν τη λίστα του φίλτρου με τις αποκλεισμένες λέξεις.

Heuristic (rule-based) Filters

Τα heuristic filters εξετάζουν τα πράγματα ένα βήμα παραπάνω από το απλό keyword-based φιλτράρισμα. Αντί να μπλοκάρουν μηνύματα που περιέχουν μια ύποπτη λέξη κλειδί, οι ευρετικοί κανόνες λαμβάνουν υπόψη τους πολλαπλούς όρους που βρίσκονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου. [15] Τα φίλτρα αυτά σαρώνουν το περιεχόμενο των εισερχόμενων

μηνυμάτων ηλεκτρονικού ταχυδρομείου και δίνουν «βαθμούς» σε λέξεις ή φράσεις. Για παράδειγμα, ύποπτες λέξεις που βρίσκονται συνήθως σε spam μηνύματα, όπως «Rolex» ή «Viagra», λαμβάνουν υψηλότερους βαθμούς, ενώ όροι που απαντώνται συχνά σε κανονικά e-mail συγκεντρώνουν χαμηλότερες βαθμολογίες. Το φίλτρο στη συνέχεια προσθέτει όλους τους βαθμούς και υπολογίζει τη συνολική βαθμολογία. Εάν το μήνυμα λαμβάνει ένα συγκεκριμένο αποτέλεσμα ή ένα αποτέλεσμα υψηλότερο από ένα όριο (που καθορίζεται από το διαχειριστή της anti-spam εφαρμογής), το φίλτρο προσδιορίζει το μήνυμα ως spam και το μπλοκάρει. Τα μηνύματα που έχουν άθροισμα βαθμών μικρότερο από το όριο, παραδίδονται κανονικά στο χρήστη.

Τα heuristic filters λειτουργούν γρήγορα – ελαχιστοποιώντας την καθυστέρηση παραλαβής των e-mail - και είναι αρκετά αποτελεσματικά αν έχουν ρυθμιστεί σωστά. Ωστόσο, φίλτρα αυτού του τύπου που έχουν ρυθμιστεί έτσι ώστε να είναι «επιθετικά», μπορούν να παράγουν false positives, αν μια νόμιμη επαφή τύχει να στείλει ένα e-mail που περιέχει ένα συγκεκριμένο συνδυασμό λέξεων και συγκεντρώνει βαθμολογία πάνω από το επιτρεπτό όριο. Ορισμένοι spammers προσπαθούν να μαντέψουν ποιες λέξεις δεν πρέπει να συμπεριλάβουν στο μήνυμά τους και προσπαθούν έτσι να εξαπατήσουν τα heuristic filters κάνοντάς τους να πιστέψουν ότι είναι καλοήθεις αποστολείς.

Bayesian Filtering

Η μέθοδος Bayesian είναι μια στατιστική τεχνική φιλτραρίσματος e-mail. [24] Στη βασική της μορφή, κάνει χρήση ενός ταξινομητή Naive Bayes για τον εντοπισμό spam e-mail, μια προσέγγιση που χρησιμοποιείται συνήθως στην κατηγοριοποίηση κειμένων. Οι ταξινομητές Naive Bayes δουλεύουν συσχετίζοντας συνήθως λέξεις (tokens), με spam και μη-spam e-mails και στη συνέχεια, χρησιμοποιώντας τη συμπερασματολογία Bayesian υπολογίζουν την πιθανότητα το e-mail να είναι ή όχι spam. Το φιλτράρισμα Naive Bayes ανεπιθύμητων μηνυμάτων είναι μια τεχνική για την αντιμετώπιση των spam που μπορεί να προσαρμοστεί στις ανάγκες μεμονωμένων χρηστών και αποτελεί έναν από τους παλαιότερους τρόπους φιλτραρίσματος ανεπιθύμητων μηνυμάτων, με ρίζες στη δεκαετία του 1990.

Συγκεκριμένες λέξεις έχουν συγκεκριμένες πιθανότητες να εμφανιστούν σε spam e-mail και σε νόμιμης μορφής μήνυμα ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, οι

περισσότεροι χρήστες ηλεκτρονικού ταχυδρομείου ίσως συναντούν συχνά τη λέξη "Viagra" σε spam e-mail, αλλά θα τη δουν σπάνια σε άλλα e-mail. Το φίλτρο δε γνωρίζει τις πιθανότητες αυτές εκ των προτέρων και θα πρέπει πρώτα να εκπαιδευτεί έτσι ώστε να μπορεί να τις δημιουργεί. Για να εκπαιδεύσει το φίλτρο, ο χρήστης θα πρέπει να αναφέρει με μη αυτόματο τρόπο αν ένα e-mail είναι spam ή όχι. Για όλες τις λέξεις στο κάθε μήνυμα ηλεκτρονικού ταχυδρομείου, το φίλτρο προσαρμόζει τις πιθανότητες εμφάνισης κάθε λέξης ως spam ή ως νόμιμου ηλεκτρονικού ταχυδρομείου, στη βάση δεδομένων του. Για παράδειγμα, τα φίλτρα Bayesian τυπικά δίνουν μια πολύ μεγάλη πιθανότητα για spam για τις λέξεις «Viagra» και «refinance», αλλά πολύ μικρή πιθανότητα spam για λέξεις που παρατηρούνται μόνο σε νόμιμο ηλεκτρονικό ταχυδρομείο, όπως τα ονόματα φίλων και μελών της οικογένειας.

Μετά την εκπαίδευση, οι πιθανότητες των λέξεων (γνωστές και ως συναρτήσεις πιθανότητας), χρησιμοποιούνται για να υπολογίσουν την πιθανότητα ένα e-mail με ένα συγκεκριμένο σύνολο λέξεων να ανήκει στην κατηγορία spam. Κάθε λέξη στο e-mail συμβάλλει στη συνολική πιθανότητα ανεπιθύμητης αλληλογραφίας του e-mail. Η πιθανότητα αυτή ονομάζεται οπίσθια πιθανότητα και υπολογίζεται χρησιμοποιώντας το θεώρημα του Bayes. Στη συνέχεια, η πιθανότητα ανεπιθύμητης αλληλογραφίας του e-mail υπολογίζεται σε σχέση με όλες τις λέξεις στο e-mail και αν το σύνολο υπερβαίνει ένα ορισμένο όριο (δηλαδή 95%), το φίλτρο θα σηματοδοτήσει το e-mail ως spam.

Χρησιμοποιώντας την τεχνική αυτή, η σωρευτική πιθανότητα ενός μηνύματος να θεωρηθεί ως ανεπιθύμητο υπολογίζεται συνδυάζοντας την πιθανότητα που σχετίζεται με tokens στο μήνυμα που συναντώνται στα πραγματικά spam με την πιθανότητα που σχετίζεται με tokens στο μήνυμα που συναντώνται σε μη-spam μηνύματα. [25] Τα μηνύματα που έχουν σκορ που υπερβαίνει το ανώτατο όριο χαρακτηρίζονται ως spam.

Το θεώρημα του Bayes δίνεται από τον παρακάτω τύπο:

$$\Pr(S|W) = \frac{\Pr(W|S) \cdot \Pr(S)}{\Pr(W|S) \cdot \Pr(S) + \Pr(W|H) \cdot \Pr(H)}$$

Ας υποθέσουμε ότι ένα ύποπτο μήνυμα περιέχει τη λέξη "replica". [42] Οι περισσότεροι άνθρωποι που είναι συνηθισμένοι στην αναγνώριση e-mail, θα ξέρουν ότι το μήνυμα αυτό είναι πιθανό να είναι spam και ίσως προσπαθεί να πουλήσει πλαστά αντίγραφα

από γνωστές μάρκες ρολογιών. Το λογισμικό ανίχνευσης ανεπιθύμητης αλληλογραφίας όμως, δεν "ξέρει" να αναγνωρίσει το μήνυμα με αυτό τον τρόπο και έτσι υπολογίζει πιθανότητες με τον τύπο του Bayes. Πιο συγκεκριμένα, με βάση τον παραπάνω τύπο για το παράδειγμα αυτό θα ισχύει:

$\Pr(S|W)$: η πιθανότητα ένα μήνυμα να είναι spam, δεδομένου ότι η λέξη «replica» βρίσκεται σε αυτό

$\Pr(S)$: η συνολική πιθανότητα κάθε δεδομένου μηνύματος να είναι spam

$\Pr(W|S)$: η πιθανότητα της λέξης «replica» να εμφανίζεται σε μηνύματα spam

$\Pr(H)$: η συνολική πιθανότητα κάθε δεδομένου μηνύματος να μην είναι spam

$\Pr(W|H)$: η πιθανότητα η λέξη «replica» να εμφανίζεται σε μηνύματα που δεν είναι spam

Όπως και σε κάθε άλλη τεχνική φιλτραρίσματος ανεπιθύμητων μηνυμάτων, τα e-mail που χαρακτηρίζονται ως spam μπορούν στη συνέχεια να μετακινηθούν αυτόματα στον φάκελο "Junk" (Ανεπιθύμητα) ή και να διαγραφούν εντελώς. [24] Κάποια λογισμικά συστήματα εφαρμόζουν μάλιστα μηχανισμούς απομόνωσης των email που ορίζουν ένα χρονικό διάστημα κατά το οποίο ο χρήστης έχει τη δυνατότητα να επανεξετάσει την απόφαση του λογισμικού και να δράσει αναλόγως.

Ορισμένα φίλτρα spam συνδυάζουν τα αποτελέσματα του φιλτραρίσματος Bayesian και άλλων ευρετικών μεθόδων με αποτέλεσμα την ακόμη μεγαλύτερη ακρίβεια φιλτραρίσματος.

Signature – Based Filtering

Τα signature – based φίλτρα λειτουργούν συγκρίνοντας τα εισερχόμενα e-mail των χρηστών με γνωστά spams. [26] Για να ελέγξουν αν δύο μηνύματα είναι τα ίδια, τα συστήματα αυτά υπολογίζουν τις "υπογραφές" τους. Ένας τρόπος για να υπολογίσουν την υπογραφή ενός μηνύματος ηλεκτρονικού ταχυδρομείου, είναι να δίνουν έναν αριθμό σε κάθε χαρακτήρα και στη συνέχεια να προσθέτουν όλους τους αριθμούς αυτούς. Η τεχνική βασίζεται στο γεγονός ότι είναι σχεδόν αδύνατο δύο διαφορετικά e-mail να έχουν ακριβώς τις ίδιες υπογραφές.

Ο τρόπος να επιτεθεί κανείς σε ένα φίλτρο signature-based είναι να προσθέσει τυχαία περιεχόμενο σε κάθε αντίγραφο του spam, για να του δώσει μια ξεχωριστή υπογραφή. Συχνά το περιεχόμενο αυτό εμφανίζεται ως τυχαίοι χαρακτήρες στη γραμμή θέματος του μηνύματος, οι οποίοι βρίσκονται εκεί για να ξεγελάσουν τα φίλτρα αυτά. Οι spammers είχαν πάντα το πάνω χέρι στη μάχη κατά των φίλτρων signature-based. Μόλις οι προγραμματιστές των φίλτρων καταλαβαίνουν πώς να αγνοήσουν ένα είδος τυχαίας εισαγωγής και το ενσωματώνουν στη δράση του φίλτρου, οι spammers στρέφονται σε μια καινούργια τεχνική. Έτσι, τα φίλτρα signature-based δεν είχαν ποτέ πολύ καλή απόδοση.

Clustering Techniques

Οι τεχνικές clustering εντοπίζουν ομάδες μηνυμάτων, στις οποίες τα μηνύματα είναι παρόμοια μεταξύ τους («συγγενή») ή διαφορετικά σε σχέση με μηνύματα από άλλες ομάδες, για να ταξινομήσουν τα μηνύματα ηλεκτρονικού ταχυδρομείου ως ανεπιθύμητα ή νόμιμα. [27] Δύο χαρακτηριστικά παραδείγματα τεχνικών clustering που έχουν εφαρμοστεί για την ταξινόμηση spam είναι η τεχνική K-nearest neighbors (KNN) και η density-based clustering.

Η μέθοδος K-nearest neighbors (KNN) είναι ίσως η πιο απλή μέθοδος μεταξύ όλων των machine learning αλγορίθμων. Ο αλγόριθμος KNN ομαδοποιεί και μετατρέπει τα μηνύματα ηλεκτρονικού ταχυδρομείου σε ένα διάνυσμα πολλών διαστάσεων και στη συνέχεια μετρά την απόσταση μεταξύ των διανυσμάτων του κάθε e-mail. Οι ομάδες αποτελούνται από γειτονικά, δηλαδή σχετικά κοντινά διανύσματα. Μόλις οι συστάδες διαμορφωθούν η ταξινόμηση spam χρειάζεται να γίνει μόνο για ένα υποσύνολο κάθε ομαδικού συμπλέγματος, καθώς το αποτέλεσμα μπορεί στη συνέχεια να εφαρμοστεί και για τα άλλα μέλη του συμπλέγματος.

Το density-based clustering είναι μία άλλη μορφή ομαδοποίησης μηνυμάτων που έχει επίσης εφαρμοστεί για ταξινόμηση spam. [17] Παρά το γεγονός ότι τα περισσότερα συμβατικά φίλτρα spam χρησιμοποιούν διανύσματα για την αναπαράσταση των δεδομένων, η μέθοδος αυτή χρησιμοποιεί την πυκνότητα του χώρου ως το βασικό στοιχείο για να διακρίνει τα spam από τα υπόλοιπα e-mails. Για την ακρίβεια, μετράει τον αριθμό των παρόμοιων e-mails. Με την καταμέτρηση του αριθμού παρόμοιων

μηνυμάτων, μπορεί να εκτιμηθεί η τοπική πυκνότητα του εγγράφου. Οι spammers προωθούν ενέργειες μάρκετινγκ, εμπορίου ή ακόμη και ανήθικο περιεχόμενο στέλνοντας ένα τεράστιο ποσό spam καθημερινά. Οι ποσότητες αυτές των μηνυμάτων είναι τόσο μεγάλες, δεδομένου ότι αυτός είναι ο μόνος τρόπος για να λάβουν αρκετό οικονομικό όφελος. Υπάρχει, συνεπώς, μια τεράστια ανισοκατανομή στην κυκλοφορία e-mail, καθιστώντας την πυκνότητα χώρου έναν καλό δείκτη για τον εντοπισμό spam. Παρά το γεγονός ότι οι απλοί χρήστες σπάνια στέλνουν περισσότερα από 1000 παρόμοια e-mails, οι spammers σχεδόν πάντα στέλνουν πολύ περισσότερα spam από αυτά.

3.3.2.3 Social networks – Based Filters

Υπάρχουν πολλές social networks – based τεχνικές που χρησιμοποιούνται για την καταπολέμηση των spam. [27] Όλες αυτές οι μέθοδοι στοχεύουν στο να αποδώσουν σε κάθε μήνυμα μια πιθανότητα του να είναι spam, με βάση το ιστορικό των συμμετεχόντων. Τα social filters ταξινομούνται σε implicit και explicit.

Τεχνικές implicit: Τα social φίλτρα χρησιμοποιούνται για να αναλύσουν τα πεδία των μηνυμάτων ηλεκτρονικού ταχυδρομείου όπως οι επικεφαλίδες «Προς» (“To”) και «Κοιν.» (“Cc”), για να χτίσουν ένα γράφημα κοινωνικών σχέσεων των χρηστών και να μπορούν να ταξινομούν τα νέα μηνύματα βάσει αυτού του γραφήματος. [27] Η Promail είναι ένα χαρακτηριστικό παράδειγμα τέτοιας τεχνικής. Τόσο η Promail, όσο και οι υπόλοιπες σχετικές τεχνικές κατασκευάζουν ένα γράφημα κοινωνικού δικτύου με e-mail που διέρχονται μέσω ενός SMTP διακομιστή, χρησιμοποιώντας στοιχεία που συλλέγονται από αρχεία καταγραφής (log files). Τυπικά, οι κόμβοι στο γράφημα αντιπροσωπεύουν λογαριασμούς ηλεκτρονικού ταχυδρομείου, ενώ οι ακμές αντιπροσωπεύουν συναλλαγές e-mail. Οι γραφικές αυτές παραστάσεις χρησιμοποιούνται για να δώσουν απαντήσεις σχετικά με το αν ένα μήνυμα προέρχεται από μία πηγή κοινωνικού δικτύου του παραλήπτη και κατά συνέπεια κρίνουν αν το μήνυμα αυτό έχει πιθανότητες να είναι νόμιμο ή όχι.

Τεχνικές explicit: Σε αντίθεση με τις implicit τεχνικές, υπάρχουν μέθοδοι που χτίζουν ρητά το κοινωνικό δίκτυο μέσω της αλληλεπίδρασης με το χρήστη και μπορεί επίσης να

χρησιμοποιούν περιεχόμενο από το χρήστη. [27] Αυτές οι μέθοδοι είναι φυσικά συμπληρωματικές με τις whitelists και τα συστήματα challenge - response.

3.3.2.4 Traffic Analysis – Based Filters

Το φιλτράρισμα με βάση την ανάλυση της κίνησης μπορεί χρησιμοποιηθεί από τον mail server του ISP [15]. [55] Εδώ τα αρχεία καταγραφής (log files) του SMTP server μπορούν να χρησιμοποιηθούν για την ανίχνευση ανωμαλιών στην κανονική ροή της κυκλοφορίας. Οι ανωμαλίες που μπορεί να εμφανίζονται και να προδώσουν το spam, είναι ανωμαλίες στο χρόνο σύνδεσης με τον server, ανωμαλίες σε σχέση με την ποσότητα της αλληλογραφίας που προέρχεται από ένα συγκεκριμένο αποστολέα, το γεγονός ότι ένα μήνυμα έχει σταλεί σε περισσότερους από έναν παραλήπτες από συγκεκριμένο αποστολέα ή το γεγονός ότι η αλληλογραφία αναμεταδίδεται. Η πιο κοινή παραδοχή που χρησιμοποιείται για να εντοπίσει τα spam, είναι να προσδιοριστεί πότε ένας κεντρικός υπολογιστής ή δίκτυο εκδίδει μια ασυνήθιστα μεγάλη ποσότητα του μηνυμάτων. Ωστόσο, η τεχνική αυτή καταλήγει σε ένα πολύ υψηλό ποσοστό false positives.

Mail - Volume Based Filters

Τα φίλτρα αυτά χρησιμοποιούν έναν αλγόριθμο που ελέγχει πόσα μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται από ένα συγκεκριμένο υπολογιστή κατά τη διάρκεια των τελευταίων συνδέσεών του. [28] Εάν το ποσό αυτό ξεπερνά ένα ορισμένο όριο, τότε το μήνυμα ταξινομείται ως spam. Όταν το φίλτρο δρα εξατομικευμένα, μπορεί να έχει μία ικανοποιητική απόδοση.

[15] ISP: Ο internet service provider (ISP) είναι ένας οργανισμός που παρέχει υπηρεσίες για την πρόσβαση, τη χρήση ή τη συμμετοχή στο Διαδίκτυο. Οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να έχουν οργανωθεί σε διάφορες μορφές, όπως εμπορικές, μη κερδοσκοπικές, κοινοτικού χαρακτήρα ή ιδιόκτητες.

3.3.2.5 Άλλοι τύποι φίλτρων

Collaborative Filtering

Το collaborative filtering βασίζεται σε μία κοινοτική προσέγγιση για την καταπολέμηση των spam, συλλέγοντας τις εισροές από τα εκατομμύρια των χρηστών e-mail σε όλο τον κόσμο. Η φύση των spam είναι τέτοια που κάθε μήνυμα τυπικά αποστέλλεται σε τεράστιο αριθμό αποδεκτών. [20] Οι πιθανότητες λένε ότι ένας συγκεκριμένος παραλήπτης δεν είναι ο πρώτος που λαμβάνει ένα συγκεκριμένο μήνυμα. Είναι πιθανό το μήνυμα αυτό όχι μόνο να έχει ληφθεί, αλλά και να έχει αναγνωριστεί ως spam από κάποιον άλλο παραλήπτη. Το collaborative spam filtering είναι η διαδικασία της σύλληψης, καταγραφής και υποβολής της κρίσης του χρήστη σε σχέση με ένα μήνυμα. Οι χρήστες των συστημάτων αυτών μπορούν να ορίζουν τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου τους ως νόμιμα ή spam και αυτοί οι συμβολισμοί καταγράφονται σε μια κεντρική βάση δεδομένων. Αν και εφόσον ένας ορισμένος αριθμός χρηστών επισημάνει ένα συγκεκριμένο μήνυμα ηλεκτρονικού ταχυδρομείου ως ανεπιθύμητη αλληλογραφία, το φίλτρο αποκλείει αυτόματα την αποστολή του στα υπόλοιπα μέλη της κοινότητας.

Τα false positive και τα false negative της συγκεκριμένης προσέγγισης εξαρτώνται τόσο από ανθρώπινους, όσο και από τεχνικούς παράγοντες που περιορίζουν την επικαιρότητα, την πληρότητα και την ακρίβεια της όλης διαδικασίας. [20] Η πληρότητα της προσέγγισης περιορίζεται από τον αριθμό των χρηστών που συμμετέχουν στο σύστημα αυτό, ως εκ τούτου, δε μετράει ο αριθμός των μηνυμάτων που αποστέλλονται από τον αποστολέα, αλλά ο αριθμός των μηνυμάτων που αποστέλλονται από τον αποστολέα σε έναν συμμετέχοντα του collaborative αυτού φίλτρου. Οι συμμετέχοντες μπορεί να μην καταφέρουν να αναγνωρίσουν ένα μήνυμα ως spam ή να μην μπουν στον κόπο να καταγράψουν τις αποφάσεις τους. Οι συμμετέχοντες πιθανολογείται επίσης να σηματοδοτήσουν ακούσια μηνύματα που δεν είναι spam ως spam, ενώ κακόβουλοι χρήστες - ίσως και οι ίδιοι οι spammers - μπορεί να το κάνουν αυτό σκόπιμα, για να αυξήσουν το ποσοστό false positives και να θέσουν σε κίνδυνο την αποτελεσματικότητα του συστήματος.

Ένα απαραίτητο στοιχείο του collaborative spam filtering θα ήταν μια βάση δεδομένων σε πραγματικό χρόνο, που να περιέχει τα αναγνωρισμένα ως spam μηνύματα και να μπορεί να ενημερώνεται και να χρησιμοποιείται από διαφορετικούς χρήστες. [20] Φυσικά υπάρχουν

πρακτικά ζητήματα τα οποία καθιστούν αδύνατη την αποθήκευση ολόκληρων μηνυμάτων σε μία τέτοια βάση δεδομένων, όπως είναι ο τεράστιος όγκος της, ο μεγάλος χρόνος ενημέρωσής της, καθώς και η εμπιστευτικότητα των μηνυμάτων που θα μπορούσε να τεθεί σε κίνδυνο.

DNS Lookup Systems

Αν και δεν είναι μια ιδιαίτερα αξιόπιστη μέθοδος από μόνη της, πολλές anti-spam μέθοδοι χρησιμοποιούν το σύστημα domain names (DNS), για τον εντοπισμό των spammers. [29] Το DNS MX (Mail Exchange) προσπαθεί να επιβεβαιώσει ότι το domain name στην ηλεκτρονική διεύθυνση του αποστολέα - το τμήμα μετά το σύμβολο (@) - υπάρχει. Αυτό επιτυγχάνεται με την αναζήτηση στο σύστημα domain names για να δούμε αν το domain name έχει έγκυρη εγγραφή MX, η οποία υποδηλώνει την παρουσία ενός υπαρκτού mail server. Αν δεν υπάρχει αντιστοιχία, το πρόγραμμα anti-spam υποθέτει ότι το μήνυμα είναι spam. Το φίλτρο θα εκτελέσει επίσης μια αντίστροφη αναζήτηση DNS (reverse DNS lookup) χρησιμοποιώντας τη διεύθυνση IP από το mail server που έστειλε το αμφισβητήσιμο μήνυμα. Αυτή η αναζήτηση θα αποκαλύψει το domain name που συνδέονταν με τον server.

Ενώ τα DNS lookups μπορεί να είναι χρήσιμα στο ξερίζωμα μηνυμάτων ηλεκτρονικού ταχυδρομείου από spammers που προσπαθούν να μεταμφιεστούν, δεν είναι τόσο αποτελεσματικά ή αξιόπιστα από μόνα τους (σε σύγκριση με άλλες μεθόδους καταπολέμησης του spam) για τη γενικότερη διακοπή ανεπιθύμητης αλληλογραφίας. [29] Ειδικότερα, τα reverse DNS lookups έχουν γίνει γνωστά για την παραγωγή false positives, δεδομένου ότι είναι τεχνικά δυνατό για τους νόμιμους αποστολείς να μπορούν να στείλουν e-mail από ένα domain name διαφορετικό από το δικό τους.

Payment – Based Approach

Οι spammers στέλνουν ένα τεράστιο αριθμό spam καθημερινά, ακριβώς γιατί πέρα από το χρόνο που δαπανούν στη διαδικασία, δε χρειάζεται να ξοδέψουν τίποτα. [30] Έτσι, η προσέγγιση payment βασίζεται στο αντικίνητρο του κέρδους από τα spam. Προκειμένου να επιτευχθεί ο σκοπός αυτός, οι e-mail servers απαιτούν μία ενδεικτική πληρωμή για να παραδοθεί το e-mail στους αποδέκτες.

Βέβαια η πληρωμή μπορεί να μην αναφέρεται συγκεκριμένα σε πραγματικό νόμισμα, αλλά σε κόστος με την έννοια της απώλειας πολύτιμου χρόνου. [30] Υπάρχει ένα είδος συστήματος που απαιτεί από τους αποστολείς να ξοδέψουν υπολογιστικό κόστος. Το σύστημα αυτό πληρωμής ονομάζεται proof-of-work. Τέτοια συστήματα είναι και τα hashcash και Penny Black. Για παράδειγμα, η Hashcash είναι μια μέθοδος για την προσθήκη ενός κειμένου stamp (σφραγίδα) στην κεφαλίδα ενός μηνύματος ηλεκτρονικού ταχυδρομείου για να αποδείξει ο αποστολέας έχει καταβάλει ένα μικρό ποσό χρόνου της CPU για τον υπολογισμό του stamp αυτού πριν από την αποστολή του e-mail. Με άλλα λόγια, όταν ο αποστολέας έχει δαπανήσει ένα ορισμένο χρονικό διάστημα για να δημιουργήσει τη σφραγίδα και να στείλει το μήνυμα ηλεκτρονικού ταχυδρομείου, είναι απίθανο να είναι spammer. Η θεωρία είναι ότι οι spammers, των οποίων το επιχειρηματικό μοντέλο βασίζεται στην ικανότητά τους να στέλνουν μεγάλο αριθμό e-mail με πολύ μικρό κόστος ανά μήνυμα, δεν μπορούν να αντέξουν αυτή την επένδυση σε κάθε επιμέρους κομμάτι των spam που στέλνουν. Ωστόσο, οι αποδέκτες μπορούν να ελέγξουν αν ο αποστολέας έχει κάνει μια τέτοια επένδυση και να χρησιμοποιήσουν τα αποτελέσματα για την περαιτέρω βελτίωση των φίλτρων ενάντια στα spam.

Συνδυασμός Φίλτρων

Η κάθε προσέγγιση φυσικά από αυτές που αναλύθηκαν παραπάνω, έχει πλεονεκτήματα και μειονεκτήματα. Οι προσεγγίσεις, οι οποίες συνδυάζουν διαφορετικές τεχνικές, όπως τα υβριδικά φίλτρα, φαίνονται να είναι οι πιο αποτελεσματικές λύσεις. Το SpamAssassin είναι μία τέτοια υβριδική μέθοδος φιλτραρίσματος που χρησιμοποιεί rule-based filters, content-based filters, Bayesian filtering, real-time DNS blacklists. [56] Η τεχνική αυτή χρησιμοποιείται σε πολλά πακέτα anti-spam φιλτραρίσματος. Ωστόσο, οι λύσεις αυτές πρέπει να σχεδιάζονται πολύ προσεκτικά, καθώς ο συνδυασμός πολλών μεθόδων μπορεί εκτός από την ασφάλεια και την ακρίβεια, να αυξάνει και την πολυπλοκότητα του χρόνου εκτέλεσης.

Βέβαια υπάρχουν και πολλές άλλες τέτοιες συνδυαστικές προσεγγίσεις. Σε γενικές γραμμές καμία από τις τεχνικές που περιεγράφηκαν σε αυτό το κεφάλαιο δεν είναι αρκετά αποτελεσματική, όταν χρησιμοποιείται από μόνη της. Τα πιο αποτελεσματικά φίλτρα spam χρησιμοποιούν συνδυασμό των παραπάνω τεχνικών για να βεβαιωθούν ότι το ποσοστό των spam στο inbox του χρήστη διατηρείται στο ελάχιστο δυνατό και ότι το ποσοστό false positives είναι επίσης ελάχιστο.

3.3.3 Τεχνικές για ερευνητές και για όργανα επιβολής του νόμου

Ολοένα και περισσότερο, οι anti-spam προσπάθειες έχουν οδηγήσει σε συντονισμό μεταξύ των αρχών επιβολής του νόμου, ερευνητών, χρηματοπιστωτικών υπηρεσιών και παρόχων υπηρεσιών Διαδικτύου για την παρακολούθηση και τον εντοπισμό spam e-mail, έτσι ώστε να εντοπίζονται περιστατικά κλοπής ταυτότητας, phishing, αλλά και να συλλέγονται αποδεικτικά στοιχεία για ποινικές υποθέσεις. [15]

Νομοθεσία: Η τεράστια και ποικιλόμορφη ζημία που προκαλείται από τα spam, συμπεριλαμβανομένων των οικονομικών απωλειών και της παραβίασης των νόμων με τη μετάδοση απαγορευμένου υλικού, έχει κατά καιρούς οδηγήσει στην ανάγκη για άμεση νομοθετική ανταπόκριση. [15] Η εφαρμογή της κατάλληλης νομοθεσίας μπορεί να έχει σημαντικές επιπτώσεις στη δραστηριότητα spamming. Οι διατάξεις περί κυρώσεων του Australian Spam Act του 2003 μείωσαν την κατάταξη της Αυστραλίας στον κατάλογο των spam παγκοσμίως από τη δέκατη στην εικοστή όγδοη θέση. Η νομοθεσία που παρέχει εντολές που πρέπει να ακολουθούν οι αποστολείς μαζικών μηνυμάτων, καθιστά τον εντοπισμό και το φιλτράρισμα των spam ευκολότερο. Βέβαια, το κύριο πράγμα που χρειάζεται οπωσδήποτε είναι οι νόμοι αυτοί κατά του spam να εφαρμόζονται. Σε πολλά κράτη υπάρχει αφθονία νόμων κατά του spam, που φαίνεται να μην έχουν καμία επίδραση.

Ανάλυση των spamvertisements [16]: Η ανάλυση των σελίδων που είναι spamvertised, συχνά οδηγεί ακόμη και στην οριστική διαγραφή domain names. [15] Οι spamvertisers εισάγουν συνδέσμους στις ιστοσελίδες τους (συνήθως, σελίδες που πωλούν κάποιο εμπορικό προϊόν) και προσθέτουν λέξεις-κλειδιά κοινών ή σχετικών αναζητήσεων. Ο προφανής στόχος είναι οι μηχανές αναζήτησης να βρουν τη «βανδαλισμένη» σελίδα που είναι γεμάτη με συνδέσμους και να βελτιώσουν τη δημοτικότητα της σελίδας αυτής. Αυτό συνήθως γίνεται με αυτοματοποιημένα προγράμματα επεξεργασίας που μοιάζουν με πεδία κειμένου σε φόρμες στο Διαδίκτυο και συμπληρώνονται αυτόματα με διαδικτυακούς συνδέσμους. Οι σύνδεσμοι συνήθως

[16] spamvertisement: πρακτική αποστολής spam e-mail για διαφήμιση ιστοσελίδων. Η λέξη προέρχεται από τις λέξεις spam και advertising. Αναφέρεται επίσης σε βανδαλισμούς blogs, online forums ή wikis με υπερσυνδέσμους, προκειμένου οι σελίδες τους να αποκτήσουν μια υψηλότερη κατάταξη στις μηχανές αναζήτησης.

οδηγούν σε χάπια, πορνό και σελίδες πόκερ κ.α.. Οι περισσότεροι νόμιμοι πάροχοι ιστοσελίδων δεν ανέχονται αυτή την πρακτική και διαγράφουν οποιοδήποτε site έχει γίνει spamvertised. Η πρακτική αυτή έχει οδηγήσει πολλά επεξεργάσιμα πεδία που υπάρχουν online να απασχολούν anti-spam αντίμετρα, συμπεριλαμβανομένης της χρήσης captchas για την αποφυγή αυτοματοποιημένων μοντάζ.

Συμπεριφορική ασφάλεια: Υπάρχουν πολλά spam filters που έχουν ενσωματώσει στη λειτουργία τους τεχνικές που χρησιμοποιούν συνήθως τα όργανα επιβολής του νόμου για ανάλυση της συμπεριφοράς ενός ατόμου. [31] Οι τεχνικές αυτές παρατηρούν τη γλώσσα του σώματος ενός ατόμου, τις εκφράσεις του προσώπου, τα λόγια και τις ενέργειές του για να προσπαθήσουν να προσδιορίσουν αν η πρόθεση του ατόμου είναι κακόβουλη ή καλοήθης. Για παράδειγμα, οι κινήσεις των ματιών, η φωνή καθώς και άλλοι παράγοντες μπορεί να δείξουν άγχος, το οποίο με τη σειρά του μπορεί να υποδηλώνει ότι ένα άτομο προσπαθεί να κρύψει κάτι.

Η ασυντόνιστη δράση μπορεί να μην είναι αποτελεσματική, δεδομένου του σημερινού όγκου των spam και του ρυθμού με τον οποίο οι εγκληματικές οργανώσεις δηλώνουν νέα domains. Ωστόσο, μια συντονισμένη προσπάθεια, που υλοποιείται με την κατάλληλη υποδομή, μπορεί να δώσει πολύ καλά αποτελέσματα στην καταπολέμηση των spam.

Κεφάλαιο 4
Συγκριτική Μελέτη Anti-spam Methods

Το ιδανικό φίλτρο spam θα αναγνώριζε αυτόνομα, άμεσα και χωρίς λάθη τα μηνύματα spam ως spam και τα μη-spam ως μη-spam. [20] Έτσι, για να αξιολογήσουμε ένα φίλτρο spam, θα πρέπει κατά κάποιο τρόπο να μετρήσουμε πόσο στενά προσεγγίζει τα ιδανικά αυτά. Επιπλέον, η μέτρηση της αποτελεσματικότητας ενός φίλτρου, θα πρέπει να αντικατοπτρίζει την καταλληλόλητα του φίλτρου για το σκοπό τον οποίο προορίζεται.

Κάθε μία από τις προσεγγίσεις για την ασφάλεια των χρηστών από τα spam που περιεγράφηκαν στο προηγούμενο κεφάλαιο, έχει τα πλεονεκτήματα και τα μειονεκτήματά της. Όλες μπορεί να οδηγήσουν σε false positives ή false negatives. Η κάθε προσέγγιση λειτουργεί καλύτερα για διαφορετικές καταστάσεις. Βέβαια, το αποτελεσματικό φιλτράρισμα ανεπιθύμητων μηνυμάτων επιτυγχάνεται από συνδυασμό των τεχνικών αυτών.

4.1 Ανάλυση Συγκριτικών Αποτελεσμάτων

Στο κεφάλαιο αυτό δίνονται αναλυτικά τα βασικά πλεονεκτήματα και μειονεκτήματα των συνηθέστερων μεθόδων spam filtering, ενώ στο τέλος παρατίθεται συγκεντρωτικός πίνακας με όλες τις μεθόδους του περιεγράφηκαν στο προηγούμενο κεφάλαιο και τα αντίστοιχα πλεονεκτήματα και μειονεκτήματά τους επιγραμματικά.

Blacklists

Το blacklisting χρησιμοποιείται για να προστατέψει τους χρήστες από ηλεκτρονικές διευθύνσεις ή domain names που είναι γνωστά για την αποστολή spam. [32] Το στοιχείο αυτό που καθιστά τις blacklists βοηθητικές είναι ότι μπλοκάρουν οποιουσδήποτε spammers είναι δηλωμένοι στις λίστες, οπότε και ο χρήστης δεν παραλαμβάνει μηνύματα από αυτούς.

Ένα κοινό πρόβλημα με τις blacklists είναι η επισήμανση μηνυμάτων από νόμιμους αποστολείς που αναφέρθηκαν ή προστέθηκαν στη λίστα, όχι επειδή είναι spammers, αλλά από δόλο. [31] Μερικά άτομα και οργανώσεις έχουν διαπιστώσει ότι είναι πολύ δύσκολο να αφαιρέσουν τις διευθύνσεις τους από τις blacklists από τη στιγμή που έχουν καταγραφεί εκεί. Αυτοί που ελέγχουν τις ευρέως κατανεμημένες blacklists, έχουν μεγάλη ευθύνη να εξασφαλίζουν ότι στις λίστες δε βρίσκονται αθώα άτομα και οργανώσεις, που έχουν μπει εκεί είτε κατά λάθος είτε εσκεμμένα. Ένα άλλο πρόβλημα με τις blacklists είναι ότι λειτουργούν μόνο εναντίον γνωστών ανεπιθύμητων αποστολέων, προγραμμάτων και οργανώσεων και δεν προστατεύουν κατά των νέων απειλών. Εκτός αυτού η σάρωση της εισερχόμενης κίνησης και η σύγκρισή της με τις blacklists μπορεί να χρησιμοποιήσει σημαντικούς πόρους του συστήματος και να επιβραδύνει την κίνηση του δικτύου. Τέλος, άλλο ένα σημαντικό μειονέκτημα των λιστών αυτών είναι η συντήρησή τους. [32] Το Διαδίκτυο δεν έχει όρια και χιλιάδες νέες θέσεις προστίθενται καθημερινά, ενώ οι spammers διαρκώς αλλάζουν τις ταυτότητές τους για να μπορούν να δρουν ανενόχλητοι. Το πρόβλημα με τις blacklists, είναι επομένως ο συνεχώς αυξανόμενος ρυθμός ανάπτυξής τους. Όπως άλλωστε προαναφέρθηκε, όσο μεγαλύτερη γίνεται η λίστα, τόσο πιο απαιτητικές είναι οι διαδικασίες που απαιτούνται για τον έλεγχό της.

Whitelists

Οι whitelists προσδιορίζουν τα άτομα από τα οποία ο χρήστης επιθυμεί να δέχεται e-mail, όπως φίλους, οικογένεια και άλλες επαφές. [33] Είναι σαφές ότι το μέγεθος του συνόλου των ανθρώπων από τους οποίους θέλουμε να δεχόμαστε μηνύματα είναι πολύ μικρότερο και διαχειρίσιμο από ό, τι το σύνολο των ανθρώπων που δεν εγκρίνουμε ως αποστολείς. Το βασικό πλεονέκτημα των whitelists είναι ότι εξασφαλίζουν την παραλαβή e-mail από αποστολείς τους οποίους έχουμε δηλώσει ότι θεωρούμε νόμιμους.

Παρόλα αυτά, οι whitelists δεν έχουν αποκτήσει μεγάλη αποδοχή ως τρόπος για να μειωθούν τα spam. Τα δύο βασικά μειονεκτήματά τους είναι αφενός η διατήρησή τους που απαιτεί πολύ δουλειά από το χρήστη και αφετέρου το γεγονός ότι βασίζονται σε πιστοποιημένες διευθύνσεις και πλέον πολύ λίγες διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι πιστοποιημένες.

Η δημοτικότητα του whitelisting ολοένα και αυξάνεται, ενώ πλέον χρησιμοποιείται συχνά και σε συνδυασμό με άλλες μεθόδους ασφάλειας. [31] Για παράδειγμα, πολλοί πάροχοι υπηρεσιών ηλεκτρονικού ταχυδρομείου περιλαμβάνουν φίλτρα spam που αναλύουν τα μηνύματα και τα σηματοδοτούν ως spam βάσει ορισμένων κριτηρίων (λέξεις-κλειδιά, μορφοποίηση, επανάληψη, κ.λπ.). Εντούτοις, επιτρέπουν στους χρήστες να συγκεντρώνουν τους ασφαλείς αποστολείς σε whitelists, έτσι ώστε τα mail από αυτές τις διευθύνσεις να μην επισημαίνονται ως spam, ακόμη και αν ικανοποιούν τα κριτήρια αυτά.

Greylists

Το greylisting είναι μία μέθοδος υπεράσπισης των χρηστών από τα spam, κατά την οποία ένας mail transfer agent (MTA [17]) προσωρινά απορρίπτει κάθε e-mail από αποστολείς που δεν αναγνωρίζει. [34] Αν το e-mail είναι νόμιμο ο server μετά από μια καθυστέρηση, προσπαθεί ξανά και εφόσον έχει παρέλθει επαρκής χρόνος, το μήνυμα γίνεται δεκτό.

[17] MTA: πρόγραμμα υπεύθυνο για τη λήψη εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου και την παράδοση των μηνυμάτων σε μεμονωμένους χρήστες - μεταφέρει μηνύματα μεταξύ των υπολογιστών.

Το κύριο πλεονέκτημα των greylists είναι το γεγονός ότι εξαλείφουν τα περισσότερα ανεπιθύμητα μηνύματα, ενώ παράλληλα δίνουν στα νόμιμα e-mail την ευκαιρία να περάσουν στα εισερχόμενα ενός χρήστη. Εκτός αυτού όχι μόνο δεν απαιτούν ιδιαίτερες προσπάθειες διαμόρφωσης από την πλευρά του τελικού χρήστη, αλλά δεν έχουν και μεγάλες απαιτήσεις συντήρησης, αφού δεν είναι απαραίτητο ο χρήστης να διατηρεί χειροκίνητα λίστες διευθύνσεων IP, blacklists, whitelists ή word lists. Επιπλέον, έχουν το πλεονέκτημα ότι δεν αποτελούν πρόσθετη επιβάρυνση στους πόρους του υπολογιστή του τελικού χρήστη.

Το μεγαλύτερο μειονέκτημα των greylists είναι ότι για τους μη αναγνωρισμένους servers, καταστρέφουν τη σχεδόν στιγμιαία φύση των e-mail που οι χρήστες έχουν μάθει να περιμένουν. Τα e-mail από άγνωστους servers συνήθως καθυστερούν περίπου 15 λεπτά, ενώ μπορεί να καθυστερήσουν μέχρι και λίγες ημέρες. Ένας χρήστης greylisting δεν μπορεί πάντα να βασίζεται στην παραλαβή κάθε e-mail σε ένα προκαθορισμένο χρονικό διάστημα. Αυτό το μειονέκτημα μετριάζεται από το γεγονός ότι όταν ένας διακομιστής έχει αναγνωριστεί, τα κοντινά παραδοτέα μηνύματα επανέρχονται, δεν απαιτείται η διαδικασία της επαλήθευσης ξανά και γενικά η διαδικασία ανταλλαγής μηνυμάτων συνεχίζεται ομαλά εφόσον οι χρήστες συνεχίζουν να ανταλλάσσουν μηνύματα. Ωστόσο, το μειονέκτημα αυτό είναι ιδιαίτερα εμφανές όταν ένας χρήστης του greylisting mailserver προσπαθεί συμπληρώσει τα διαπιστευτήριά του σε μια ιστοσελίδα που χρησιμοποιεί e-mail επιβεβαίωσης για να επαναφέρει τους κωδικούς πρόσβασης. Σε ακραίες περιπτώσεις, η καθυστέρηση παράδοσης που επιβάλλεται από την greylist μπορεί να υπερβεί το χρόνο λήξης του διακριτικού επαναφοράς κωδικού πρόσβασης που παραδίδεται με e-mail. Σε αυτές τις περιπτώσεις μπορεί να απαιτείται χειροκίνητη παρέμβαση στη whitelist του mailserver, έτσι ώστε να μπορεί να χρησιμοποιηθεί το e-mail που περιέχει το διακριτικό επαναφοράς πριν από τη λήξη του.

Challenge – Response Filtering

Όταν ο χρήστης λαμβάνει ένα e-mail από κάποιον που δεν είχε πάρει e-mail ξανά πριν, το challenge-response φίλτρο στέλνει ένα e-mail πίσω στον αποστολέα, ενημερώνοντάς τον ότι πρέπει να συμπληρώσει μια φόρμα με περαιτέρω στοιχεία ή ότι με κάποιο άλλο τρόπο πρέπει να αποκριθεί, πριν το e-mail παραδοθεί. [26] Τα φίλτρα αυτά υπολογίζεται να «πιάνουν» το 99,9% των spam μηνυμάτων, παρουσιάζοντας όμως σημαντικά μειονεκτήματα έναντι άλλων μεθόδων που έχουν την ίδια απόδοση με ελάχιστα μειονεκτήματα.

Το πλεονέκτημα των φίλτρων πρόκλησης-απόκρισης είναι ότι αφήνουν πολύ λίγα spam να εισέλθουν στα εισερχόμενα του χρήστη. Το σύστημα διασφαλίζει ότι μηνύματα από έγκυρους αποστολείς μπορούν να περάσουν μέσα, ενώ η αυτοματοποιημένη μαζική αλληλογραφία των spammers θα απορριφθεί. Μόλις ένας αποστολέας περάσει την πρόκληση, ο αποστολέας προστίθεται στο whitelist του παραλήπτη με τους επιτρεπόμενους αποστολείς που δε θα χρειαστεί να αποδείξουν ξανά την εγκυρότητά τους αν επιχειρήσουν να στείλουν πάλι ένα μήνυμα στον ίδιο παραλήπτη.

Ωστόσο, το βασικό τους μειονέκτημα είναι ότι απαιτείται πολύ παραπάνω εργασία από τους αποστολείς μηνυμάτων, οι οποίοι σε περίπτωση που είναι νόμιμοι πρέπει να χάσουν χρόνο άδικα για να προβούν στην επαλήθευση του e-mail τους. Ένα άλλο μειονέκτημα των φίλτρων αυτών είναι ότι ένα μεγάλο μέρος νόμιμων e-mail είτε θα χαθεί, είτε θα καθυστερήσει τόσο πολύ να φθάσει που δεν θα είναι πλέον χρήσιμο.

Rule-Based (Heuristic) Filtering

Η απόδοση των rule-based φίλτρων ποικίλλει σημαντικά από φίλτρο σε φίλτρο, με υπολογισμούς που τα θέλουν να αναγνωρίζουν το 90-95% των spam μηνυμάτων επιτυχώς. [26] Η απλούστερη μορφή τους, απλά απορρίπτει κάθε e-mail που περιέχει ορισμένες "κακές" λέξεις. Ωστόσο, η μέθοδος αυτή όχι μόνο είναι πολύ εύκολο να νικηθεί από τους spammers, αλλά τείνει επίσης να απορρίπτει νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου. Από την άλλη πλευρά, ορισμένα εξελιγμένα φίλτρα βασισμένα στη rule-based τεχνική, όπως το Spamassassin, μπορούν να είναι αρκετά αποτελεσματικά. Το Spamassassin (όπως και παρόμοια τέτοια εργαλεία) αξιολογεί μεγάλο αριθμό προτύπων - ως επί το πλείστον εκφράσεων – σε ένα υποψήφιο μήνυμα. Μερικά προκαθορισμένα πρότυπα προσθέτουν πόντους στο «σκορ» ενός μηνύματος, ενώ άλλα αφαιρούν από αυτό. Αν η βαθμολογία ενός μηνύματος υπερβαίνει ένα ορισμένο όριο, το μήνυμα φιλτράρεται ως spam, αλλιώς θεωρείται νόμιμο. Ένα καλό rule-based φίλτρο σαν αυτό υπολογίζεται να πιάνει το 90-95% των σημερινών spam. Το σημαντικό πλεονέκτημα των φίλτρων αυτών έναντι των απλών rule-based φίλτρων είναι η εύκολη εγκατάσταση και αρχικοποίησή τους.

Το κύριο μειονέκτημα των rule-based φίλτρων είναι ότι τείνουν να έχουν υψηλά ποσοστά false positives - συχνά φθάνουν το 0,5% (το ποσοστό false positives ενός εκπαιδευμένου Bayesian

φίλτρου θα ήταν λιγότερο από το ένα δέκατο από αυτό). Ένα ακόμη μειονέκτημα των κανόνων αυτών είναι το γεγονός ότι είναι στατικοί. Όταν οι spammers μαθαίνουν νέα κόλπα, οι συγγραφείς των φίλτρων πρέπει να γράφουν νέους κανόνες για να τα πιάσουν. Και ακριβώς επειδή τα rule-based φίλτρα αποτελούν στατικούς στόχους, οι spammers μπορούν να συντονίσουν τα e-mail τους, έτσι ώστε να τα ξεπερνούν. Οι πιο εξελιγμένοι spammers δοκιμάζουν μάλιστα τα e-mail τους στα πιο δημοφιλή από αυτά τα φίλτρα πριν τα στείλουν. Στην πραγματικότητα, έχουν δημιουργηθεί ιστοσελίδες που το κάνουν αυτό δωρεάν.

Bayesian Filtering

Τα φίλτρα Bayesian υπολογίζουν την πιθανότητα ένα μήνυμα να είναι spam με βάση το περιεχόμενό του. [26] Σε αντίθεση με απλά content-based φίλτρα, η μέθοδος Bayesian μαθαίνει από τα spam και από τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου, με αποτέλεσμα να αποτελεί μια πολύ ισχυρή, προσαρμοστική και αποτελεσματική anti-spam προσέγγιση, η οποία δεν επιστρέφει σχεδόν καθόλου false positives.

Η μέθοδος Bayesian εντοπίζει περίπου το 99 με 99,9% των spam μηνυμάτων με σχετικά λίγα false positives συγκριτικά με τις άλλες μεθόδους, ποσοστό που την καθιστά την αποτελεσματικότερη anti-spam μέθοδο αυτή τη στιγμή. [26] Μάλιστα σε άρθρο του BBC το 2003 αναφέρεται ότι η μέθοδος Bayesian ανιχνεύει την ανεπιθύμητη αλληλογραφία σε ποσοστό 99.7% με πολύ χαμηλό αριθμό false positives. Τα κυριότερα πλεονεκτήματα της μεθόδου είναι τα παρακάτω:

- Η μέθοδος Bayesian λαμβάνει υπόψη ολόκληρο το μήνυμα και αναγνωρίζει τόσο τις λέξεις-κλειδιά που προσδιορίζουν τα spam, όσο και τις λέξεις που δηλώνουν έγκυρη αλληλογραφία. [35] Για παράδειγμα, δεν αποτελούν όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν τις λέξεις «free» (δωρεάν) και «cash» (μετρητά), spam. Το πλεονέκτημα της μεθόδου Bayesian είναι ότι βρίσκει τις πιο «ενδιαφέρουσες» λέξεις (σε σχέση με την απόκλισή τους από τη μέση τιμή) και ελέγχει την πιθανότητα το μήνυμα να είναι spam. Η Bayesian μέθοδος θα θεωρήσει τις λέξεις «free» και «cash» ενδιαφέρουσες, αλλά θα αναγνωρίσει επίσης το όνομα της επιχείρησης που έστειλε το μήνυμα και θα το κατατάξει αναλόγως ως νόμιμο ή όχι. Με άλλα λόγια, το φιλτράρισμα Bayesian είναι μια έξυπνη προσέγγιση, διότι εξετάζει όλες τις πτυχές ενός μηνύματος, σε αντίθεση με τον

έλεγχο για παράδειγμα των λέξεων-κλειδιά που ταξινομεί ένα μήνυμα ως spam με βάση μία και μόνο λέξη.

- Το φίλτρο Bayesian αυτοπροσαρμόζεται συνεχώς. [35] Εξελίσσεται και προσαρμόζεται στις νέες τεχνικές spam, μέσα από τα νέα spam και μέσω της έγκυρης εξερχόμενης αλληλογραφίας. Για παράδειγμα, όταν οι spammers άρχισαν να χρησιμοποιούν τη λέξη «f-r-e-e» αντί για «free» κατάφεραν να αποφεύγουν τον έλεγχο, μέχρι που η λέξη «f-r-e-e» προστέθηκε επίσης στη βάση δεδομένων λέξεων-κλειδιών. Εκτός αυτού, το φίλτρο Bayesian εντοπίζει αυτόματα τέτοιες τακτικές. Όταν δηλαδή βρίσκει τη λέξη «5ex» αντί για «Sex», οι πιθανότητες να θεωρηθεί το μήνυμα spam είναι μεγάλες, δεδομένου ότι είναι απίθανο να σταλεί με αυτή τη λανθασμένη σύνταξη σε ένα έγκυρο e-mail.
- Η τεχνική Bayesian είναι ευαίσθητη προς το χρήστη. [35] Μαθαίνει τις συνήθειες e-mail των εταιρειών και καταλαβαίνει ότι, για παράδειγμα, η λέξη «υποθήκη» μπορεί να σημαίνει spam, αν η εταιρεία είναι μία αντιπροσωπεία αυτοκινήτων, ενώ δε θα αναφερθεί ως spam αν η εταιρεία είναι ένα χρηματοπιστωτικό ίδρυμα που ασχολείται με υποθήκες.
- Η μέθοδος Bayesian είναι πολυγλωσσική και διεθνής. [35] Τα φίλτρα Bayesian, μπορούν να προσαρμόζονται και να χρησιμοποιούνται για κάθε γλώσσα που απαιτείται. Οι περισσότερες λίστες λέξεων-κλειδιών είναι διαθέσιμες μόνο στα αγγλικά και είναι ως εκ τούτου σχεδόν άχρηστες σε μη αγγλόφωνες περιοχές. Επιπλέον, το φίλτρο Bayesian λαμβάνει υπόψη τη διαφορετική χρήση ορισμένων λέξεων σε διάφορες περιοχές, ακόμη και αν ομιλείται η ίδια γλώσσα. Αυτή η νοημοσύνη της τεχνικής αυτής επιτρέπει τον εντοπισμό περισσότερων spam.
- Ένα φίλτρο Bayesian είναι δύσκολο να ξεγελαστεί, σε αντίθεση με ένα φίλτρο λέξεων κλειδιών. [35] Ένας έμπειρος spammer που θέλει να παραπλανήσει ένα φίλτρο Bayesian μπορεί να χρησιμοποιήσει είτε λιγότερες λέξεις που να το κατατάσσουν στα spam (όπως δωρεάν, μετρητά, κλπ.), ή περισσότερες λέξεις που να το καθιστούν έγκυρη αλληλογραφία (όπως ένα έγκυρο όνομα επαφής, κλπ.). Το τελευταίο είναι σχεδόν αδύνατο, αφού ο spammer θα πρέπει να γνωρίζει το προφίλ ηλεκτρονικού ταχυδρομείου για κάθε δικαιούχο, έχοντας συγκεντρώσει αυτό το είδος των πληροφοριών. Ο διαχωρισμός των λέξεων που σχετίζονται με τα spam, όπως για παράδειγμα η χρήση της λέξης «m-o-r-t-g-a-g-e» αντί για «mortgage», απλά θα αυξήσει την πιθανότητα το μήνυμα να θεωρηθεί spam, δεδομένου ότι ένας νόμιμος χρήστης σπάνια θα γράψει τη λέξη με αυτόν τον τρόπο.

Όπως όλες οι μέθοδοι, έτσι και η μέθοδος Bayesian έχει κάτι που θα μπορούσε να θεωρηθεί μειονέκτημα. [35] Για να μπορέσουμε να χρησιμοποιήσουμε και να κρίνουμε τα Bayesian

φίλτρα, θα πρέπει να περιμένουμε ένα μικρό χρονικό διάστημα μέχρι το φίλτρο να εκπαιδευτεί. Ωστόσο, με την πάροδο του χρόνου, το φίλτρο Bayesian γίνεται όλο και πιο αποτελεσματικό, δεδομένου ότι μαθαίνει περισσότερα για τις συνήθειες του χρήστη ή του οργανισμού στον οποίο είναι τοποθετημένο. Αυτό λοιπόν το στοιχείο είναι σημαντικό να λαμβάνεται υπόψη κατά τη διαδικασία αξιολόγησης των φίλτρων anti-spam.

Νομοθεσία

Υπολογίζεται ότι με την κατάλληλη νομοθεσία το ποσοστό των spam μπορεί να περιοριστεί μέχρι και κατά 80%, ωστόσο αν και είναι πολλά τα κράτη που έχουν θεσπίσει νόμους κατά της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, λίγα είναι εκείνα που τελικά τους εφαρμόζουν. [26] Το βασικό κενό στη νομοθεσία ενάντια στα spam βρίσκεται συνήθως στον ορισμό του spam. Οι περισσότεροι anti-spam νόμοι επιτρέπουν τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου σε παραλήπτες που έχουν κάποια προηγούμενη σχέση με τον αποστολέα. Αυτό είναι εύλογο, όμως θα πρέπει να καθοριστεί προσεκτικά τι είδους είναι αυτή η προηγούμενη σχέση. Υπάρχει μια ολόκληρη κατηγορία από spammers (που αποκαλούν τους εαυτούς τους "permission-based e-mail marketers"), οι οποίοι αγοράζουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από ιστοσελίδες με αδίστακτες πολιτικές προστασίας προσωπικών δεδομένων. Αποκαλώντας τα site από τα οποία αγόρασαν τη διεύθυνση του χρήστη ως «συνέταιρους», οι spammers ισχυρίζονται ότι έχουν μια προηγούμενη σχέση με το χρήστη και επομένως, απαλλάσσονται από τους anti-spam νόμους. Στην ενότητα 5.4 παρουσιάζονται αναλυτικά στοιχεία σχετικά με την αποτελεσματικότητα των anti-spam νόμων.

Filtering Method	Πλεονεκτήματα	Μειονεκτήματα
Blacklists	- Μπλοκάρει τα μηνύματα από γνωστές πηγές spam - Άμεσα διαθέσιμα σύνολα τέτοιων καταλόγων	- Πιθανότητα μπλοκαρίσματος αβλαβών μηνυμάτων - Χρειάζεται διαρκής ενημέρωση - Υψηλές απαιτήσεις πόρων του συστήματος και πιθανότητα επιβράδυνσης της κίνησης του δικτύου
Whitelists	- Εγγυάται την παράδοση μηνυμάτων από γνωστούς αποστολείς	- Η συντήρηση της λίστας μπορεί να μην είναι εύκολη - Δεν παραλαμβάνονται μηνύματα από διευθύνσεις που δεν είναι στη λίστα
Greylists	- Εξαλείφουν τα περισσότερα ανεπιθύμητα μηνύματα - Δεν απαιτούν ιδιαίτερες προσπάθειες διαμόρφωσης από την πλευρά του τελικού χρήστη - Μικρές απαιτήσεις συντήρησης - Χαμηλές απαιτήσεις πόρων συστήματος	- Καθυστέρηση στην παραλαβή e-mail

Filtering Method	Πλεονεκτήματα	Μειονεκτήματα
Realtime Blackhole Lists	- Απαιτούν λιγότερη συντήρηση από τους χρήστες σε σχέση με τις blacklists	- Μικρός έλεγχος του χρήστη σε σχέση με τα ονόματα στη λίστα - Σχετικά υψηλό ποσοστό false positives
DNS-based Blackhole lists (DNSBL)	- Πολύ χαμηλές απαιτήσεις πόρων του συστήματος - Συμπληρώνει άλλες μεθόδους spam filtering	- Σχετικά μικρό ποσοστό ανίχνευσης spam - Πιθανότητα υψηλού ποσοστού false positives
Challenge – Response Filtering	- Επιτρέπει στους νόμιμους αποστολείς να στείλουν μηνύματα αν αποκριθούν στην πρόκληση του συστήματος - Χαμηλές απαιτήσεις πόρων του συστήματος - Δύσκολο για τους spammers να το παρακάμψουν	- Προκαλεί καθυστερήσεις παράδοσης των μηνυμάτων - Δεν μπορεί να αντιμετωπίσει νόμιμα αυτοματοποιημένα μηνύματα, όπως τιμολόγια e-commerce, newsletters κ.α. - Διακρίσεις έναντι χρηστών με προβλήματα όρασης - Προκαλεί ενόχληση στου νόμιμους αποστολείς

Filtering Method	Πλεονεκτήματα	Μειονεκτήματα
Word – Based Filters	- Η τεχνική που βασίζεται στα συγκεκριμένα φίλτρα είναι σχετικά απλή	- Χρειάζεται μεγάλη προσπάθεια για την ανάπτυξη και τη διατήρηση των word lists - Παρακάμπτεται εύκολα με κόλπα όπως εναλλακτικές μορφές ορθογραφίας - Υψηλό ποσοστό false positives
Heuristic Filters	- Σε ορισμένες περιπτώσεις πολύ υψηλή ακρίβεια εύρεσης spam - Μέτριες απαιτήσεις πόρων του συστήματος	- Οι έλεγχοι πρέπει να ανανεώνονται συχνά, για να συμβαδίζουν με τις νέες τακτικές των spammers - Μπορεί να έχουν υψηλό ποσοστό false positives, αν οι κανόνες είναι κακώς γραμμένοι - Εύκολο να παρακαμφθεί από τους spammers
Bayesian Filtering	- Μεγάλη ακρίβεια στην εύρεση spam - Προσαρμόζεται στις νέες τακτικές των	- Χρειάζεται περισσότερη επεξεργαστική ισχύ από άλλες μεθόδους - Χρειάζεται περίοδος εκπαίδευσης για το

Filtering Method	Πλεονεκτήματα	Μειονεκτήματα
	spammers αυτόματα και τις χρησιμοποιεί ενάντιά τους - Χαμηλό ποσοστό false positives (όταν έχει εκπαιδευτεί σωστά) - Εύκολο στη χρήση χωρίς ιδιαίτερες παρεμβάσεις από το χρήστη	διαχωρισμό των spam μηνυμάτων έναντι των νόμιμων
Signature – based Filtering	- Σταματά τα γνωστά spam βάσει signature - Χαμηλό ποσοστό false positives - Ελάχιστες απαιτήσεις πόρων του συστήματος	- Μπορεί εύκολα να παρακαμφθεί από τυχαίο περιεχόμενο σε κάθε αντίγραφο spam - Χαμηλό ποσοστό εύρεσης spam
Clustering technigues	- Απόρριψη μηνυμάτων που είναι πολύ διαφορετικά από ένα συγκεκριμένο σύνολο	- Υψηλές απαιτήσεις πόρων του συστήματος - Υψηλό ποσοστό false positives
Social networks – based filters	- Αποδέχονται όλα τα μηνύματα του «κοινωνικού δικτύου» ενός χρήστη	- Υψηλό ποσοστό false positives - Δε συνίσταται η χρήση τους ως μοναδικό φίλτρο
Mail - volume based	- Απορρίπτει μηνύματα από δίκτυα που στέλνουν	- Υψηλό ποσοστό false positives

Filtering Method	Πλεονεκτήματα	Μειονεκτήματα
filters	μεγάλες ποσότητες spam	- Προτιμάται ο συνδυασμός τους με άλλα φίλτρα
Collaborative Filtering	- Απορρίπτει όλα τα μηνύματα που είναι κοινώς χαρακτηρισμένα από μία ομάδα ως spam	- Μπορεί να μην είναι ακριβή ή πλήρη ανάλογα με τους συμμετέχοντες - Η database της δεν είναι real-time
DNS Lookup systems	- Απορρίπτουν μηνύματα από μη υπαρκτά domain names	- Δεν είναι αξιόπιστη μέθοδος από μόνη της - Υψηλό ποσοστό false positives
Payment – based approach	- Αποτρεπτική μέθοδος για τους spammers (σχεδόν κανείς τους δε δαπανά χρήματα ή χρόνο για όλο αυτό τον όγκο μηνυμάτων)	- Η πληρωμή ή η απώλεια χρόνου αφορά και τους νόμιμους αποστολείς, εκτός αν βρίσκονται στη whitelist

Πίνακας 4.1: Συγκεντρωτικός πίνακας παράθεσης πλεονεκτημάτων και μειονεκτημάτων μεθόδων spam filtering

4.2 Email Services και Spam Filters

Στην συγκεκριμένη ενότητα παρουσιάζονται στοιχεία που προέκυψαν μετά από έρευνα σχετικά με τα spam filters που χρησιμοποιούν ορισμένα από τα δημοφιλέστερα δωρεάν email services παγκοσμίως.

Yahoo! Mail

Το Yahoo!Mail περιλαμβάνει μία συνεχώς εξελισσόμενη κλάση ασφαλείας για να βοηθάει τους χρήστες να νιώθουν ασφαλείς, κρατώντας τους εισβολείς και τους απατεώνες μακριά από τα εισερχόμενα μηνύματά τους. [47]

Το SpamGuard, περιλαμβάνεται δωρεάν με το Yahoo!Mail και χρησιμοποιεί machine learning τεχνικές, έτσι ώστε τα φίλτρα που μπλοκάρουν τα spam και άλλα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου να βελτιώνονται συνεχώς. Μάλιστα οι χρήστες μπορούν να συμμετέχουν στην εκπαίδευση του φίλτρου, κάνοντας κλικ στο κουμπί "Spam" κάθε φορά που συναντούν ένα junk e-mail ή "Not Spam" για τα μηνύματα που θέλουν να πάνε στα εισερχόμενά τους. Εκτός των άλλων, το SpamGuard επιτρέπει στους χρήστες να διαχειρίζονται τη δική τους whitelist για να επιτρέπουν πάντα μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από αξιόπιστες διευθύνσεις ή domain names. [48] Τέλος, το φίλτρο SpamGuard κάνει χρήση heuristic φίλτρων, χρησιμοποιώντας rules που παρακολουθούνται και ανανεώνονται συνεχώς, για την ανεύρεση όλο και περισσότερων spam και ιών.

Επίσης, το Yahoo!Mail χρησιμοποιεί image filtering τεχνικές, δίνοντας στο χρήστη τη δυνατότητα να επιλέγει από ποιες διευθύνσεις επιθυμεί να παραλαμβάνει μηνύματα με εικόνες, κρατώντας τον έτσι ασφαλή από μηνύματα με κακόβουλο περιεχόμενο ή ιούς που συχνά μεταδίδονται μέσω των μηνυμάτων αυτών. [47]

Για να αποφεύγονται περιπτώσεις phishing, όπου οι spammers προσπαθούν να υποκλέψουν ζωτικής σημασίας προσωπικές πληροφορίες, όπως κωδικοί πρόσβασης ή οικονομικά δεδομένα

του παραλήπτη, το Yahoo!Mail έχει προβλέψει χρησιμοποιώντας δύο βασικούς μηχανισμούς, τον DKIM και τον DMARC. [47] Ο μηχανισμός DomainKeys Identified Mail (DKIM), επιτρέπει στους αποστολείς να υπογράφουν ψηφιακά τα μηνύματα ηλεκτρονικού ταχυδρομείου τους, έτσι ώστε το Yahoo!Mail να μπορεί να επαληθεύει την αυθεντικότητά τους. Επιπρόσθετα, το συγκεκριμένο email service υποστηρίζει το Domain-based Message Authentication, Reporting and Conformance (DMARC), μια προδιαγραφή της οποίας ηγούνται μεγάλοι πάροχοι τεχνολογίας και αποστολείς e-mail για να καταπολεμήσουν το spam και τις απάτες phishing.

Outlook.com (Hotmail)

Η ασφάλεια του ηλεκτρονικού ταχυδρομείου της Microsoft περιλαμβάνει μια απαράμιλλη προσέγγιση μεταξύ προϊόντων που στόχο έχουν να προσφέρουν μία ολοκληρωμένη και εύχρηστη υπηρεσία στους χρήστες που να βοηθά στον εντοπισμό ανεπιθύμητων e-mail, απειλών phishing και ιών. [49]

Για να μειώσει τις συνέπειες των junk e-mail, η Outlook.com χρησιμοποιεί την πατενταρισμένη τεχνολογία SmartScreen, η οποία σκανάρει τα μηνύματα ηλεκτρονικού ταχυδρομείου για να ξεχωρίσει τα spam από τα νόμιμα email. [49] Με βάση την κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας machine learning τεχνολογία Microsoft Research, το content filter SmartScreen μαθαίνει από γνωστά spam, από απειλές phishing, από το feedback των χρηστών, καθώς και από χρήστες του Outlook.com που έχουν επιλεγεί να είναι μέλη του προγράμματος διαμόρφωσης και κατάταξης της ανεπιθύμητης αλληλογραφίας. Αυτοί οι τύποι των δεδομένων συμβάλλει τρένο SmartScreen πώς να αναγνωρίζει τα νόμιμα email και junk e-mail και είναι βασικές εισροές σε φήμη αποστολέα. Οι τεχνικές machine learning βασίζονται σε probability-based αλγορίθμους, που χρησιμοποιούνται για τη διάκριση μεταξύ των διαφορετικών χαρακτηριστικών των νόμιμων και των junk e-mail. Η συνεχής ανατροφοδότηση από τους χρήστες του Outlook.com στο πρόγραμμα ταξινόμησης junk email, βοηθά στη συνεχή εκπαίδευση και βελτίωση της τεχνολογίας SmartScreen.

Εκτός από την Microsoft SmartScreen, τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου φιλτράρονται από το Symantec Brightmail anti-spam content filter. [49] Αξιοποιώντας την Probe Network, μια συλλογή με περισσότερες από 200.000 διευθύνσεις ηλεκτρονικού ταχυδρομείου που έχουν σχεδιαστεί για να προσελκύουν την ανεπιθύμητη αλληλογραφία, το συγκεκριμένο

φίλτρο εντοπίζει και εξαλείφει τα junk e-mail πριν ακόμα φτάσουν στο inbox των χρηστών του Outlook.com.

Εκτός από αυτές τις τεχνολογίες anti-spam filtering, το Outlook.com επίσης δίνει σε κάθε χρήστη τη δυνατότητα να καθορίσει επίπεδα φίλτρων για να βελτιώσει περαιτέρω την διαδικασία παράδοσης μηνυμάτων ηλεκτρονικού ταχυδρομείου στο λογαριασμό του. [49] Οι χρήστες μπορούν εύκολα να προσθέσουν έναν αποστολέα ή ένα domain name στη λίστα με τους ασφαλείς αποστολείς, έτσι ώστε τα μηνύματα από αυτούς τους αποστολείς να μην αντιμετωπίζονται ως ανεπιθύμητη αλληλογραφία, ανεξάρτητα από το περιεχόμενό τους. Επίσης, οι χρήστες μπορούν να ενεργοποιήσουν την «exclusive» λειτουργία για να δέχονται μηνύματα μόνο από τις επαφές τους και τη λίστα ασφαλών αποστολέων. Η παρακάτω εικόνα (εικόνα 4.1) δείχνει ακριβώς τον τρόπο με τον οποίο ο χρήστης μπορεί να επιλέξει επίπεδο προστασίας για τα εισερχόμενα μηνύματά του. Τέλος, μηνύματα από συγκεκριμένες διευθύνσεις e-mail ή domain names μπορούν επίσης να αποκλειστούν με την προσθήκη των αποστολέων στη λίστα αποκλεισμένων αποστολέων, είτε κάνοντας κλικ στο κουμπί «Mark ως junk».

Εικόνα 4.1: Παράδειγμα επιλογής επιπέδου φίλτρων στο Outlook.com

Το Outlook.com προσφέρει εκτός των άλλων προστασία από απειλές phishing, ως μέρος μιας πατενταρισμένης τεχνολογίας του φίλτρου SmartScreen. [49] Η τεχνολογία αυτή αναλύει τα μηνύματα ηλεκτρονικού ταχυδρομείου για να βοηθήσει στον εντοπισμό ύποπτων links ή πλαστογραφημένων domain names και να προστατεύσει τους χρήστες από τέτοιου είδους online απάτες.

Το domain spoofing είναι ένας τρόπος μίμησης νόμιμων διευθύνσεων ηλεκτρονικού ταχυδρομείου για να φαίνονται τα δόλια μηνύματα σαν νόμιμα. [49] Η πλαστογράφηση χρησιμοποιείται από κακόβουλα άτομα και οργανώσεις για απάτες phishing και να δελεάσουν ανθρώπους να αποκαλύψουν ευαίσθητες προσωπικές τους πληροφορίες. Η αποκάλυψη αυτών των πληροφοριών μπορεί να οδηγήσει μετέπειτα σε κλοπή ταυτότητας και άλλες μορφές απάτης. Για το λόγο αυτό, το Outlook.com χρησιμοποιεί το Sender Protection Framework (SPF), το DomainKeys Identified Mail (DKIM), και το Domain-based Message Authentication, Reporting, and Conformance (DMARC), για να είναι σίγουρο ότι τα μηνύματα προέρχονται όντως από το domain name που ισχυρίζονται ότι προέρχονται.

Gmail

Η ομάδα Gmail χρησιμοποιεί μία σειρά από προηγμένες τεχνολογίες της Google προς αποφυγή των spam μηνυμάτων. [50] Σύμφωνα με τον τρόπο λειτουργίας της Gmail το καλύτερο όπλο τους είναι οι ίδιοι οι χρήστες, οι οποίοι αναφέροντας ένα συγκεκριμένο email ως spam, το σύστημά τους μαθαίνει γρήγορα και αρχίζει να αποκλείει παρόμοια μηνύματα. Όσο περισσότερα spam εντοπίζει η κοινότητά τους, τόσο εξυπνότερο γίνεται το σύστημά τους.

Τα φίλτρα και οι αλγόριθμοι του Gmail προσαρμόζονται γρήγορα κάθε φορά που εμφανίζονται νέα δεδομένα στο χώρο των spam. [50] Εκτός των άλλων, χρησιμοποιείται η τεχνική optical character recognition (OCR), που αναπτύχθηκε από την ομάδα Google Book Search, για να προστατεύονται οι Gmail χρήστες από τα image spam. Επίσης, οι machine-learning αλγόριθμοι που έχουν αναπτυχθεί για να συγχωνεύουν και να κατατάσσουν τα μεγάλα σύνολα αποτελεσμάτων της Google, επιτρέπουν στο Gmail να συνδυάζει εκατοντάδες παράγοντες για να ταξινομεί τα spam. Εκτός των άλλων, το Gmail υποστηρίζει πολλαπλά συστήματα πιστοποίησης, συμπεριλαμβανομένων των SPF (Sender Policy Framework) και DKIM (DomainKeys Identified

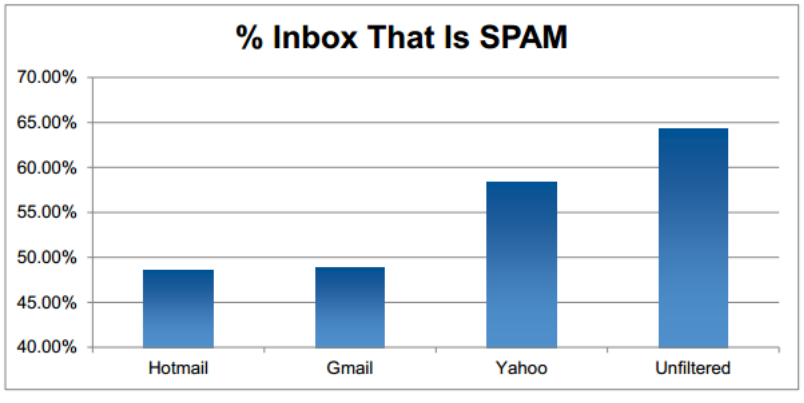
Mail), για να μπορούν οι χρήστες να είναι σίγουροι ότι τα μηνύματα προέρχονται όντως από αυτούς που ισχυρίζονται.

Σύγκριση αποτελεσματικότητας email services στο spam filtering

Η εταιρεία Cascade Insights πραγματοποίησε ερευνητική μελέτη το 2012 για να συγκρίνει τις δυνατότητες φιλτραρίσματος spam για τα webmail services Microsoft Hotmail, Google Gmail και Yahoo!Mail και να εξακριβωθεί η αποτελεσματικότητα φιλτραρίσματος SPAM για κάθε πάροχο. [51] Οι μετρήσεις κλειδιά στην συγκεκριμένη έρευνα ήταν η ποσότητα και το ποσοστό των spam μηνυμάτων στο inbox των χρηστών.

Τα αποτελέσματα της έρευνας κατηγοριοποιήθηκαν σε ham[18] και spam στο inbox των χρηστών για να διαπιστωθεί το ποσοστό των εισερχόμενων που ήταν spams. [51] Στην παρακάτω εικόνα (εικόνα 4.2) φαίνονται τα αποτελέσματα της έρευνας.

Mail Provider	Inbox HAM emails	HAM % of inbox	Inbox SPAM emails	SPAM % of inbox
Hotmail	233	51.43%	220	48.57%
Gmail	252	51.12%	241	48.88%
Yahoo	180	41.67%	252	58.33%
Unfiltered	302	35.78%	542	64.22%



Εικόνα 4.2: Αποτελέσματα έρευνας για την αποτελεσματικότητα στο spam filtering σε γνωστά email services

[18] ham: λέγονται τα email που δεν είναι spam. Θα λέγαμε ότι αποτελεί συντόμευση/συνώνυμο του non-spam

Τα αποτελέσματα δείχνουν ότι περίπου το 48% των μηνυμάτων ηλεκτρονικού ταχυδρομείου στο φάκελο εισερχομένων για το Gmail και το Hotmail ήταν spam. [51] Για το Yahoo!Mail, το ποσοστό ανήλθε στο 58%. Για λογαριασμό ενός εντελώς αφιλτράριστου ταχυδρομείου, το 64% των e-mail ήταν spam. Ως εκ τούτου, τα ευρήματα δείχνουν ότι το Hotmail και το Gmail είναι σχεδόν ίσα στη διατήρηση των spam μηνυμάτων έξω από το inbox των χρηστών.

Κεφάλαιο 5
Νομοθετικό Πλαίσιο για τα Spam

Το spamming έχει αποτελέσει αντικείμενο νομοθετικών μεταρρυθμίσεων σε πολλές χώρες, ενώ σε κάποιες χώρες η αποστολή spam διώκεται ποινικά. Στο συγκεκριμένο κεφάλαιο θα αναλυθεί η σημασία των νόμων που στοχεύουν στην καταπολέμηση των spam (anti-spam νόμοι), καθώς επίσης και οι παράμετροι με βάση τις οποίες αυτοί οι νόμοι καθορίζονται. Επίσης, θα παρουσιαστεί το ισχύον νομοθετικό πλαίσιο τόσο της Ευρώπης, όσο και της Ελλάδας. Τέλος, θα δοθούν ορισμένα στοιχεία, σε σχέση με την αποτελεσματικότητα των νόμων αυτών.

5.1 Πώς προκύπτουν οι Anti-spam Νόμοι

Κατά καιρούς έχουν εξελιχθεί και αναπτυχθεί πολλά διαφορετικά μέτρα για την καταπολέμηση των spam, όπως νόμοι, κανονισμοί, οργανωτικές προσεγγίσεις, μέτρα συμπεριφοράς καθώς και οικονομικά ή τεχνολογικά μέτρα. [36] Αυτά στοχεύουν στην ασφάλεια των χρηστών και εξετάζουν τρία κριτήρια: τα κίνητρα των spammers, την ικανότητα τους και τη νόμιμη άδεια. Τα κίνητρα και η ικανότητα θεωρούνται υποχρεωτικά για τους spammers. Ο τρίτος παράγοντας αναφέρεται στη νόμιμη άδεια που εκμεταλλεύονται ορισμένοι αποστολείς spam μηνυμάτων για να αποφύγουν πιθανή αντιδικία.

Δεδομένης της σοβαρότητας και της πιθανής ζημιάς που μπορούν να προκαλέσουν τα spam, οι αρχές πολλών χωρών και κρατών, έχουν αρχίσει να ασχολούνται με τα spam και τη νομοθεσία γύρω από αυτά. Η Ευρωπαϊκή Ένωση (ΕΕ), ξεκίνησε την οδηγία 2002/58/ΕΚ [08], η οποία έπρεπε να εφαρμοστεί νομοθετικά από κάθε κράτος μέλος της, από τις 31 Οκτωβρίου του 2003. Ωστόσο, σήμερα η νομοθετική κάλυψη σε παγκόσμιο επίπεδο των μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ετερογενής και η αποτελεσματικότητα των μέτρων που υπάρχουν είναι αμφιλεγόμενη.

Υπάρχουν κάποιες βασικές παράμετροι με βάση τις οποίες οι νόμοι για τα spam μπορούν να διαφοροποιούνται και σε αυτές συγκαταλέγονται: το πεδίο εφαρμογής του νόμου, το είδος της εγγραφής του παραλήπτη, το είδος του αποστολέα και του παραλήπτη, και το σύνολο των βασικών κατηγόρων. [36] Κάθε μία από αυτές περιγράφεται εκτενέστερα παρακάτω.

Πεδίο εφαρμογής του νόμου: Οι νόμοι που αφορούν τα spam στρέφονται είτε άμεσα είτε έμμεσα κατά της αποστολής συγκεκριμένων ειδών e-mail και της σχετικής βλάβης που αυτά μπορούν να προκαλέσουν. Αυτό το είδος αντιμετώπισης εξαρτάται από το πεδίο εφαρμογής του νόμου, το οποίο μπορεί να καλύψει: είτε έμμεσα, γενικά την αποστολή e-mail κακόβουλου περιεχομένου, είτε άμεσα και πιο ειδικά την αποστολή μηνυμάτων συγκεκριμένου περιεχομένου, όπως παραδείγματος χάριν πορνογραφικού υλικού.

Όταν τα spam αντιμετωπίζονται άμεσα, πολλοί νόμοι καθορίζουν το είδος των e-mail που καλύπτονται, συνήθως εστιάζοντας στα εμπορικά μηνύματα (UCE). [36] Στα ακόλουθα παραδείγματα, φαίνεται η πολυμορφία με την οποία οι νόμοι αντιμετωπίζουν τα spam και τις βλαβερές συνέπειές τους:

- Στην Αυστρία, η αποστολή e-mail σε περισσότερους από 50 δικαιούχους με σκοπούς απευθείας εμπορικής προώθησης, παραβιάζει το νόμο § 107 Telekommunikationsgesetz (Austrian Law of Telecommunications) (TKG), εκτός αν ο παραλήπτης έχει δώσει τη συγκατάθεσή του πριν από την αποστολή.
- Στη Γερμανία, το spamming μπορεί να θεωρηθεί ως εισβολή στις εμπορικές δραστηριότητες μίας εταιρείας σύμφωνα με την οδηγία §1004 B¨urgerliches Gesetzbuch (Γερμανικός Αστικός Κώδικας) (BGB) 2002
- Το CANSPAM Act του 2003 που ισχύει στις ΗΠΑ, επιτρέπει στους αποστολείς εμπορικών e-mail να στέλνουν τα μηνύματά τους, εκτός εάν ο δικαιούχος έχει αρνηθεί ρητά την παραλαβή τους (§ 1037): «(Α) Είναι παράνομο για

οποιοδήποτε πρόσωπο να κινήσει τη μετάδοση οποιουδήποτε μηνύματος εμπορικού ηλεκτρονικού ταχυδρομείου σε προστατευμένο υπολογιστή, εκτός εάν το μήνυμα παρέχει (i) σαφή και ευδιάκριτο χαρακτηρισμό ότι το μήνυμα αφορά διαφημιστικούς σκοπούς (ii) σαφή και εμφανή προειδοποίηση της δυνατότητας του παραλήπτη να αρνηθεί να λάβει περαιτέρω εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου από τον αποστολέα αυτόν και (iii) μια έγκυρη φυσική ταχυδρομική διεύθυνση του αποστολέα. (Β) Το εδάφιο (Α) (i) δεν ισχύει για τη μετάδοση ενός εμπορικού μηνύματος ηλεκτρονικού ταχυδρομείου, στην περίπτωση που ο δικαιούχος έχει δώσει εκ των προτέρων την ενεργητική συναίνεση για την παραλαβή του μηνύματος. »

Για δικαστικούς σκοπούς, οι νομοθέτες πρέπει να προσδιορίζουν με ακρίβεια, πότε ένα e-mail μπορεί να θεωρηθεί ως ανεπιθύμητο και ως εκ τούτου, ο αποστολέας του παραβιάζει την αντίστοιχη νομοθεσία. [36] Θα πρέπει να σημειωθεί ότι οι anti-spam νόμοι αποφεύγουν τη χρήση του όρου «spam», επειδή η νομοθετική σημασιολογία του δεν έχει ακόμη ορισθεί.

Εγγραφή: Οι νόμοι μπορεί να διαφέρουν ως προς τον τρόπο με τον οποίο ο αποδέκτης μπορεί να αρνηθεί την παραλαβή των e-mail, με άλλα λόγια, διαφοροποιείται το είδος της εγγραφής του παραλήπτη σε κάποια λίστα. [36] Υπάρχουν δύο είδη προσεγγίσεων: μια προσέγγιση «opt-in», η οποία απαιτεί ο αποστολέας να έχει την άδεια του παραλήπτη πριν την αποστολή του μηνύματος και μια προσέγγιση «opt-out», η οποία παρέχει ένα μηχανισμό τερματισμού της παραλαβής περαιτέρω e-mail από ένα συγκεκριμένο αποστολέα. Οι προσεγγίσεις αυτές περιλαμβάνουν τις ακόλουθες διατάξεις:

Unconfirmed opt-in: Ο χρήστης δίνει αρχικά μια διεύθυνση email σε μία λίστα λογισμικού (για παράδειγμα, σε μια ιστοσελίδα), αλλά δεν έχουν ληφθεί τα κατάλληλα μέτρα για να βεβαιωθούμε ότι η διεύθυνση αυτή ανήκει πραγματικά στο πρόσωπο το οποίο την υποβάλλει. [37] Οπότε, χωρίς επαλήθευση υπάρχει περίπτωση τα μηνύματα να σταλούν σε κάποιον άλλο και κατά συνέπεια να θεωρηθούν spam.

Confirmed opt-in: Ο νέος συνδρομητής ζητεί να εγγραφεί στη λίστα, αλλά σε αντίθεση με το unconfirmed opt-in, ένα e-mail επιβεβαίωσης στέλνεται στη διεύθυνση που έδωσε για να επαληθεύσει ότι ήταν πραγματικά αυτός. [37] Σε γενικές γραμμές, αν δε χρησιμοποιηθεί η επαλήθευση διεύθυνσης του τελικού συνδρομητή (όπως κάνοντας κλικ σε ένα ειδικό σύνδεσμο ή αποστέλλοντας ένα e-mail επιβεβαίωσης) είναι δύσκολο

να αποδειχθεί ότι η διεύθυνση e-mail ανήκει πράγματι στο πρόσωπο που υπέβαλε το αίτημα. Χρησιμοποιώντας την confirmed opt-in (COI) διαδικασία, μπορεί να εξασφαλιστεί ότι δεν μπορεί κάποιος να εγγραφεί κατά λάθος ή από δόλο, δεδομένου ότι εάν δε ληφθεί δράση από την πλευρά του παραλήπτη, απλά δε θα λαμβάνει πλέον κανένα μήνυμα από το διαχειριστή της λίστας. Ορισμένοι διαχειριστές συστημάτων αλληλογραφίας αναφέρονται σε αυτή τη διαδικασία και με τους όρους confirmed subscription ή closed-loop opt-in.

Double opt-in: Αυτός ο όρος επινοήθηκε στα τέλη της δεκαετίας του '90 για να το διαφοροποιήσει από αυτό που αποκαλούν "single opt-in", στο οποίο ο νέος συνδρομητής λαμβάνει ένα email επιβεβαίωσης το οποίο τον ενημερώνει ότι θα αρχίσει να λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου εάν δε λάβει δράση (εάν δηλαδή δεν κάνει τίποτα για να διαγραφεί από τη λίστα). [37] Ορισμένοι υποστηρίζουν ότι το double opt-in είναι σαν να ζητάμε την άδεια δύο φορές από το το χρήστη (γι' αυτό ονομάζεται και «διπλό») και ότι αποτελεί περιττή παρεμβολή σε κάποιον ο οποίος έχει ήδη δηλώσει ότι θέλει να λαμβάνει μηνύματα από τον διαφημιστή.

Plain opt-in: Δεν περιλαμβάνει κανενός είδους επιβεβαίωση. [36] Μόλις μία διεύθυνση e-mail εγγράφεται, προστίθεται και στη λίστα ακόμη και αν ο κάτοχός της δεν έχει δώσει τη συγκατάθεσή του.

Opt-out: Ακόμη και αν ο χρήστης λάβει ένα e-mail, χωρίς να έχει δώσει την άδειά του εκ των προτέρων, αυτό είναι εφοδιασμένο με ένα σύνδεσμο διαγραφής ή μια διεύθυνση e-mail που μπορεί να χρησιμοποιηθεί για την παύση της επικοινωνίας με το συγκεκριμένο e-mail. [36] Ο όρος opt-out αναφέρεται λοιπόν στις διάφορες μεθόδους με τις οποίες οι χρήστες μπορούν να αποφύγουν τη λήψη μηνυμάτων με ανεπιθύμητα προϊόντα ή υπηρεσίες παροχής πληροφοριών. Ορισμένες χώρες, όπως οι ΗΠΑ, προτείνουν τη διατήρηση μιας λίστας διευθύνσεων που περιέχει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των καταναλωτών που δεν επιθυμούν να λαμβάνουν ηλεκτρονικά μηνύματα εμπορικού χαρακτήρα (Robinson list ή αλλιώς μητρώα opt-out). [38] Οι πάροχοι υπηρεσιών οφείλουν να ελέγχουν τακτικά αυτά τα μητρώα και να σέβονται τους καταναλωτές που είναι εγγεγραμμένοι σε αυτά.

Αποστολέας και Παραλήπτης: Οι νόμοι μπορούν να στοχεύουν σε συγκεκριμένους τύπους αποστολέων και παραληπτών για να εφαρμοστούν, όπως για παράδειγμα ιδιώτες χρήστες ή οργανώσεις. [36] Για παράδειγμα, η οδηγία 2002/58/ΕΚ [08, το

άρθρο 13 5.] περιορίζει τη "γενική" opt-in προσέγγισή της στους παραλήπτες που είναι φυσικά πρόσωπα.

Πιθανοί κατήγοροι: Οι νόμοι μπορούν να επιβάλλουν περιορισμούς σε σχέση με το ποιος μπορεί να μηνύσει τους αποστολείς μηνυμάτων. Πολλοί anti-spam νόμοι, όπως ο CANSPAM Act του 2003, δεν παρέχουν νομοθετικά μέσα για τα άτομα, αλλά μόνο για τις κρατικές αρχές και κάποιες άλλες οργανώσεις. Παράδειγμα αποτελεί ο γερμανικός νόμος ενάντια στον αθέμιτο ανταγωνισμό (UWG) 2004 που ανοίγει την πόρτα για την άσκηση προσφυγής στους ανταγωνιστές, τις συνδικαλιστικές ενώσεις, τα εμπορικά επιμελητήρια, τα βιοτεχνικά επιμελητήρια και μόνο κάποιες πιο "εξειδικευμένες" οργανώσεις.

Περαιτέρω απαιτήσεις: Οι νόμοι μπορεί να προχωρούν στην ανάλυση περαιτέρω απαιτήσεων των e-mail. Όπως αναφέρθηκε παραπάνω, ο CANSPAM Act του 2003 (§ 1037), για παράδειγμα, απαγορεύει τη χρήση μίας τυχαίας διεύθυνσης e-mail, απαιτεί η διαφήμιση να είναι εμφανής και ορίζει ότι κάθε e-mail θα πρέπει να περιέχει μία έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου που να επιτρέπει στον αποδέκτη να το προσθέσει στην λίστα εμπορικών e-mail και να μην παραλαμβάνει πια μηνύματα από τη διεύθυνση αυτή (opt-out).

5.2 Νομοθετικό Πλαίσιο Anti-spam στην Ευρώπη

Ακριβώς όπως αυξάνεται ο αριθμός των spam τα τελευταία χρόνια, έτσι ακριβώς αυξάνονται και οι νόμοι anti-spam ανά τον κόσμο. [36] Έρευνες που πραγματοποιήθηκαν από τους οργανισμούς International Telecommunication Union (ITU) και Organization for Economic Co-operation and Development (OECD), ανέδειξαν μεγάλο αριθμό anti-spam νόμων και τεράστια ανομοιογένεια μεταξύ τους. Σε γενικές γραμμές παρατηρούμε ότι δεν υπάρχει συναίνεση σχετικά με τη νομοθετική στάση απέναντι στα spam και το χειρισμό τους. Υπάρχουν ακόμη χώρες που δεν έχουν καθόλου ή έχουν χαμηλής αποτελεσματικότητας anti-spam νόμους και αυτό αποτελεί και το λόγο για τον οποίο οι spammers στρέφονται σε περιοχές με λιγότερη νομοθεσία και κανονισμούς, που θα μπορούν να περιορίζουν τη δράση τους.

Στην Ευρώπη αυτή τη στιγμή ισχύει η οδηγία 2002/58/ΕΚ, που αφορά την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. [40] Παρόλα αυτά , η κάθε ευρωπαϊκή χώρα αυτή τη στιγμή εφαρμόζει τη δική της εθνική anti-spam νομοθεσία. Παρακάτω παρουσιάζεται το

άρθρο 13 της οδηγίας αυτής, όπως ακριβώς εκδόθηκε από το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο στις 12 Ιουλίου 2002 και αφορά (γενικά) τις αυτόκλητες κλήσεις:

1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.

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

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

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

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

Ενδεικτικά δίδεται ο παρακάτω πίνακας (πίνακας 5.1) όπου παρουσιάζονται συγκεντρωτικά οι πιο γνωστές νομοθεσίες που εφαρμόζονται ενάντια στα spam ανά τον κόσμο. [41] [45] [46]

	Νόμος
Ηνωμένες Πολιτείες	CAN-SPAM Act of 2003 (Opt-Out)
Καναδάς	Canada's Anti-Spam Legislation 2014 (CASL) (Opt-In)
Ευρωπαική Ένωση	E-Privacy Directive (2002/58/EC) (Opt-In)
Κύπρος	Regulation of Electronic Communications and Postal Services Law of 2004 (Opt-In)
Αυστραλία	Spam Act 2003 (Opt-Out)
Ελλάδα	Hellenic Data Protection Authority (law 3471/2006, art. 11) (Opt-Out)
Γερμανία	Gesetz gegen Unlauteren Wettbewerb (UWG) (Opt-In)

Πίνακας 5.1: Παραδείγματα νόμων ενάντια στα spam που εφαρμόζονται σήμερα παγκοσμίως

5.3 Νομοθετικό Πλαίσιο Anti-spam στην Ελλάδα

Στην Ελλάδα η αζήτητη επικοινωνία ρυθμίζεται από το άρ. 11 του Νόμου 3471/2006 που ενσωμάτωσε την Οδηγία 2002/58/ΕΚ για την προστασία προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. [41]

Σύμφωνα με τον παραπάνω νόμο (άρθρο 11 παρ. 3 ν. 3471/2006), η αποστολή μη ζητηθέντων μηνυμάτων με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας επιτρέπεται μόνο στην περίπτωση που ο παραλήπτης έχει δώσει την συγκατάθεσή του εκ των προτέρων, ανεξάρτητα αν ο παραλήπτης είναι φυσικό ή νομικό πρόσωπο. Κατά συνέπεια, κάθε μήνυμα (π.χ. e-mail, SMS, MMS, IM) που αποστέλλεται στους χρήστες χωρίς να έχουν δώσει ρητά τη συγκατάθεσή σας (spam), θεωρείται παράνομο. Εξαίρεση αποτελεί η περίπτωση κατά την οποία αποστέλλονται στους χρήστες διαφημιστικά

μηνύματα από εταιρείες ή ιδιώτες με τους οποίους είχαν ήδη προηγούμενες συναλλαγές και είχαν δηλώσει τη διεύθυνση τους (π.χ. μετά την αγορά κάποιου προϊόντος ή υπηρεσίας από ένα κατάστημα). Στην περίπτωση αυτή τα στοιχεία του παραλήπτη έχουν αποκτηθεί νομίμως από τον αποστολέα, οπότε και επιτρέπεται η αποστολή μηνυμάτων που διαφημίζουν παρόμοια προϊόντα ή υπηρεσίες μέχρι ο χρήστης να δηλώσει την εναντίωσή του στη λήψη των μηνυμάτων αυτών.

Επιπρόσθετα όλα τα διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνει κάποιος πρέπει να έχουν έγκυρη διεύθυνση αποστολέα και να αναφέρουν ευδιάκριτα την ταυτότητά του ή την ταυτότητα του προσώπου προς όφελος του οποίου γίνεται η αποστολή (άρθρο 11 παρ. 3 ν. 3471/2006). Εκτός των άλλων, οι αποστολείς μηνυμάτων οφείλουν να παρέχουν τη δυνατότητα εναντίωσης στη λήψη τους με απλό και εύκολο τρόπο (σύστημα "opt-out"), όπως για παράδειγμα με έναν σύνδεσμο στο newsletter (unsubscribe), μέσω της διαδικτυακής σελίδας τους ή μέσω της αποστολής ενός μηνύματος ηλεκτρονικού ταχυδρομείου.

Ως «συγκατάθεση» του χρήστη ορίζεται κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και με πλήρη επίγνωση και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν (άρθρο 2 ια΄ Ν. 2472/1997). Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

Σε περίπτωση που η συγκατάθεση δίδεται με ηλεκτρονικά μέσα, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη ή συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί (άρθρο 5 § 3 Ν. 3471/2006).

Ειδικές νόμιμες διαδικασίες αναφορικά με την ηλεκτρονική συγκατάθεση για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, SMS/MMS και την πραγματοποίηση φωνητικών κλήσεων προβλέπονται στην Απόφαση 2/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). [39] Πιο συγκεκριμένα η απόφαση αυτή στο άρθρο 4, για την ηλεκτρονική συγκατάθεση για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) μέσω διαδικτύου, αναφέρει τα εξής:

1. Όταν ο συνδρομητής ή χρήστης δηλώνει τη συγκατάθεσή του για την αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε συγκεκριμένη ηλεκτρονική διεύθυνση, ο υπεύθυνος επεξεργασίας οφείλει καταρχάς, να επιβεβαιώνει ότι ο συνδρομητής ή χρήστης έχει πρόσβαση στη διεύθυνση αυτή. Η δήλωση συγκατάθεσης στην περίπτωση αυτή γίνεται συνήθως είτε με την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου από την ηλεκτρονική διεύθυνση του συνδρομητή ή χρήστη σε ηλεκτρονική διεύθυνση του υπεύθυνου επεξεργασίας, είτε με άλλο τρόπο, όπως π.χ. μέσω της ιστοσελίδας του υπεύθυνου επεξεργασίας.

2. Ο υπεύθυνος επεξεργασίας οφείλει να ακολουθεί ειδικές διαδικασίες για την επιβεβαίωση της δήλωσης συγκατάθεσης του συνδρομητή ή χρήστη, όπως οι ακόλουθες:

α) διαδικασία δήλωσης συγκατάθεσης με πρόσθετη ενημέρωση. Η διαδικασία αυτή πρέπει κατ' ελάχιστο να εφαρμόζεται σε όλες τις περιπτώσεις που ο συνδρομητής ή χρήστης δηλώνει τη συγκατάθεσή του για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου.

αα) Μετά τη δήλωση της συγκατάθεσης του συνδρομητή ή χρήστη, ο υπεύθυνος επεξεργασίας αποστέλλει αρχικό ενημερωτικό μήνυμα ηλεκτρονικού ταχυδρομείου προς τη διεύθυνση ηλεκτρονικού ταχυδρομείου που δηλώθηκε ως στοιχείο επικοινωνίας του συνδρομητή ή χρήστη. Στο μήνυμα αυτό ο συνδρομητής ή χρήστης ενημερώνεται σχετικά με το γεγονός ότι δήλωσε τη συγκατάθεσή του για τη συγκεκριμένη επεξεργασία, ενώ παράλληλα του παρέχεται ένας εύκολος τρόπος ανάκλησης της συγκατάθεσής του, εφόσον το επιθυμεί. Η ανάκληση της συγκατάθεσης πρέπει να μπορεί να πραγματοποιηθεί άμεσα και εύκολα μετά τη λήψη του παραπάνω ενημερωτικού μηνύματος και σε οποιαδήποτε χρονική στιγμή επιθυμεί ο συνδρομητής ή χρήστης, π.χ. μέσω αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου προς συγκεκριμένη διεύθυνση του υπεύθυνου επεξεργασίας ή μέσω ειδικού υπερσυνδέσμου (URL) στην ιστοσελίδα του υπεύθυνου επεξεργασίας, μοναδικού για κάθε συνδρομητή ή χρήστη.

ββ) Στο αρχικό ενημερωτικό μήνυμα πρέπει επίσης να αναγράφεται ο σκοπός αποστολής του (για την ενημέρωση του συνδρομητή ή χρήστη σχετικά με τη συγκεκριμένη δήλωση συγκατάθεσής του), η προέλευσή του (π.χ. ταυτότητα του

υπεύθυνου επεξεργασίας ή/και ιστοσελίδα από την οποία έχει προέλθει το μήνυμα) και να υπάρχει υπερσύνδεσμος προς το κείμενο ενημέρωσης σχετικά με την επεξεργασία προσωπικών δεδομένων που αφορά η εν λόγω δήλωση συγκατάθεσης, σύμφωνα με τα προβλεπόμενα στο άρθρο 3 της Οδηγίας.

β) διαδικασία επιβεβαιωμένης συγκατάθεσης. Η διαδικασία αυτή, που περιλαμβάνει τη διπλή επιβεβαίωση της συγκατάθεσης του συνδρομητή ή χρήστη («double opt-in»), μπορεί να εφαρμόζεται ως εναλλακτική αυτής που αναφέρεται στο στοιχείο α) της παρούσας παραγράφου, ιδίως σε περιπτώσεις που η δήλωση της συγκατάθεσης περιλαμβάνει και τη λήψη περαιτέρω υπηρεσιών από τον συνδρομητή ή χρήστη (όπως π.χ. την εγγραφή σε ιστοσελίδα με username και password).

αα) Μετά τη δήλωση της συγκατάθεσης του συνδρομητή ή χρήστη, ο υπεύθυνος επεξεργασίας αποστέλλει αρχικό επιβεβαιωτικό μήνυμα ηλεκτρονικού ταχυδρομείου προς τη διεύθυνση ηλεκτρονικού ταχυδρομείου που δηλώθηκε ως στοιχείο επικοινωνίας του συνδρομητή ή χρήστη. Με το μήνυμα αυτό ο συνδρομητής ή χρήστης καλείται να ενεργοποιήσει τη δήλωση συγκατάθεσής του, π.χ. μέσω αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου προς συγκεκριμένη διεύθυνση του υπεύθυνου επεξεργασίας ή μέσω επιλογής ειδικού υπερσυνδέσμου (URL), μοναδικού για κάθε συνδρομητή ή χρήστη, στην ιστοσελίδα του υπεύθυνου επεξεργασίας.

ββ) Στο αρχικό επιβεβαιωτικό μήνυμα πρέπει να αναγράφεται ο σκοπός αποστολής του (για την ενεργοποίηση της δήλωσης συγκατάθεσης), η προέλευσή του (π.χ. ταυτότητα του υπεύθυνου επεξεργασίας ή/και ιστοσελίδα από την οποία έχει προέλθει το μήνυμα) και να υπάρχει υπερσύνδεσμος προς το κείμενο ενημέρωσης σχετικά με την επεξεργασία προσωπικών δεδομένων που αφορά η εν λόγω δήλωση συγκατάθεσης, σύμφωνα με τα προβλεπόμενα στο άρθρο 3 της Οδηγίας. Το μήνυμα πρέπει επίσης να αναφέρει τον τρόπο με τον οποίο ο συνδρομητής ή χρήστης μπορεί να ανακαλέσει τη συγκατάθεσή του όποτε το επιθυμήσει.

γγ) Η συγκατάθεση στην περίπτωση αυτή θεωρείται έγκυρη μόνο εφόσον ο συνδρομητής ή χρήστης ενεργοποιήσει τη δήλωσή του. Αν η ενεργοποίηση δεν

πραγματοποιηθεί εντός χρονικού διαστήματος, που ορίζεται από τον υπεύθυνο επεξεργασίας, η διεύθυνση ηλεκτρονικού ταχυδρομείου που έχει δηλωθεί πρέπει να διαγράφεται αυτόματα από το αρχείο του υπεύθυνου επεξεργασίας.

δδ) Όταν για την εγγραφή σε διαδικτυακή υπηρεσία έχει πραγματοποιηθεί διαδικασία επιβεβαίωσης της διεύθυνσης ηλεκτρονικού ταχυδρομείου, σύμφωνη με τα παραπάνω, δεν απαιτείται εκ νέου επιβεβαίωση της πρόσβασης του συνδρομητή ή χρήστη στο δηλούμενο λογαριασμό ηλεκτρονικού ταχυδρομείου.

3. Ο υπεύθυνος επεξεργασίας οφείλει να καταγράφει, με ασφαλή τρόπο, τα στοιχεία που είναι απαραίτητα για την απόδειξη της δήλωσης της συγκατάθεσης του συνδρομητή ή χρήστη. Συγκεκριμένα οφείλει να καταγράφει τον τρόπο δήλωσης της συγκατάθεσης για τη συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου, καθώς και την ημέρα και ώρα της δήλωσης. Στην περίπτωση της επιβεβαιωμένης συγκατάθεσης, τα παραπάνω στοιχεία πρέπει να τηρούνται τόσο για την αρχική δήλωση, όσο και για την επιβεβαίωση της δήλωσης συγκατάθεσης.

4. Η ανάκληση της συγκατάθεσης πρέπει να είναι δυνατή, ανά πάσα στιγμή, με χρήση συστήματος αντίστοιχου με αυτό μέσω του οποίου δηλώθηκε η συγκατάθεση, π.χ. μέσω ηλεκτρονικού ταχυδρομείου ή ειδικού υπερσυνδέσμου στην ιστοσελίδα του υπεύθυνου επεξεργασίας, ή μέσω επιλογών στην ειδική περιοχή χρήστη της ιστοσελίδας (π.χ. σε περιπτώσεις εγγεγραμμένων χρηστών). Ο συνδρομητής ή χρήστης είναι σκόπιμο να ενημερώνεται για την ολοκλήρωση της διαδικασίας ανάκλησης της συγκατάθεσης, π.χ. με μήνυμα ηλεκτρονικού ταχυδρομείου.

5.4 Η αποτελεσματικότητα των Anti-spam Νόμων

Εκτός από μεμονωμένες επιτυχείς περιπτώσεις καταπολέμησης των spam, στο σύνολό τους οι anti-spam νόμοι φαίνονται αν μην μπορούν να αντιταχθούν στα spam, πράγμα που αποδεικνύεται και από το γεγονός ότι 2 στα 3 e-mails που στέλνονται σήμερα είναι spam. [36] Το ITU (International Telecommunication Union) επισημαίνει «Ακόμη και αν οι νόμοι anti-spam είχαν τεθεί σε εφαρμογή με καλές βλέψεις, φαίνεται να μην εξετάζουν το πρόβλημα με ουσιαστικό τρόπο». Περισσότερο από το ήμισυ των spam παγκοσμίως, προέρχεται από χώρες χωρίς anti-spam νόμους ή με κανόνες opt-out. Αυτό

δείχνει ότι οι opt-in νόμοι έχουν μία θετική επίδραση στο spamming, ενώ οι opt-out είναι σχεδόν απαγορευτικοί. Απ' την άλλη πλευρά βέβαια οι opt-out νόμοι εξακολουθούν να είναι χρήσιμοι, διότι παρέχουν σαφείς νομοθετικές κατευθυντήριες γραμμές για τις επιχειρήσεις και τους αποδέκτες, περιορίζοντας έτσι το ανεξέλεγκτο e-mail μάρκετινγκ ορισμένων εταιρειών. Οπότε, μπορεί να θεωρηθεί ότι υπάρχει μια μερικώς θετική επίδραση των anti-spam νόμων σχετικά με την αποστολή ανεπιθύμητων μηνυμάτων. Αυτό κινητοποιεί περαιτέρω εργασίες για την δημιουργία περισσότερων anti-spam νόμων. Στην πραγματικότητα τα περισσότερα από τα ανεπιθύμητα μηνύματα που απευθύνονται σε χρήστες του Διαδικτύου στη Βόρεια Αμερική και την Ευρώπη παράγονται από ένα σκληρό πυρήνα μίας ομάδας γνωστών επαγγελματιών spammers, των οποίων τα ονόματα ή ψευδώνυμα και οι πράξεις βρίσκονται τεκμηριωμένες στη βάση δεδομένων του Spamhaus' Register Of Known Spam Operations (ROKSO). Οπότε, η δίωξη έστω και μικρού αριθμού των spammers αυτών θα ήταν πιθανό να μειώσει τον συνολικό αριθμό spam παγκοσμίως σε μεγάλο βαθμό.

Ένα βασικό πρόβλημα των νομοθετικών μέτρων κατά των spam e-mails είναι ότι ένα διεθνές φαινόμενο, αντιμετωπίζεται από την εθνική νομοθεσία κάθε κράτους. Αν εξετάσουμε το θέμα λεπτομερώς, εντοπίζουμε τα ακόλουθα προβλήματα:

- Σημαντικό μέρος των spam διασχίζει κατά καιρούς τα διεθνή σύνορα. Ένα σημαντικό ερώτημα που τίθεται για την κάθε χώρα, είναι αν έχει αρμοδιότητα πάνω σε μηνύματα που προέρχονται εντός των συνόρων της, αλλά που αποστέλλονται σε διαφορετική χώρα. Οι εγχώριες διατάξεις που απαγορεύουν την αποστολή των spam ή που θεσπίζουν κανόνες για τα νόμιμα μηνύματα, είναι πιθανό να έχουν πολύ μικρή επίδραση στα μηνύματα εξω-εδαφικής προέλευσης. Άλλο ένα σοβαρό ερώτημα είναι αν μια εθνική αρχή ή ακόμα και ένας απλός χρήστης σε μια χώρα, έχει τη δυνατότητα να ξεκινήσει αντιδικία με έναν spammer που κατοικεί σε μία άλλη χώρα.
- Το διεθνές τοπίο νομοθεσίας anti-spam είναι ετερογενές, παρουσιάζοντας πολλά προβλήματα στην αντιμετώπιση ανεπιθύμητων μηνυμάτων. Μία λύση θα ήταν η δημιουργία έστω και ενός ελάχιστου προτύπου νομοθεσίας για τα spam σε όλο τον κόσμο. Ωστόσο, η εναρμόνιση αυτή σε παγκόσμιο επίπεδο φαίνεται να είναι πολύ δύσκολο έργο, με τις ΗΠΑ και την Ευρωπαϊκή Ένωση να διατηρούν τα καθεστώτα opt-in και opt-out.

- Η εφαρμογή των νόμων χρειάζεται παράλληλα πόρους και δεξιότητες, τα οποία συχνά δεν είναι διαθέσιμα. Για παράδειγμα, αρκετές αναπτυσσόμενες χώρες, όπως η Ινδία, έχουν νόμους που απαγορεύουν το hacking, καταδιώκουν την παρενόχληση μέσω του Διαδικτύου κ.λπ., αλλά στη συνέχεια, η εφαρμογή των νόμων αυτών είναι στα χέρια της τοπικής αστυνομίας ή άλλων οργανισμών επιβολής του νόμου, οι οποίοι είτε έχουν δωροδοκηθεί επαρκώς για την απαλλαγή των υπαιτίων, είτε είναι ανεπαρκώς εκπαιδευμένοι για να συμβαδίσουν με τις τάσεις της εγκληματικότητας στον κυβερνοχώρο, πόσο μάλλον με θέματα που αφορούν το spam.

Κεφάλαιο 6
Επίλογος

Ο πολλαπλασιασμός των αυτόκλητων ηλεκτρονικών μηνυμάτων, έχει φθάσει σε σημείο να δημιουργεί πρόβλημα για την ανάπτυξη του ηλεκτρονικού εμπορίου και τις σημερινές κοινωνίες της πληροφορίας. Η αντιμετώπιση των spam έχει γίνει κοινή υπόθεση όλων μας και έχει αναχθεί σε ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζει σήμερα το Internet.

Όσο περισσότερο το πρόβλημα των spam κλιμακώνεται, τόσο πιο πολύ απαιτείται η εύρεση αποτελεσματικών και αποδοτικών φίλτρων spam για το έλεγχό τους. Τα φίλτρα spam πρέπει να σχεδιάζονται, έτσι ώστε να διατηρούν κριτήρια όπως η ασφάλεια, η αξιοπιστία και η συμβατότητα με τα υπάρχοντα συστήματα. Η κάθε προσέγγιση για την ασφάλεια των χρηστών από τα spam έχει τα πλεονεκτήματα και τα μειονεκτήματά της. Κάθε μία μπορεί να οδηγήσει σε false negatives και false positives. Η κάθε διαφορετική προσέγγιση μπορεί να λειτουργήσει καλύτερα σε διαφορετικές καταστάσεις. Όταν πρόκειται για το φιλτράρισμα ανεπιθύμητων μηνυμάτων βέβαια, ο συνδυασμός των τεχνικών αυτών φαίνεται να λειτουργεί καλύτερα. Το μόνο σίγουρο είναι ότι το πρόβλημα των αυτόκλητων μηνυμάτων απαιτεί μια πολύπλευρη λύση που συνδυάζει ένα ευρύ φάσμα τεχνικών φιλτραρίσματος με διάφορες αλλαγές στην υποδομή, τις μεταβολές των οικονομικών κινήτρων για τους spammers και νομικές προσεγγίσεις.

Επιπλέον, τα φίλτρα spam πρέπει να βελτιώνονται πάντα σύμφωνα με τις απαιτήσεις και τη φύση των νέων τύπων ανεπιθύμητων μηνυμάτων.

Από την έρευνα που διεξήχθη στην παρούσα εργασία βρέθηκε ότι το Bayesian filtering είναι από τις αποτελεσματικότερες μεθόδους για την αντιμετώπιση spam, δίνοντας τα λιγότερα false positives, ενώ μπορεί να δώσει ακόμα καλύτερα αποτελέσματα όταν συνδυαστεί με άλλα φίλτρα. Εξίσου καλές αποδόσεις φαίνονται να έχουν τα rule-based φίλτρα (heuristic), ενώ υπάρχουν και λιγότερο αποτελεσματικές μέθοδοι όπως το challenge-response filtering και τα word-based filters τα οποία από μόνα τους φαίνονται να μην μπορούν να σταθούν στην πρόκληση αντιμετώπισης των spam μηνυμάτων.

Ωστόσο, η έρευνα για νέα αποτελεσματικότερα φίλτρα spam φαίνεται να μην τελειώνει ποτέ, με τους spammers να σκαρφίζονται συνεχώς νέες μεθόδους για να καταφέρουν να ξεγελάσουν τα υπάρχοντα φίλτρα και να στείλουν μαζική αλληλογραφία.

Το σημαντικό είναι ότι η παρούσα εργασία κατόρθωσε με την διεξοδική ανάλυσή της να παρέχει στον οποιοδήποτε χρήστη μία ολοκληρωμένη εικόνα γύρω από τα spam filters. Η εύρεση και σύγκριση των χαρακτηριστικών του κάθε φίλτρου μεμονωμένα, αποτελούσε μέχρι σήμερα μία ατέρμονη διαδικασία. Μέσω των συγκριτικών αποτελεσμάτων της εργασίας, καθίσταται πλέον ευκολότερη η επιλογή του καταλληλότερου φίλτρου anti-spam ανάλογα με τις ανάγκες του κάθε χρήστη. Επιπρόσθετα, ο κάθε χρήστης αποκτά ενημέρωση τέτοια ώστε να καθίσταται πλέον ικανός, όχι μόνο να προστατεύεται από τις πολυπληθείς απειλές στο ηλεκτρονικό ταχυδρομείο του, αλλά και να κρίνει το φίλτρο αυτό που χρειάζεται να χρησιμοποιήσει κάθε φορά, ανάλογα με την περίπτωση spam μηνυμάτων που θέλει να αντιμετωπίσει.

Πίνακας Ορολογίας (Ελληνική Απόδοση)

Ξενόγλωσσος όρος	Απόδοση όρου στα Ελληνικά
spam	“ανεπιθύμητη αλληλογραφία” ή “αυτόκλητη και αζήτητη αποστολή ηλεκτρονικών μηνυμάτων”
newsletter	διαφημιστική e-mail καμπάνια
hyperlink	υπερσύνδεσμος
server	εξυπηρετητής, διακομιστής
junk	ανεπιθύμητη αλληλογραφία
blog	ιστολόγιο
forum	φόρουμ
antivirus	αντιϊκό λογισμικό
firewall	τείχος προστασίας
malware	κακόβουλο λογισμικό
false positive	ψευδώς θετικά
false negative	ψευδώς αρνητικά
blacklist	μαύρη λίστα
whitelist	άσπρη λίστα
greylist	γκρι λίστα
challenge-response	πρόκληση-απόκριση
heuristic filters	ευριστικά φίλτρα
machine learning	μηχανική μάθηση
log files	αρχεία καταγραφής
collaborative filtering	συνεργατικό φιλτράρισμα

Πίνακας Ορολογίας (Ξενόγλωσση Απόδοση)

Ξενόγλωσσος όρος	Απόδοση όρου στα Αγγλικά
“ανεπιθύμητη αλληλογραφία” ή “αυτόκλητη και αζήτητη αποστολή ηλεκτρονικών μηνυμάτων”	spam
διαφημιστική e-mail καμπάνια	newsletter
υπερσύνδεσμος	hyperlink
εξυπηρετητής, διακομιστής	server
ανεπιθύμητη αλληλογραφία	junk
ιστολόγιο	blog
φόρουμ	forum
αντιϊκό λογισμικό	antivirus
τείχος προστασίας	firewall
κακόβουλο λογισμικό	malware
ψευδώς θετικά	false positive
ψευδώς αρνητικά	false negative
μαύρη λίστα	blacklist
άσπρη λίστα	whitelist
γκρι λίστα	greylist
πρόκληση-απόκριση	challenge-response
ευριστικά φίλτρα	heuristic filters
μηχανική μάθηση	machine learning
αρχεία καταγραφής	log files
συνεργατικό φιλτράρισμα	collaborative filtering

Συντμήσεις – Αρκτικόλεξα - Ακρωνύμια

SEO:	**S**earch **E**ngine **O**ptimization
ARPANET:	**A**dvanced **R**esearch **P**rojects **A**gency **N**etwork
CAPTCHA:	**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part
URL:	**U**niform **R**esource **L**ocator
UCE:	**U**nsolicited **C**ommercial **E**-mail
UBE:	**U**nsolicited **B**ulk **E**-mail
DNS:	**D**omain **N**ame **S**ystem
DNSBL:	**DNS B**lackhole **L**ists
ISP:	**I**nternet **S**ervice **P**rovider
IP:	"**I**nternet **P**rotocol" **ή** "**I**ntellectual **P**roperty"
KNN:	**K-N**earest **N**eighbors
SMTP:	**S**imple **M**ail **T**ransfer **P**rotocol
MTA:	**M**ail **T**ransfer **A**gent
ΕΕ:	**Ε**υρωπαϊκή **Έ**νωση
ITU:	**I**nternational **T**elecommunication **U**nion
OECD:	**O**rganization for **E**conomic **C**o-operation and **D**evelopment
άρ. :	**άρ**θρο
παρ. :	**παρ**άγραφος
ν. :	**ν**όμος
ΕΚ:	**Ε**υρωπαικό **Κ**οινοβούλιο
ΑΠΔΠΧ:	**Α**ρχής **Π**ροστασίας **Δ**εδομένων **Π**ροσωπικού **Χ**αρακτήρα

Βιβλιογραφία

[01] SPAM (2006). Ανακτήθηκε από:
http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

[02] Email spam (2014, June 30). Ανακτήθηκε από http://en.wikipedia.org/wiki/Email_spam

[03] Spamming (2014, June 18). Ανακτήθηκε από http://en.wikipedia.org/wiki/Spamming

[04] Origin of the term "spam" to mean net abuse (n.d.). Ανακτήθηκε από
http://www.templetons.com/brad/spamterm.html

[05] V. V. Arutyunov. «Spam: Its Past, Present, and Future». published in
Nauchno_Technicheskaya Informatsiya, No. 8,, pp. 24–32., 2013.

[06] What is Email Spam? (n.d.). Ανακτήθηκε από
http://emailmarketing.comm100.com/email-marketing-ebook/email-spam.aspx

[07] Mobile phone spam (2014, August 6). Ανακτήθηκε από:
http://en.wikipedia.org/wiki/Mobile_phone_spam

[08] Forum spam (2014, July 30). Ανακτήθηκε από:
http://en.wikipedia.org/wiki/Forum_spam

[09] Spamdexing (2014, July 20). Ανακτήθηκε από:
http://en.wikipedia.org/wiki/Spamdexing

[10] Damage caused by spam (n.d.). Ανακτήθηκε από
http://securelist.com/threats/damage-caused-by-spam/

[11] SPAM (n.d.). Ανακτήθηκε από
http://www.securitymanagement.com/archive/library/AussieSpam_tech0703.pdf

[12] Spam: The silent ROI Killer (n.d.). Ανακτήθηκε από
http://www.spamhelp.org/articles/d59.pdf

[13] Επιτροπή των Ευρωπαϊκών Κοινοτήτων (2004, January 1), Ανεπίκλητα μηνύματα εμπορικού χαρακτήρα ή 'spam'. Ανακτήθηκε από http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0028:FIN:EL:PDF

[14] Spam Evolution 2013 (n.d.). Ανακτήθηκε από http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf

[15] Anti-spam techniques (2014, March 14). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Anti-spam_techniques

[16] What Is a Spam Filter? (n.d.). Ανακτήθηκε από: http://www.wisegeek.com/what-is-a-spam-filter.htm

[17] Kenichi Yoshida, Fuminori Adachi, Takashi Washio, Hiroshi Motoda, Teruaki Homma, Akihiro Nakashima, Hiromitsu Fujikawa, Katsuyuki Yamazaki (n.d.). Density-Based Spam Detector. published in IEICE TRANSACTIONS on Information and Systems Vol.E87-D No.12 pp.2678-2688. Ανακτήθηκε από: http://www.msci.memphis.edu/~linki/7118papers/Yoshida04DensityBasedSpam.pdf

[18] Joon S. Park*, Hsin-Yang Lu and Chia-Jung Tsui (2009). Anti-Spam Approaches: Analyses and Comparisons. published in The Open Information Systems Journal, 2009, 3, 36-47. Ανακτήθηκε από: http://benthamopen.com/toisj/articles/V003/36TOISJ.pdf

[19] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati (n.d.). P2P-Based Collaborative Spam Detection and Filtering. published in Peer-to-Peer Computing, 2004. Proceedings. Fourth International Conference on 25-27 Aug. 2004 pp. 176 – 183, IEEE. Ανακτήθηκε από: http://spdp.di.unimi.it/papers/ieee_p2p.pdf

[20] Gordon V. Cormack (2008). Email Spam Filtering: A Systematic Review. published in Journal Foundations and Trends in Information Retrieval Volume 1 Issue 4, April 2007 pp. 335-455. DOI: 10.1561/1500000006

[21] Saima Hasib, Mahak Motwani, Amit Saxena (2012). Anti-Spam Methodologies: A Comparative Study. published in International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5341-5345. Ανακτήθηκε από: http://www.ijcsit.com/docs/Volume%203/vol3Issue6/ijcsit2012030611.pdf

[22] DNSBL (2014, July 8). Ανακτήθηκε από: http://en.wikipedia.org/wiki/DNSBL

[23] Challenge – response spam filtering (2014, June 14). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Challenge-response_spam_filtering

[24] Bayesian Spam Filtering (2014, June 30). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Bayesian_spam_filtering

[25] Spam and Anti-spam techniques (2014, January 6). Ανακτήθηκε από: http://resources.infosecinstitute.com/spam-anti-spam-techniques/

[26] Stopping Spam (2003). Ανακτήθηκε από: http://www.paulgraham.com/stopspam.html

[27] Hasan ShojaaAlkahtani, Paul Gardner- Stephen, Robert Goodwin (n.d.). A taxonomy of email spam filters. published in The 12th International Arab Conference on Information Technology (ACIT). 2011. pp. 351-356. Ανακτήθηκε από: http://www.nauss.edu.sa/acit/PDFs/f3064.pdf

[28] Yves Deswarte, Frederic Cuppens, Susbil Jajodia, Lingyu Wang (2004). Security and Protection in Information Processing Systems. published in IFIP 18th World Computer Congress TC11 19th International Information Security Conference 22–27 August 2004 Toulouse, France. DOI: 10.1007/978-1-4020-8143-9

[29] Ten Spam-Filtering Methods Explained (2006). Ανακτήθηκε από: http://www.techsoupcanada.ca/learning_center/10_sfm_explained

[30] Di Xu (2010). Solutions to Spam. PhD Thesis. Hochschule Furtwangen. Ανακτήθηκε από: http://webuser.hs-furtwangen.de/~heindl/ebte-2010ws-Is%20there%20solution%20of%20email%20 Spam.pdf

[31] Deb Shinder (2008). The Pros and Cons of Behavioral Based, Signature Based and Whitelist Based Security. Ανακτήθηκε από: http://www.windowsecurity.com/articles-tutorials/misc_network_security/Pros-Cons-Behavioral-Signature-Whitelist-Security.html

[32] Sherasiya Firozbhai A. (2014). An Improved Spam Filter for Filtering Repeated Spam E-mails. Ανακτήθηκε από: http://www.ijaerd.co.in/Current%20Issue/Volume%201%20Issue%205/ijaerd%2014-097.pdf

[33] David Erickson, Martin Casado, Nick McKeown (n.d.). The Effectiveness of Whitelisting: a User-Study. publiched in CEAS. 2008 Ανακτήθηκε από: http://www.ceas.cc/2008/papers/ceas2008-paper-20.pdf

[34] Greylisting (2014, July 2). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Greylisting

[35] GFI White Paper (2011). Why Bayesian filtering is the most effective anti-spam technology. Ανακτήθηκε από: http://www.gfi.com/whitepapers/why-bayesian-filtering.pdf

[36] Guido Schryen (2007). Anti-Spam Measures, Analysis and Design. Aachen published by Springer Berlin Heidelberg, 2007

[37] Opt-in email (2014, July 19). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Opt-in_email

[38] Madeleine de Cock Buning, Ewoud Hondius, Corien Prins and Marc de Vries (2001). Consumer@Protection.EU. An Analysis of European Consumer Legislation in the Information Society. published in Journal of Consumer Policy, Volume 24, Issue 3-4 , pp. 287-338, Netherlands by Kluwer Academic Publishers. DOI: 10.1023/A:1013965627370

[39] ΟΔΗΓΙΑ 2/2011 (2011). Ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL

[40] ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 (2002, July 12). Ανακτήθηκε από http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[41] ΝΟΜΟΣ 3471/2006 (ΦΕΚ 133/Α'/28.6.2006). Ανακτήθηκε από http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/%CE%9D3471_06.PDF

[42] Filtering your spam (2008, Jun 22). Ανακτήθηκε από http://rickconner.net/spamweb/filtering.html

[43] CAPTCHA (2004, June 9). Ανακτήθηκε από https://www.drupal.org/project/captcha

[44] Manage User Spam Settings (n.d). Ανακτήθηκε από: http://www.rackspace.com/apps/support/portal/1709

[45] Overarching Anti-Spam Frameworks in the United States, Canada, and the European Union (n.d). Ανακτήθηκε από http://www.law.cornell.edu/wex/inbox/anti-spam_frameworks_international_table

[46] Email spam legislation by country (2014). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Email_spam_legislation_by_country

[47] Secure your inbox (n.d.). Ανακτήθηκε από: https://antispam.yahoo.com/?tool=1

[48] Spam & Virus Protection (n.d.). Ανακτήθηκε από: http://www.dotcomhost.com/menu/spam_filtering/index.shtml

[49] Fighting Junk Email (n.d.). Ανακτήθηκε από: https://mail.live.com/mail/junkemail.aspx

[50] About Gmail (n.d.). Ανακτήθηκε από: http://www.gmail.com/intl/en/mail/help/fightspam/spamexplained.html

[51] Web Mail Provider, Spam Filtering Effectiveness Research (2012). Ανακτήθηκε από: http://www.cascadeinsights.com/wp-content/uploads/2012/02/Web_Mail_Provider_SPAM_Filtering_Effectiveness_Research.pdf

[52] Adult Content in Spam (n.d.). Ανακτήθηκε από: http://www.spamlaws.com/adult-spam.html

[53] Spam and Privacy Issues (2006, March 30). Ανακτήθηκε από: http://privacy.org.nz/assets/Files/1490516.pdf

[54] Whitelist (2014, August 20). Ανακτήθηκε από: http://en.wikipedia.org/wiki/Whitelist

[55] Garcia, F. D., Hoepman, J. H., & Van Nieuwenhuizen, J. (2004). Spam filter analysis. published in Security and Protection in Information Processing Systems (pp. 395-410). Springer US. Ανακτήθηκε από: http://arxiv.org/pdf/cs/0402046.pdf

[56] SpamAssasin (2014, August 25). Ανακτήθηκε από: http://en.wikipedia.org/wiki/SpamAssassin