ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΝΕΠΙΘΥΜΗΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΜΗΝΥΜΑΤΑ: ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΑΝΤΙΜΕΤΡΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Νικόλαου Βελιμαχίτη

Επιβλέπων : Μαρία Καρύδα

Μέλη εξεταστικής επιτροπής: Γ. Καμπουράκης, Σ. Κοκολάκης

Σάμος, [Μάρτιος 2020]

Πρόλογος και ευχαριστίες

Η εργασία αυτή εκπονήθηκε το ακαδημαϊκό έτος 2019-2020 στο τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων του Πανεπιστημίου Αιγαίου. Θα ήθελα να ευχαριστήσω την καθηγήτριά μου κ. **Μ. Καρύδα** για την πολύτιμη βοήθειά της. Ακόμα, τον κ. **Γ. Καμπουράκη** και τον κ. **Σ. Κοκολάκη** οι οποίοι είχαν την καλή θέληση να συμμετάσχουν στην εξεταστική επιτροπή.

Πίνακας περιεχομένων

Περίληψη

Ανεπιθύμητο ηλεκτρονικό μήνυμα ή spam, όπως αλλιώς ονομάζεται, είναι ένα αυξανόμενο πρόβλημα στο διαδίκτυο. Το πρόβλημα στην περίπτωση αυτή είναι ότι με τον καιρό όλο και περισσότεροι χρήστες λαμβάνουν μεγαλύτερες ποσότητες ανεπιθύμητων μηνυμάτων , το οποίο κοστίζει τόσο σε χρόνο όσο και σε χρήματα. Αυτό το πρόβλημα οφείλεται στο γεγονός ότι το ηλεκτρονικό ταχυδρομείο σχεδιάστηκε και βασίστηκε σε σχέσεις αμοιβαίας εμπιστοσύνης μεταξύ των χρηστών. Έτσι, αργότερα όλες οι ελλείψεις ασφάλειας και ιδιωτικότητας χρησιμοποιήθηκαν από κακόβουλους χρήστες με πολλαπλούς τρόπους, όπως για παράδειγμα spam (ανεπιθύμητη αλληλογραφία), DOS (άρνηση παροχής υπηρεσιών), κ.α. , ώστε να αποσκοπούν σε λειτουργικά, οικονομικά ακόμη και σε πολιτικά συμφέροντα. Επίσης από τα πιο διαδεδομένα spam μηνύματα είναι αυτά που περιέχουν διαφημιστικό υλικό, ψευδείς ειδοποιήσεις ιών ή ψευδείς επιβεβαιώσεις πολιτικών ασφαλείας του αντίστοιχου τομέα, εταιρείας, οργανισμού, κράτους και πολλών άλλων κλάδων.

Τα emails τα οποία στέλνονται από ένα αποστολέα προς πολλές διευθύνσεις ονομάζονται UBE (μη-ενοποιημένο μαζικό μήνυμα). Αυτού του είδους τα μηνύματα, εμπορικής φύσεως σημασίας ονομάζονται UCE (μη-ενοποιημένο εμπορικό μήνυμα). Στις περισσότερες περιπτώσεις αυτά τα μηνύματα θεωρούνται spam. Αξίζει να σημειωθεί ότι ένα τεράστιο ποσοστό της κυκλοφορίας των μηνυμάτων μέσω ηλεκτρονικών ταχυδρομείων είναι spam. Αυτό το ποσοστό στις μέρες μας αγγίζει σύμφωνα με έρευνες το 70-80%. **[1]**

Abstract

The aim of this thesis is to study the ways according to which spam emails can be transmitted, the threats that such emails can conceal but also the impact of these spam emails have in large organizations and ordinary users who prefer to use emails as a mean of communication, instead of other alternatives ways. Reference will also be made to the legal and institutional framework of Greece, as well as to other states. We will also formulate, analyze and evaluate the various countermeasures (technical or non-technical) to face this threat.

1 *Εισαγωγή*

1.1 Ανεπιθύμητα μηνύματα: τρόποι μετάδοσης, απειλές, επιπτώσεις, θεσμικό πλαίσιο και μέτρα προστασίας.

Σκοπός της εργασίας αυτής είναι να μελετήσουμε τους τρόπους με τους οποίους μπορούν να μεταδοθούν, τις απειλές που μπορεί να κρύβουν τέτοιου είδους μηνύματα αλλά επίσης και τις επιπτώσεις που έχουν αυτά τα spam emails τόσο σε έναν μεγάλο οργανισμό όσο και σε απλούς χρήστες οι οποίοι προτιμούν να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ως μέσο επικοινωνίας, αντί άλλων εναλλακτικών μέσων. Ακόμα θα διατυπώσουμε, θα αναλύσουμε και θα αξιολογήσουμε τα διάφορα αντίμετρα που μπορεί να υπάρξουν (τεχνικά ή μη τεχνικά μέτρα προστασίας) για την αντιμετώπιση αυτού του είδους την απειλή.

1.2 Δομή της διπλωματικής

Η εργασία θα εξηγήσει κατ' αρχάς τι είναι τα ανεπιθύμητα μηνύματα και με ποιους τρόπους μπορούν να μεταδοθούν. Έπειτα, πρέπει να αναφέρουμε και να εξηγήσουμε τις απειλές που μπορεί να κρύβουν τέτοιου είδους μηνύματα. Ακόμα θα εστιάσουμε σε ένα σημαντικό παράγοντα των μηνυμάτων αυτών, που δεν είναι κάτι άλλο από τις επιπτώσεις που φέρουν στον ιδιωτικό τομέα. Στην συνέχεια θα αναλύσουμε και το θεσμικό πλαίσιο που υπάρχει στην χώρα μας για την ανεπιθύμητη αλληλογραφία, αλλά και σε άλλες χώρες. Έπειτα θα αναφέρουμε κάποια σημαντικά τεχνικά μέτρα προστασίας αλλά και κάποια από τα σημαντικότερα μη τεχνικά μέτρα προστασίας. Τέλος, υπάρχουν κάποια γενικά συμπεράσματα της εργασίας αυτής.

2 *Τρόποι μετάδοσης και απειλές ανεπιθύμητων μηνυμάτων*

2.1 Ηλεκτρονικά και ψηφιακά ανεπιθύμητα μηνύματα. Τρόποι μετάδοσης τους.

Τα ανεπιθύμητα μηνύματα μπορούν να μεταφερθούν και να διαδοθούν με διάφορους τρόπους αλλά ο όρος συνήθως αναφέρεται σε μηνύματα ηλεκτρονικού ταχυδρομείου. Ενώ όμως γενικότερα τα spam αναφέρονται συνήθως σε ηλεκτρονικού ταχυδρομείου μηνύματα (emails), υπάρχει μία εξελισσόμενη απειλή που έχει εξαπλωθεί πλέον σε όλους σχεδόν τους τύπους των επικοινωνιών, συμπεριλαμβανομένων των sms, μηνύματα post σε κοινωνικά μέσα, συστήματα ανταλλαγής άμεσων μηνυμάτων και ακόμα και σε επικοινωνιακά forum. Πέρα από την ενόχληση και την σπατάλη χρόνου που δημιουργούν, τα μηνύματα αυτά μπορούν να προκαλέσουν σημαντική ζημιά σε υπολογιστικά συστήματα, μολύνοντάς τους με κακόβουλο λογισμικό ικανό ακόμα και να υποκλέψει προσωπικά στοιχεία. Οι γνωστοί “spammers” είναι αρκετά εφευρετικοί και αμείλικτοι. Κατασκευάζουν συνεχώς όλο και πιο ελκυστικό δόλωμα ώστε να προσελκύσουν τους χρήστες να ανοίξουν τα μηνύματα που περιέχουν κακόβουλο λογισμικό. Επίσης, ακόμα μία τακτική τους είναι να προσπαθούν συνεχώς να βρίσκουν νέες λίστες διευθύνσεων ηλεκτρονικού ταχυδρομείου και νέα μέσα επικοινωνίας να στοχεύσουν.

Τα ανεπιθύμητα μηνύματα, πιο συγκεκριμένα, εκμεταλλεύονται συνήθως αδυναμίες του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol). Το SMTP είναι ένα standard πρωτόκολλο που λειτουργεί μεταξύ δύο επικοινωνούντων μέσων μεταφοράς μηνυμάτων ή όπως ονομάζεται αλλιώς Message Transfer Agent (MTA) χρησιμοποιώντας ένα προκαθορισμένο σύνολο εντολών. Ο MTA αποστολέας δέχεται μηνύματα από τελικούς χρήστες και τα παραδίδει στον αντίστοιχο MTA του παραλήπτη χρησιμοποιώντας και αυτός το SMTP. Δηλαδή, ο MTA αποστολέας εντοπίζει την IP του MTA δέκτη μέσω ενός ερωτήματος στον DNS server. Όμως το SMTP και η εφαρμογή του έχει και αδυναμίες τις οποίες εκμεταλλεύονται οι spammers ώστε να στείλουν τα μηνύματα αυτά. Το σημαντικότερο είναι ότι το πρωτόκολλο αυτό δεν έχει κανέναν έλεγχο ταυτότητας του αποστολέα για να επαληθεύσει την αυθεντικότητά του. Ακόμα υπάρχουν και διάφορα

άλλα ελαττώματα του συγκεκριμένου πρωτοκόλλου όπως: open relays και open proxies που χρησιμοποιούνται από τους αποστολείς ανεπιθύμητων μηνυμάτων.

Έναν SMTP διακομιστής λέγεται ότι είναι ενεργός με δυνατότητα αναμετάδοσης ή αλλιώς “relay-enabled” αν δέχεται μηνύματα ηλεκτρονικού ταχυδρομείου από οποιονδήποτε τομέα (εκτός καθορισμένης λίστας διευθύνσεων) και τα προωθεί. Οπότε, οι αποστολείς των ηλεκτρονικών μηνυμάτων χρησιμοποιούν το SMTP για να επικοινωνήσουν με τον παραπάνω διακομιστή, όπου αυτός έπειτα προωθεί τα μηνύματα αυτά στους παραλήπτες. Συνήθως, πλέον αυτοί οι ενδιάμεσοι διακομιστές χρησιμοποιούν διάφορους μηχανισμούς ασφαλείας για την εξακρίβωση της ταυτότητας των χρηστών που στέλνουν τα διάφορα μηνύματα. Όταν όμως δεν υπάρχει κάποιος μηχανισμός επαλήθευσης από τους ενδιάμεσους διακομιστές και οποιοσδήποτε αποστολέας μπορεί να στείλει την αλληλογραφία του σε οποιονδήποτε παραλήπτη, κάτι που ήταν σύνηθες στο παρελθόν διότι οι προηγούμενες εκδόσεις των περισσότερων λογισμικών που χρησιμοποιούσαν SMTP είχαν από προεπιλογή την αναμετάδοση ανοικτή ή αλλιώς “relay-open”, οι spammers με την βοήθεια του αυτού του open relay, το οποίο δεν περιορίζει τον πελάτη από την προώθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου από έναν τομέα σε έναν άλλο, μπορούσαν να στείλουν τα ανεπιθύμητα μηνύματά τους ανώνυμα παρακάμπτοντας τα φίλτρα ανεπιθύμητης αλληλογραφίας.

Αντίστοιχο με τα “open relays” είναι και τα “open proxies”. Ένας διακομιστής μεσολάβησης πρέπει να δέχεται μηνύματα και αιτήματα μόνο από τους δικούς του πελάτες, είτε αναγκάζοντάς τους να συνδεθούν από ένα συγκεκριμένο εύρος IP διευθύνσεων είτε χρησιμοποιώντας κάποιον έλεγχο ταυτότητας. Αν ο διακομιστής δεν περιορίζει την βάση πελατών του σε δικό του σύνολο από χρήστες και επιτρέπει σε οποιονδήποτε πελάτη να το χρησιμοποιεί ονομάζεται ανοικτός διακομιστής μεσολάβησης ή “open proxy server”. Ένας τέτοιος διακομιστής θα μπορεί να δέχεται συνδέσεις πελατών από οποιαδήποτε IP διεύθυνση και θα του επιτρέπει να κάνει συνδέσεις σε κάθε πόρο του διαδικτύου. Οπότε, οι διακομιστές αυτοί λειτουργούν ως τυφλοί ενδιάμεσοι σε άλλες διευθύνσεις δικτύου χωρίς έλεγχο ταυτότητας. Έτσι τα “open proxies” χρησιμοποιούνται από τους αποστολείς ανεπιθύμητης αλληλογραφίας για μαζική αποστολή με πλαστές ταυτότητες. Επίσης, ένας ανοικτός διακομιστής μεσολάβησης μπορεί να χρησιμοποιηθεί από έναν spammer για να συνδεθεί ανώνυμα σε έναν διακομιστή αλληλογραφίας. Επιπλέον, οποιαδήποτε αλληλογραφία στέλνεται με αυτόν τον τρόπο εμφανίζεται στον παραλήπτη να προέρχεται από τον proxy server και όχι από την πραγματική IP. Επίσης ένας ανοικτός διακομιστής μεσολάβησης μπορεί να χρησιμοποιηθεί για να παρακάμψει διάφορα φίλτρα που εστιάζουν τόσο στο όνομα του τομέα (domain name) όσο και στην IP διεύθυνση (IP address).

Μία άλλη τακτική των κακόβουλων χρηστών είναι οι μηχανές “spam zombies”. Οι μηχανές αυτές είναι συνήθως υπολογιστές με ευρυζωνική σύνδεση όπου κυβερνούνται από “Trojan Remote Access” (RAT) και μπορούν να ενεργοποιηθούν εξ αποστάσεως από τους επιτιθέμενους για να ξεκινήσουν μια μαζική επίθεση εναντίον κάποιου στόχου. Έτσι, οι spammers εκμεταλλεύονται τα συστήματα αυτά αφού υπολογίζεται ότι περίπου το 1/3 των ανεπιθύμητων μηνυμάτων προέρχονται από αυτά. Επίσης τα συστήματα αυτά έχουν χρησιμοποιηθεί κατά καιρούς και κατά των spammers. **[2]**

Τώρα, από μια άλλη οπτική γωνία μπορούμε τα διακρίνουμε τα ανεπιθύμητα μηνύματα ή spam σύμφωνα με τους 4 πιο γνωστούς τρόπους εκδοχής τους.

- **Spoofed Name-** Αυτή η εκδοχή είναι η συνηθέστερη και αντιπροσωπεύει το 75% των επιθέσεων. Χρησιμοποιείται το όνομα του spoofed στελέχους στο πεδίο «from». Όμως η διεύθυνση του email προέρχεται από εξωτερική υπηρεσία, όπως το Hotmail, και ανήκει στον επιτιθέμενο.
- **Reply-To Spoofing-** Αυτή η τεχνική χρησιμοποιεί το πραγματικό όνομα και email του αποστολέα που πλαστοπροσωπείται. Το όνομα στο «Reply-to» χρησιμοποιεί επίσης το όνομα του πλαστοπροσωποποιημένου αποστολέα. Όμως η διεύθυνση «απάντηση σε», όπου αποστέλλονται οι απαντήσεις, ανήκει στον επιτιθέμενο.
- **Spoofed Sender (with No Reply-to address)-** Αυτή η μορφή απάτης μέσω email χρησιμοποιεί το όνομα και το email του spoofed στελέχους. Όμως το μήνυμα δεν περιλαμβάνει διεύθυνση «Απάντηση σε», οπότε είναι αδύνατη η αμφίδρομη αλληλογραφία. Το μήνυμα συχνά περιλαμβάνει οδηγίες μεταφοράς χρημάτων, που καταργούν την ανάγκη για περεταίρω διευκρινήσεις.
- **Lookalike Domain-** Σε αυτήν την μορφή απάτης μέσω email, η διεύθυνση «Από» του επιτιθέμενου έχει παρόμοια εμφάνιση με αυτή του πλαστοπροσωποποιημένου στελέχους. Το παρόμοιο domain μπορεί να διαφέρει μόνο προς ένα γράμμα από το πραγματικό. Για παράδειγμα, το metronlogistics.com μπορεί να γίνει metronlogstics.com. **[3]**

    - Εκτός από όλα αυτά όμως, μια καλή ερώτηση είναι το γιατί πετυχαίνει η απάτη αυτή μέσω των emails;

Για τους κυβερνοεγκληματίες, η διαφορά μεταξύ επιτυχίας και αποτυχίας μπορεί να εξαρτάται από το πόσο καλά έχουν μελετήσει τον οργανισμό, ιδιωτικό ή κρατικό, όπου επιτίθονται, αν στοχεύει στους σωστούς ανθρώπους και επίσης να χρονομετρήσει την παράδοση των spoof emails. Εκτός από να μιμούνται την εμφάνιση κάποιου νόμιμου email, οι κυβερνοεγκληματίες χρησιμοποιούν και δοκιμασμένα ψυχολογικά κόλπα. Εκμεταλλεύονται το πάθος των υπαλλήλων να ευχαριστήσουν τους ανωτέρω τους, δημιουργώντας μία ψευδή αίσθηση ανάγκης για ταχύτητα και μυστικότητα. Τα spoof emails συνήθως καταφθάνουν όταν λείπουν οι υπεύθυνοι από το γραφείο, κάνοντας έτσι δύσκολη την επαλήθευσή τους. Εναλλακτικά μπορούν να καταφθάνουν σε ώρες αιχμής, όταν τα θύματα συνήθως κάνουν πολλές δουλειές μαζί, και δίνουν λιγότερη προσοχή στις απειλές των απατών μέσω email. Για τους κυβερνοεγκληματίες, η απάτη μέσω email προσφέρει μία ευκαιρία χαμηλού ρίσκου και υψηλού κέρδους. Δεν απαιτεί καμία ακριβή υποδομή, και εφόσον οι επιθέσεις συνήθως ξεπερνούν τα όρια μεταξύ χωρών, λίγοι είναι αυτοί που διώκονται ποινικά.

    - Ποιοι είναι όμως στην πραγματικότητα αυτοί που χρησιμοποιούν τα ανεπιθύμητα μηνύματα στην Ελλάδα;

Σε αρκετές χώρες τα ανεπιθύμητα μηνύματα αποτελούν ένα από τα μεγαλύτερα προβλήματα στη διαδικτυακή ζωή πολλών χρηστών και στην πλειοψηφία των επιχειρήσεων. Στην Ελλάδα το πρόβλημα αυτό βρισκόταν σε πολύ πιο περιορισμένο επίπεδο το 1995 όταν έκανε την εμφάνιση του . Την τελευταία δεκαετία όμως η χώρα μας έχει γνωρίζει τρομερή αύξηση, όπου αίσθηση είχε προκαλέσει και η εκτίμηση του στελέχους της Symantec, Ηλία Χάντζου (*ότι το 53% των e-mails που λαμβάνουν οι Έλληνες χρήστες* είναι spam) και παρά το νομοθετικό πλαίσιο που υπάρχει, σαφώς όμως δεν μπορεί να υπάρξει εφησυχασμός.

Οι ομάδες spammer και ένα ποσοστό από τους υπόλοιπους, για να αποφύγουν τις νομικές και οικονομικές συνέπειες των πράξεων τους, πλαστογραφούν τις ηλεκτρονικές διευθύνσεις τους ώστε να μην είναι δυνατός ή να είναι αρκετά δύσκολος ο εντοπισμός τους. Τις περισσότερες φορές, η ηλεκτρονική διεύθυνση και το όνομα που παρουσιάζεται ως ο αποστολέας των ανεπιθύμητων ηλεκτρονικών μηνυμάτων είναι κάποιος, εντελώς αθώος, χρήστης του διαδικτύου, του οποίου χρησιμοποιήθηκε εν αγνοία του η ηλεκτρονική διεύθυνσή του.

Η πιο συνηθισμένη τακτική των spammers είναι η αποστολή υπερβολικά μεγάλου αριθμού ανεπιθύμητων μηνυμάτων με συνεπεία να προκαλείται υπερφόρτωση της θυρίδας του ηλεκτρονικού ταχυδρομείου, με αποτέλεσμα να εμποδίζεται η είσοδος επιθυμητών και σημαντικών για το χρήστη μηνυμάτων. Εκτός αυτού, καλείται να ανεχθεί και χαμηλότερες ταχύτητες λειτουργίας του διαδικτύου λόγω της επιβάρυνσης του διακομιστή. Αυτό έχει σαν συνέπεια να μπλοκάρει ο λογαριασμός του από τις επιστροφές των ανεπίδοτων ανεπιθύμητων ηλεκτρονικών μηνυμάτων (κάθε αποστολή ανεπιθύμητου μηνύματος, περιλαμβάνει χιλιάδες ή και εκατομμύρια διευθύνσεις, πολλές από τις οποίες έχουν καταργηθεί) από τις εκατοντάδες και χιλιάδες διαμαρτυρίες των παραληπτών του spam.

Οι spammers επιστρατεύουν πλήθος τακτικών (harvesting) **[4]** για να αποκτήσουν διευθύνσεις ηλεκτρονικού ταχυδρομείου, όπως είναι η συλλογή διευθύνσεων από mailing lists ή από ιστότοπους κοινωνικής δικτύωσης (social networking sites) με τη χρήση ειδικού λογισμικού που ανιχνεύει το σύμβολο «@» ή με την μέθοδο του "*dictionary attack*", όπου ο spammer προσπαθεί να μαντέψει και να συνθέσει πραγματικές ηλεκτρονικές διευθύνσεις συνδυάζοντας τυχαία γράμματα ή λέξεις που αντλεί από το λεξικό. Ένας ιδιαίτερα διαδεδομένος τρόπος απόκτησης ηλεκτρονικών διευθύνσεων είναι η εξαγορά τους από άλλο spammer ή από εταιρίες που διαθέτουν αντίστοιχες βάσεις δεδομένων **[5]**. Χαρακτηριστική είναι η ευκολία με την οποία μπορεί να γίνει μια τέτοια αγοραπωλησία ακόμη και μέσω διαδικτύου, αφού αρκεί να πληκτρολογήσει κανείς στη μηχανή αναζήτησης (π.χ. στο Google) τη φράση "bulk email" για να εμφανιστούν αμέσως καταχωρήσεις όπως "*Buy email lists - email addresses - email marketing*". Η εμπορευματοποίηση προσωπικών δεδομένων στο διαδίκτυο έχει εδραιωθεί ως πρακτική, ενώ ο χαρακτηρισμός, της εν γένει διαδικασίας εξαγωγής πληροφοριών από μεγάλες βάσεις δεδομένων, γνωστός και ως "*data mining*" **[6]**, αποδεικνύει την αντιμετώπισή τους ως πολύτιμα «*κοιτάσματα*» τα οποία «*εξ ορύσσονται*».

Οι τεχνικές των spam εξελίσσονται. Οι spammers που παρακινούνται από τα οικονομικά οφέλη και το χαμηλότερο κόστος για την ανάπτυξη των spam, μαθαίνουν πως

λειτουργούν τα τρέχον anti-spam εργαλεία και υιοθετούν συνεχώς νέες τεχνικές που μπορούν να τα παρακάμψουν.

Το διαδίκτυο (υποδομή και χρήστες) στην Ελλάδα αναπτύσσεται συνεχώς, ακόμα όμως δεν μπορεί, εκ των πραγμάτων, να συγκριθεί με το διαδίκτυο των Η.Π.Α, της Γερμανίας ή της Μεγάλης Βρετανίας. Όπως έχουν δείξει έρευνες που δημοσιεύονται κατά καιρούς στις αθηναϊκές εφημερίδες, το ποσοστό των Ελλήνων που χρησιμοποιούν το διαδίκτυο είναι πολύ μικρό σε σχέση με την Ευρώπη. Πραγματικά δεν θα περίμενε κανείς να υπάρχουν Έλληνες spammers, αλλά από ότι φαίνεται όμως υπάρχουν αρκετοί webmasters και αρκετοί άλλοι επαγγελματίες που καταφεύγουν σε μεθόδους spam για να διαφημίσουν την ιστοσελίδα και τα προϊόντα τους.

Παρακάτω, παραθέτω μια πραγματική λίστα Ελλήνων spammer όπως αυτή ανακοινώθηκε από το site freestuff.gr **[7]** *στις 30/07/2009.*

afrogo@ath.forthnet.gr

ajamfam@crosswind.net

bf@globalgreece.gr

bgca@otenet.gr

club@plus4u.gr

delphigroup@myfastmail.com

entypanetpromo@yahoo.gr

f.papapetrou@gmail.com

home@homed.gr

inbox@e-travelling.gr

info@autoscan.gr

info@futurebs.com

info@geegle.gr

info@networknews.gr

info@oikodomein.gr

info@onbusinessbook.com

info@refink.gr

info@safe-shop.gr

info@yourbaby.gr

intron112@yahoo.gr

jenios114@gmail.com

mani1@otenet.gr

marketing@desm.gr

mmantousis@praxi.gr

mshop@mshop.gr

news@e-poema.eu

newsletter@detoxcenter.gr

newsletter@my-space.gr

noreply@computron-ypologistes.com

noreply@economico.gr

noreply@mailinglist.gr

press@greekliberals.net

salesprivelife@gmail.com

seminars@agsseminars.gr

sofo10@hol.gr

tiodastribuidores@lafloristeria.com

vagelisk@salesmanager.gr

veitas@alfredograf.com

ventlapaz@naturexbolivia.com

2.2 Απειλές που μπορεί να κρύβουν αυτά τα ανεπιθύμητα μηνύματα.

Συνήθως αποτελούν την συχνότερη απειλή στο διαδίκτυο. Τέτοιου είδους μηνύματα μπορεί να είναι διαφημιστικά, για διαδικτυακά αγαθά, πορνογραφικού περιεχομένου, τζόγου, dating, ψεύτικες ειδοποιήσεις για ιούς, φιλανθρωπικές δωρεές κ.ο.κ. και περιέχουν γενικούς κινδύνους όπως:

- Ιούς και spyware που θα «προσβάλλουν» τον υπολογιστή του θύματος, πιθανώς θα υποκλέψουν διάφορα δεδομένα και δεν αποκλείεται ακόμα και να καταστρέψουν πολύτιμα αρχεία.
- Πιθανώς να αποτελούν «όχημα» για διαδικτυακές απειλές, όπως το phishing.
- Επίσης το ανεπιθύμητο email μπορεί να περιέχει ακατάλληλο περιεχόμενο.

Αναλυτικότερα τώρα έχουμε:

Phishing επιθέσεις, οι οποίες προσπαθούν να πείσουν τα θύματά τους να ανοίξουν κάποιο επισυναπτόμενο, όπου περιέχει συνήθως κάποιο κακόβουλο πρόγραμμα, ή τα ξεγελούν ώστε να εισάγουν τους κωδικούς τους ή άλλες ευαίσθητες πληροφορίες σε κάποιου είδους φόρμα. Τις περισσότερες φορές, τα phishing emails φαίνεται να έρχονται από αυθεντικές πηγές και αναφέρονται σε σημαντικά ζητήματα, ώστε να τραβήξουν την προσοχή του θύματος και να το «αναγκάσουν» να δώσει κάποια στοιχεία ή να ανοίξει κάποιο σύνδεσμο κλπ. Στόχος των spammers είναι η απόσπαση ευαίσθητων πληροφοριών, όπως στοιχεία τραπεζικού λογαριασμού, κωδικοί πρόσβασης στα κοινωνικά μέσα και άλλα.

Ακόμα, spoofing είναι μία μέθοδος η οποία ουσιαστικά πλαστογραφεί την διεύθυνση email των ανθρώπων από το περιβάλλον του θύματος, ώστε να φαίνεται ότι λαμβάνει κάποιο email από αυτούς. Στόχος των spammers είναι για άλλη μία φορά να διαδώσουν κάποιο κακόβουλο λογισμικό, χωρίς να κινήσουν υποψίες, αφού το θύμα νομίζει ότι ανοίγει το email ενός γνωστού του προσώπου.

Επιπλέον ο πιο γνωστός τρόπος για την εγκατάσταση κάποιου κακόβουλου λογισμικού στο σύστημα του θύματος είναι τα επισυναπτόμενα αρχεία ή σύνδεσμοι σε email. Μέσω των επισυναπτόμενων, οι spammers μπορούν να πραγματοποιήσουν πολλές διαφορετικές επιθέσεις και να αποκτήσουν πλήρη πρόσβαση στο σύστημα.

Επίσης μια άλλη γνωστή απειλή είναι και η παραβίαση εταιρικών email ή αλλιώς “whaling”, όπως ονομάζεται. Οι εταιρίες και οι επιχειρήσεις, ανεξαρτήτου μεγέθους, πέφτουν όλο και πιο συχνά θύματα επιθέσεων από spammers και hackers. Συνήθως, οι επιτιθέμενοι χρησιμοποιούν συγκεκριμένες μεθόδους, που ξεγελούν τους υπαλλήλους των εταιριών. Προσποιούνται κάποιο συνεργάτη και ζητούν την μεταφορά μεγάλων χρηματικών ποσών.

Για να πραγματοποιηθούν όλες αυτές οι επιθέσεις όμως, οι κακόβουλοι χρήστες πρέπει να ανακαλύψουν και να συλλέξουν διευθύνσεις email. Αυτό είναι το μεγάλο πρόβλημα των spammers. Δηλαδή δεν είναι αρκετό για έναν spammer να συλλέξει μεγάλους αριθμούς διευθύνσεων email. Η μεγάλη πρόκληση που έχει να αντιμετωπίσει, είναι να αποκτήσει αυτές τις διευθύνσεις χωρίς να κινδυνεύει να ανιχνευτεί. Αυτό μπορεί να το πετύχει με διάφορους τρόπους. Ένας από τους πιο συνηθισμένους είναι να υποκλέψει εταιρικές βάσεις δεδομένων εξασφαλίζοντας έτσι και ένα μεγάλο αριθμό διευθύνσεων προς χρήση. Το φιάσκο της Yahoo είναι ένα τρανταχτό παράδειγμα τέτοιας υποκλοπής που δημιούργησε τεράστιες ζημιές, τόσο σε ανυποψίαστους χρήστες, όσο και στις εταιρίες που υπέκλεψαν. Οι διακομιστές αλληλογραφίας καθώς και οι διακομιστές που φιλοξενούν λίστες διευθύνσεων είναι επίσης συχνά στο στόχαστρο των κυβερνοεγκληματιών, όπως είναι και διάφορες κοινωνικές ιστοσελίδες και φόρουμ. Εμφανίζοντας μια διαφήμιση σε μία μη ασφαλές ιστοσελίδα κοινωνικής δικτύωσης, ο spammer ή ο hacker μπορεί εύκολα να συλλέξει όλες τις επαφές των

εγγεγραμμένων χρηστών. Το phishing σε μέσα κοινωνικής δικτύωσης και οι επιθέσεις “man-in-the-middle” είναι δύο ακόμα συνήθεις τρόποι χρήσης του spam. Το πιο επικίνδυνο από όλα τα spam όμως, είναι το ransomware. Κάποια ransomware από την στιγμή που περνούν στο σύστημα του θύματος, προγραμματίζονται να συνδεθούν στους λογαριασμούς του και στην συνέχεια συλλέγουν όλες του τις επαφές και τις διαρρέουν σε έναν διακομιστή που ελέγχει ο κυβερνοεγκληματίας. Ένα γνωστό παράδειγμα είναι το “WannaCry”.

Οπότε ένα spam email μπορεί να εξαπολύσει μια κυβερνοεπίθεση. Τα μηνύματα που μεταφέρουν τα spam mails προσπαθούν να δελεάσουν τον χρήστη να ακολουθήσει τις οδηγίες τους, με σκοπό να μεταφέρουν κάποιο malware στην συσκευή του χρήστη. Το συνηθέστερο μοτίβο επίθεσης των spams που έχουν σκοπό να μεταδώσουν malware είναι το εξής: Το ανυποψίαστο θύμα ανοίγει το spam email. Το μήνυμα τον καθοδηγεί να κάνει “click” σε έναν σύνδεσμο που του δίνει και έπειτα συνδέεται σε μία ιστοσελίδα που είναι «μολυσμένη» με malware. Ένα δεύτερο σενάριο είναι ο χρήστης να κατεβάσει ένα συνημμένο αρχείο που έχει «μολυνθεί» με ένα “payload” που σαρώνει το σύστημά του για κενά ασφαλείας, συνδέεται στον διακομιστή του επιτιθέμενου και περιμένει εντολές. Στην συνέχεια η «μόλυνση» εξαπλώνεται σύμφωνα με το σχέδιο και τον σκοπό του spammer-hacker.

Πλέον στις μέρες μας υπάρχουν διάφοροι νέοι τρόποι εξαπάτησης και διαφθοράς μέσω των spam emails. Για παράδειγμα, μία νέα τέτοια απειλή είναι το λεγόμενο “Sextortion scam”. Τον τελευταίο καιρό έχει παρατηρηθεί αυτή η νέα απειλή, διεθνώς γνωστή ως απάτη μέσω σεξουαλικής εκβίασης (έτσι προκύπτει και το όνομά της), που εκδηλώνεται με μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε διάφορους αποδέκτες ανεξαρτήτου φύλου και ηλικίας, με σκοπό την εξαπάτησή τους. Ειδικότερα άγνωστοι δράστες με την χρήση απατηλών λογαριασμών ηλεκτρονικού ταχυδρομείου, στέλνουν μαζικά μηνύματα σε αποδέκτες και τους ενημερώνουν ότι γνωρίζουν τους κωδικούς ασφαλείας (password) τους. Παράλληλα τους γνωστοποιούν ότι έχει εγκατασταθεί κακόβουλο λογισμικό, μετά από την επίσκεψή τους σε κάποιον ιστότοπο, το οποίο έχει ενεργοποιήσει την κάμερά και τους έχει καταγράψει σε προσωπικές στιγμές. Στην συνέχεια αναφέρεται ότι το κακόβουλο λογισμικό έχει συλλέξει όλες τις επαφές των χρηστών από τα μέσα κοινωνικής δικτύωσης και οι δράστες απειλούν με την αποστολή του επίμαχου υλικού στις επαφές τους, σε περίπτωση που δεν λάβουν bitcoins (συνήθως επιθυμούν τέτοιου είδους πληρωμές με κρυπτονομίσματα, τα οποία δεν είναι ανιχνεύσιμα). Η προσπάθεια εκβίασης των θυμάτων με την απειλή δημοσιοποίησης αρχείων ερωτικού περιεχομένου αναφέρεται διεθνώς ως σεξουαλική εκβίαση “sextortion”. Σημειώνεται ότι τα εκβιαστικά αυτά μηνύματα ηλεκτρονικού ταχυδρομείου έχουν κυρίως αναφορές σε πραγματικούς κωδικούς ώστε οι χρήστες να πεισθούν για το αληθινό της απειλής. Ωστόσο, σύμφωνα με τους καταγγέλλοντες, τις περισσότερες φορές οι κωδικοί αυτοί είναι αρκετά παλιοί και δεν χρησιμοποιούνται πλέον, γεγονός που καταδεικνύει ότι προέρχονται από παλαιότερη διαρροή δεδομένων.

Οργανωμένο έγκλημα

Ο κατακλυσμός των spam που έχει πλήξει τα τελευταία χρόνια το Διαδίκτυο αποδίδεται από τους αναλυτές στο γεγονός ότι οι spammer αντεπιτίθενται με την ποσότητα στις

προσπάθειες των υπηρεσιών ασφαλείας να μπλοκάρουν τα μηνύματά τους. Η τακτική αποδεικνύεται επιτυχημένη: όσο περισσότερα είναι τα spam που εξαπολύονται, τόσο μεγαλύτερος φαίνεται να είναι ο αριθμός αυτών που ξεφεύγουν από τα φίλτρα και φθάνουν σε πραγματικούς παραλήπτες. Επί πλέον αυτό το σύστημα των spammers φαίνεται να αποδίδει και μεγάλα οικονομικά οφέλη. *«Οι έρευνές μας δείχνουν ότι το 8% -10% των ανθρώπων που λαμβάνουν spam αγοράζει τις υπηρεσίες ή τα προϊόντα που προφέρονται. Το ποσοστό μπορεί να μη φαίνεται πολύ μεγάλο, στην πραγματικότητα όμως είναι. Σημαίνει ότι στα 100 μηνύματα που στέλνει κανείς, βρίσκει από 8 ως 10 αγοραστές. Βρείτε την αναλογία σε χιλιάδες ή σε εκατομμύρια. Η δε αποστολή κοστίζει ελάχιστα ή, αν χρησιμοποιείτε botnet, απολύτως τίποτε»*. **[8]**

Το γεγονός ότι η μαζική αποστολή των ανεπιθύμητων μηνυμάτων είναι μια ιδιαίτερα προσοδοφόρα επιχείρηση απεικονίζεται επίσης, σύμφωνα με τους αναλυτές, στην απόλυτη εξειδίκευση που χαρακτηρίζει όλο και περισσότερο τις δραστηριότητες του είδους: άλλοι γράφουν τα προγράμματα Trojan που μετατρέπουν τους υπολογιστές σε ζόμπι, άλλοι γίνονται «κύριοι» των υπολογιστών-ρομπότ και άλλοι, συγκεκριμένα οι δημιουργοί spam, «νοικιάζουν» από τους τελευταίους χρόνο στα botnet για να προωθήσουν τα μηνύματά τους. Αυτό σημαίνει ότι ο κάθε τομέας αποδίδει αρκετά χρήματα ώστε κάποιος να προτιμά να ασχοληθεί αποκλειστικά με αυτόν.

Οι αρχές ασφαλείας μιλούν για μια καλά οργανωμένη μαφία η οποία κινείται και ανθεί γύρω από τα spam. *«Ναι, υπάρχουν οργανωμένες συμμορίες πίσω από τα spam και αυτές απασχολούν τις διωκτικές αρχές. Δεν είναι ακριβώς ο δικός μας τομέας, γνωρίζουμε όμως ότι υπάρχουν δίκτυα, τα περισσότερα εκ των οποίων βρίσκονται στη Ρωσία και στην Ανατολική Ευρώπη, πολλά είναι στη Μέση Ανατολή, στην Τουρκία...»*.. **[8]**

Η Spamhaus, διεθνής μη κερδοσκοπικός οργανισμός ο οποίος έχει στόχο να ανιχνεύει τους αποστολείς spam και να διευκολύνει τις διωκτικές αρχές, εκτιμά ότι το 80% των ανεπιθύμητων μηνυμάτων που κατακλύζουν καθημερινά τη Βόρεια Αμερική και την Ευρώπη προέρχεται από 200 συμμορίες «επαγγελματιών του spam». Τα ονόματα των αρχηγών και πολλών μελών τους περιλαμβάνονται στην περίφημη λίστα ROKSO (Μητρώο των γνωστών επιχειρήσεων spam), έναν κατάλογο με τους πλέον καταζητούμενους κακοποιούς στο Internet.

Προϊόντα spam

Παρά τον απίστευτο όγκο των spam, τα «αγαθά» που προσφέρονται μέσω των ανεπιθύμητων μηνυμάτων είναι ουσιαστικά περιορισμένα. Το μεγαλύτερο ποσοστό (25%) προωθεί προϊόντα, κυρίως φάρμακα και συμπληρώματα διατροφής, αντίγραφα επώνυμων ρούχων, αξεσουάρ και ρολογιών και άλλα σχετικά. Ειδικά τα φάρμακα και τα συμπληρώματα διατροφής προκαλούν ιδιαίτερη ανησυχία στις αρχές καθώς έχει διαπιστωθεί ότι στο μεγαλύτερο μέρος τους είναι πλαστά και επομένως άκρως επικίνδυνα για τη δημόσια υγεία. Επόμενη μεγάλη κατηγορία αποτελούν οι οικονομικές υπηρεσίες και η προσφορά επενδύσεων, στην πλειονότητά τους ύποπτες.

Το 19% απευθύνεται καθαρά σε «ενηλίκους». Όπως δημοσιεύεται στις στατιστικές του *Spam Filter Review* το 2006, αξίζει να σημειωθεί, ότι τα ποσοστά των spam ήταν πολύ μικρότερα από τα σημερινά - η αποστολή spam πορνογραφικού περιεχομένου ανερχόταν σε 2,5 δισ. μηνύματα την ημέρα. Κατ' αναλογία αυτό αντιστοιχεί στο 4,5% του ηλεκτρονικού ταχυδρομείου του μέσου χρήστη σε καθημερινή βάση.

Στο υπόλοιπο μέρος τους τα spam προσπαθούν να εξαπατήσουν με διάφορους τρόπους τους παραλήπτες τους, να τους παράσχουν ιατρικές υπηρεσίες - στην πλειονότητά τους θεραπείες αδυνατίσματος και επεμβάσεις παχυσαρκίας - και υπηρεσίες του Διαδικτύου. Μια από τις πιο μεγάλες πρόσφατες απάτες έλαβε χώρα με ένα απειλητικό μήνυμα που κυκλοφόρησε τον περασμένο Μάιο στις Ηνωμένες Πολιτείες. *«Με έχουν προσλάβει για να σε δολοφονήσω»* έγραφε ο σκοτεινός υπογράφων, υποτιθέμενος έμμισθος επαγγελματίας δολοφόνος. *«Δεν ξέρω γιατί θέλουν τον θάνατό σου, ξέρω όμως ότι σε παρακολουθούν»*. Το υποψήφιο θύμα καλούνταν, για να σώσει τη ζωή του, να τοποθετήσει χρήματα σε λογαριασμό.

Οι ποινές για τους spammer, όταν οι αρχές κατορθώνουν να τους συλλάβουν, είναι συνήθως εξαιρετικά αυστηρές. Αυτό όμως δεν αποθαρρύνει τους επαγγελματίες του τομέα: τα κέρδη ανέρχονται σε εκατομμύρια δολάρια, στερλίνες, ευρώ, γεν, ρούβλια, γιουάν.

Επίσης, για να αποδίδει και να απευθύνεται σε όσο το δυνατόν περισσότερους παραλήπτες η τέχνη των spam φροντίζει να προσαρμόζεται στις εξελίξεις. Τώρα πλήττει και δικτυακούς τόπους οι οποίοι ως πρόσφατα θεωρούνταν εκτός του ενδιαφέροντος της, όπως τα message boards, το YouTube ή το Skype, αλλά και τα κινητά τηλέφωνα.

Απειλές και στα κινητά

Στα κινητά τηλέφωνα τα spam μεταδίδονται με τη μορφή SMS και είναι γνωστά κυρίως ως mobile spam ή m-spam, αλλά και ως SMS spam ή SpaSMS. Η ιδιαιτερότητά τους έγκειται στο γεγονός ότι ο παραλήπτης τους είναι συνήθως υποχρεωμένος να τα ανοίξει προτού τα διαγράψει, με αποτέλεσμα να είναι διπλά ενοχλητικά. «Χτύπησαν» για πρώτη φορά ανάμεσα στο 2001 και στο 2002 στην Ιαπωνία, παραλύοντας κυριολεκτικά τα συστήματα της DoCoMo, της μεγαλύτερης εταιρείας κινητής τηλεφωνίας στη χώρα: οι γραμμές μπλοκάρισαν, οι οθόνες των χρηστών πάγωσαν και τα κινητά τους άρχισαν να καλούν από μόνα τους, διάφορους αριθμούς κλήσης έκτακτης ανάγκης.

Με την εξάπλωση των m-spam μέσω των κινητών τηλεφώνων, δεν άργησαν να κάνουν και την εμφάνισή τους στη Βόρεια Αμερική και στην Ευρώπη, όχι όμως στην ίδια έκταση. Για παράδειγμα, το 2004, μέσω Ρωσίας, ίππευσαν τον δούρειο ίππο των Trojan με έναν ιό ο οποίος πρόσβαλλε τους ηλεκτρονικούς υπολογιστές, έτσι ώστε να στέλνουν μηνύματα κειμένου σε κινητά τηλέφωνα. Ως αποτέλεσμα, και ανάλογα με το σύστημα τηλεφωνίας, πολλοί χρήστες είδαν έκπληκτοι τους λογαριασμούς τους να φουσκώνουν με την αποστολή SMS που οι ίδιοι δεν είχαν στείλει ποτέ.

Ακόμα μία συνηθισμένη μορφή spam στα κινητά τηλέφωνα είναι τα μηνύματα που προτρέπουν τον παραλήπτη τους να καλέσει έναν αριθμό. Ο αριθμός αυτός έχει συνήθως υψηλή χρέωση, την οποία εισπράττει ο κάτοχός του. Αν το θύμα ξεγελαστεί και κάνει το

τηλεφώνημα, θα βρεθεί να περιμένει στην αναμονή με τη χρέωση να τρέχει. Το άλλο διαδεδομένο είδος spam στα κινητά δεν έχει τη μορφή μηνύματος αλλά κλήσης. Είναι το περίφημο κόλπο με τις αναπάντητες κλήσεις: το spam είναι σχεδιασμένο ώστε να στέλνει κλήσεις οι οποίες «χτυπούν» μόνο μία φορά και καταχωρούνται ως αναπάντητες, αφήνοντας έναν αριθμό τηλεφώνου στην οθόνη. Ο ανυποψίαστος παραλήπτης καλεί για να δει ποιος του τηλεφώνησε και χρεώνεται προς όφελος των spammers.

Τα τελευταία χρόνια πολλοί αναλυτές προειδοποιούν ότι τα spam στην κινητή τηλεφωνία θα πάρουν ανάλογες διαστάσεις με αυτά του Internet. Άλλοι όμως διαφωνούν. Κύριο επιχείρημα είναι αυτό του κόστους. Στο Διαδίκτυο το κόστος είναι ελάχιστο έως μηδενικό, αν χρησιμοποιεί κανείς botnet. Το σύστημα αυτό δεν μπορεί όμως να λειτουργήσει στα κινητά τηλέφωνα, τα οποία χρεώνονται. Ακόμη και με τις χαμηλότερες χρεώσεις SMS που υπάρχουν στην αγορά, η αποστολή εκατομμυρίων μηνυμάτων καταλήγει να κοστίζει ακριβά.

3 *Επιπτώσεις και θεσμικά πλαίσια.*

3.1 Επιπτώσεις που φέρουν τα μηνύματα αυτά στον ιδιωτικό τομέα.

Οι απειλές που αντιμετωπίζουν συχνότερα οι επιχειρήσεις στα ηλεκτρονικά συστήματά τους είναι κατά κύριο λόγο malwares, spam και phishing.

Έτσι μπορούμε να πούμε σύμφωνα και από τα ευρήματα μιας παγκόσμιας έρευνας με τίτλο Global Corporate IT Security Risks, που γίνεται κάθε ένα ή δύο χρόνια από την εταιρία B2B International σε συνεργασία με την εταιρία Kaspersky Lab, ότι ενώ τα επίπεδα των επιθέσεων, καθώς εξελίσσεται η τεχνολογία, συνεχώς αυξάνονται περίπου το 1/3 των ιδιωτικών επιχειρήσεων δεν έχουν πλήρη προστασία. Η παραπάνω έρευνα έδειξε ότι:

Οι επιθέσεις που χρησιμοποιούν μια ποικιλία κακόβουλων προγραμμάτων, οι επιθέσεις phishing και το spam παραμένουν οι ψηφιακές απειλές που συναντούν πιο συχνά οι επιχειρήσεις. Την ίδια στιγμή, ο όγκος των κακόβουλων επιθέσεων και των μηνυμάτων spam αυξάνεται σημαντικά χρόνο με τον χρόνο. Ο όγκος των επιθέσεων spam είναι μεγάλος και αναφέρθηκε από το 77% των εταιρειών (σε παγκόσμιο επίπεδο παρόμοιες επιθέσεις αναφέρθηκαν από το 61% των εταιρειών, έναντι 55% του προηγούμενου έτους). Οι επιθέσεις phishing στοχοποίησαν το 46% των ελληνικών επιχειρήσεων (36% σε παγκόσμιο επίπεδο), με το phishing να παραμένει στην κορυφαία τριάδα των πιο διαδεδομένων απειλών που χρησιμοποιούνται σε εξωτερικές επιθέσεις ενάντια σε εταιρείες.

Οι κακόβουλες επιθέσεις είναι στην πραγματικότητα ο Νο 1 λόγος πίσω από τις σοβαρές διαρροές εμπιστευτικών δεδομένων — το 22% των εταιρειών παγκοσμίως και το 21% των εταιρειών στην Ελλάδα ανέφεραν ότι έχουν υποστεί διαρροές δεδομένων έπειτα από τέτοιου είδους επιθέσεις. Τις περισσότερες φορές, αυτά τα περιστατικά σημειώνονται σε μικρού και μεσαίου μεγέθους επιχειρήσεις (23%), ενώ οι μεγάλες εταιρείες γίνονται στόχος των κακόβουλων επιθέσεων λιγότερο συχνά (17%). **[9]**

Οι διαρροές δεδομένων είναι αποτέλεσμα επιθέσεων phishing πιο περιστασιακά, με το 5% των επιχειρήσεων σε παγκόσμιο επίπεδο να αντιμετωπίζουν παρόμοια περιστατικά. Στην Ελλάδα, αυτό το ποσοστό είναι μόλις 3%. Ωστόσο, το ποσοστό των μεγάλων εταιρειών που έχασαν δεδομένα λόγω επιθέσεων phishing είναι λίγο υψηλότερο (6%) από το αντίστοιχο ποσοστό για τις μικρομεσαίες επιχειρήσεις (5%).

Ο αριθμός των ψηφιακών απειλών αυξάνεται συνεχώς. Για παράδειγμα, η Kaspersky Lab ανακαλύπτει 200.000 νέα δείγματα malware καθημερινά. Αυτό αναγκάζει τις εταιρίες να δώσουν μεγαλύτερη προσοχή στην ασφάλεια τους, ειδικά αφού αντιμετωπίσουν κάποιο περιστατικό παραβίασης της ψηφιακής προστασίας τους. Ωστόσο, σύμφωνα με την έρευνα, λίγες είναι εκείνες οι επιχειρήσεις που έχουν πλήρως εφαρμόσει anti-malware (anti-virus και anti-spyware) προστασία. Σε παγκόσμιο επίπεδο, το ποσοστό αυτό ανέρχεται στο 71%, σημειώνοντας μικρή βελτίωση σε σχέση με το προηγούμενα έτη (67%). Η κατάσταση στο χώρο της εταιρικής ασφάλειας αλλάζει καθώς ολοένα και περισσότερες εταιρείες στρέφονται σε πολύπλοκες λύσεις.

Το ευρύ φάσμα των επιθέσεων που δέχονται οι επιχειρήσεις σημαίνει ότι οι εταιρείες χρειάζονται μια επαγγελματική λύση ασφάλειας ικανή να αντιμετωπίσει αποτελεσματικά τις επικίνδυνες ψηφιακές απειλές.

Οπότε ένα από τα πιο σημαντικά ζητήματα και θέματα που πρέπει να αντιμετωπίσουν οι επιχειρήσεις και ο ιδιωτικός τομέας γενικότερα, όσον αφορά το spam και το phishing είναι η ανυπολόγιστη διαρροή δεδομένων του κάθε οργανισμού που μπορεί να υπάρξει.

Μία δεύτερη και επίσης σημαντική επίπτωση των ανεπιθύμητων μηνυμάτων είναι ότι τα μηνύματα αυτά στις επιχειρήσεις και στους οργανισμούς συνεπάγονται απώλεια παραγωγικότητας και κέρδους.

Μία εταιρία όταν πρόκειται να διαφημίσει ένα προϊόν, σύμφωνα με το κόστος του προϊόντος, υπολογίζει και την εκτύπωση των διαφημιστικών και την αποστολή αυτών. Οπότε το κόστος υπολογίζεται από τους αποστολείς και όχι από τους δέκτες. Η ιδέα της αλληλογραφίας αυτής λειτουργεί αντίστροφα όταν πρόκειται για ανεπιθύμητη αλληλογραφία. Δεν κοστίζει σχεδόν τίποτα για τους αποστολείς ανεπιθύμητης αλληλογραφίας να στέλνουν μεγάλες αλληλογραφίες μαζικής αποστολής σε δεκάδες χιλιάδες απρόθυμους παραλήπτες. Εντυπωσιακό είναι ότι έστω ο 1 στους 25000 παραλήπτες ανεπιθύμητων μηνυμάτων πρέπει να αγοράσει ένα προϊόν ή μία υπηρεσία μέσω αυτών των μηνυμάτων διαφήμισης ώστε να είναι κερδοφόρα η εταιρία ή ο ιδιώτης αποστολέας. Επιπλέον, οι λογαριασμοί ανεπιθύμητης αλληλογραφίας αντιπροσωπεύουν περίπου το 70% των παγκόσμιων μηνυμάτων, οι οποίοι προέρχονται από περίπου 14,5 δισεκατομμύρια ηλεκτρονικά μηνύματα την ημέρα. Σύμφωνα με την Microsoft και την Google, το spam κοστίζει στην παγκόσμια οικονομία σχεδόν 20 εκατομμύρια ετησίως σε χαμένη παραγωγικότητα, ενώ οι spammers κερδίζουν συνολικά 200 εκατομμύρια ετησίως.

Πώς όμως επηρεάζεται άμεσα η παραγωγικότητα μιας επιχείρησης από το spam;

Τα ανεπιθύμητα μηνύματα ισοδυναμούν με πραγματική απώλεια χρόνου των εργαζομένων. Κατά μέσο όρο, οι εργαζόμενοι χρειάζονται περίπου 16 δευτερόλεπτα για δουν, να καταλάβουν και να διαγράψουν ένα ανεπιθύμητο μήνυμα (Nucleus Research). Εάν η επιχείρηση δεν διαθέτει υπηρεσία φιλτραρίσματος ανεπιθύμητων μηνυμάτων, τότε το 70% των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου ενός υπαλλήλου ανά ημέρα μπορεί να είναι μηνύματα ανεπιθύμητης αλληλογραφίας. Οπότε αν υποθέσουμε ότι ένας εργαζόμενος λαμβάνει την ημέρα 10 ηλεκτρονικά μηνύματα, τα 7 εκ των οποίων είναι ανεπιθύμητα θα

σπαταλήσει περίπου στο 1,5 λεπτό μέχρι να επεξεργαστεί, να το καταλάβει και να το διαγράψει. Επομένως αν αναλογιστούμε ότι κάποιος λαμβάνει 100 ηλεκτρονικά μηνύματα ανά ημέρα, ο χρόνος που θα σπαταλήσει θα είναι πολύ μεγαλύτερος. Ακόμα αν σκεφτούμε ότι μία επιχείρηση ή ένας οργανισμός μπορεί να έχει 100, 200 ή 300 εργαζόμενους, και ο καθένας θα λάβει κάποια ανεπιθύμητα ηλεκτρονικά μηνύματα, ο χρόνος που θα καταβάλουν όλοι οι εργαζόμενοι θα είναι πολύ μεγαλύτερος. Λίγα δευτερόλεπτα εδώ μπορεί να μην φαίνονται πολλά, αλλά αυξάνεται σταδιακά σε ημέρες, εβδομάδες, μήνες και χρόνια. Μία επιχείρηση θα μπορούσε να χάσει απίστευτα πολλές δεκάδες χιλιάδες χρήματα κάθε χρόνο λόγω της ανεπάρκειας που προκαλείται από το spam.

Επίσης τα ανεπιθύμητα μηνύματα μπορεί να προκαλέσουν νομικούς κινδύνους. Στατιστικές δείχνουν ότι οι εικόνες και τα μηνύματα με σεξουαλικό και πορνογραφικό περιεχόμενο αυξάνονται με την δυνατότητα του spam. Στην πραγματικότητα, το πορνογραφικό spam έχει διπλασιαστεί τα τελευταία χρόνια και πλέον είναι η ταχύτερη αναπτυσσόμενη κατηγορία ανεπιθύμητων εμπορικών ηλεκτρονικών μηνυμάτων. Αν όμως οι υπάλληλοι μιας επιχείρησης λαμβάνουν πορνογραφικό spam στο χώρο εργασίας τους δύο πράγματα θα μπορούσαν να συμβούν: Παράξενα προσβεβλημένοι, οι εργαζόμενοι μπορούν να καταθέσουν καταγγελίες για σεξουαλική παρενόχληση και εχθρικό περιβάλλον εργασίας – ακόμα και αν η επιχείρηση αυτή δεν είναι η πηγή αυτών των ανεπιθύμητων μηνυμάτων. Αν η κάθε επιχείρηση ειδοποιεί για το πορνογραφικό spam και δεν προβεί σε ενέργειες για να τα εμποδίσει, οι εργαζόμενοι θα έχουν λόγους να προβούν σε νομικές ενέργειες κατά της επιχείρησης. Οι πονοκέφαλοι και το άγχος καθώς επίσης και τα πρόστιμα, οι αμοιβές και οι συμβιβασμοί που προκύπτουν από την απώλεια μιας αγωγής όπως αυτή, θα μπορούσαν να είναι μια σοβαρή επαγγελματική αποτυχία. Επίσης, το πορνογραφικό spam παρουσιάζει μια ευκαιρία για έναν υπάλληλο, να ανοίξει το μήνυμα ηλεκτρονικού ταχυδρομείου και να απορροφήσει τις εμφανείς εικόνες και το περιεχόμενό του μέσα σε πολύτιμες ώρες εργασίας. Εάν πληρώνει κάποιος τους υπαλλήλους του κατά μέσο όρο 25€-50€, δεν θα ήθελε να κοιτάζουν πορνογραφικό υλικό όταν πρέπει να συμβάλλουν στην συνολική παραγωγή και ευημερία της επιχείρησης ή του οργανισμού.

Ένα επίσης πολύ σημαντικό πρόβλημα που δημιουργείται με τα ανεπιθύμητα αυτά μηνύματα είναι ότι τέτοιου είδους μηνύματα μπορεί να περιέχουν διάφορες απειλές κακόβουλου λογισμικού. Στην τρέχουσα ψηφιακή εποχή, το spam δεν είναι πλέον απλώς ενοχλητικό αλλά και αβλαβές για τον κάθε υπολογιστή, το δίκτυο υπολογιστών ή τους διακομιστές. Ένας μεγάλος αριθμός μηνυμάτων ανεπιθύμητης αλληλογραφίας προέρχεται από νόμιμες επιχειρήσεις, χρηματοπιστωτικά ιδρύματα, νομικές αρχές ή προσωπικούς φίλους και οικογένειες. Συνήθως γραμμένο με κακή γραμματική ή κακή ορθογραφία, τα μηνύματα αυτά μας ενθαρρύνουν να “κάνουμε κλικ” σε ένα σύνδεσμο, να “ανοίξουμε” ή να “κατεβάσουμε” ένα αρχείο, μέσω του οποίου ένα κακόβουλο λογισμικό μπορεί να βρει τον τρόπο να διεισδύσει στον υπολογιστή. Το κακόβουλο spam χρησιμοποιεί επίσης απειλές για να μας κάνει να “κάνουμε κλικ” σε ένα σύνδεσμο ή ένα συνημμένο ηλεκτρονικού ταχυδρομείου, όπως το “θα κλείσουμε τον λογαριασμό σας αν δεν το κάνετε”. Έτσι, αν συναντήσει κάποιος ένα μήνυμα ηλεκτρονικού ταχυδρομείου που να έχει αυτά τα χαρακτηριστικά, θα πρέπει απλά να το διαγράψει. Πόσο μάλλον αν πρέπει να “ακολουθήσουμε” κάποιον σύνδεσμο. Γενικότερα, οι αποστολείς αυτών των μηνυμάτων χρησιμοποιούν κακόβουλο λογισμικό ικανό κυρίως για να

κλέψει ευαίσθητες πληροφορίες, όπως π.χ. αριθμούς κοινωνικής ασφάλισης, αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης και άλλα εμπιστευτικά δεδομένα που αφορούν τραπεζικούς λογαριασμούς. Ο λόγος είναι αρκετά απλός. Αυτοί οι spammers προσπαθούν να υποκλέψουν αυτές τις οικονομικές λεπτομέρειες ώστε να πάρουν χρήματα από τραπεζικούς λογαριασμούς ή να διαπράξουν απάτες με πιστωτικές κάρτες.

Γενικότερα όμως, το spam δημιουργεί την αναγκαιότητα για την αντιμετώπισή του, διότι το μεγαλύτερο πρόβλημα το αντιμετωπίζουν οι χρήστες που χρησιμοποιούν για μεγάλα διαστήματα της ημέρας το ηλεκτρονικό ταχυδρομείο και είναι αναγκασμένοι να σβήνουν όλη αυτή την ανεπιθύμητη αλληλογραφία. Επίσης τα μηνύματα αυτά για αρκετούς χρήστες φθάνουν να είναι πολλές φορές εκατοντάδες σε μία ημέρα. Οπότε η αναγκαιότητα αντιμετώπισής του εντοπίζεται στα ακόλουθα σημεία:

- **Είναι φαινόμενο δυσάρεστο, ενοχλητικό και απαράδεκτο από τους παραλήπτες**. Πολλές φορές προβάλει αμφίβολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων κλπ. Άλλα μηνύματα πιθανόν να περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.
- **Οδηγεί σε κατάχρηση πόρων του Διαδικτύου**. Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με κατανάλωση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στα κεντρικά συστήματα διανομής αλληλογραφίας (e-mail servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και στα συστήματα των χρηστών.
- **Θέτει σε κίνδυνο την ασφάλεια και την αξιοπιστία του διαδικτύου**: Οι spammers βρίσκονται σε συνεχή αναζήτηση συστημάτων, τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους. Πολλά μηνύματα αυτής της κατηγορίας μεταφέρουν επισυναπτόμενα αρχεία, τα οποία μπορεί να είναι ιοί ή δούρειοι ίπποι, όπου θέτουν σε κίνδυνο την ασφάλεια των συστημάτων. Το τελευταίο διάστημα, μεγάλο ποσοστό ανεπιθύμητης και επικίνδυνης αλληλογραφίας είναι αποτέλεσμα της δράσης ιών που έχουν προσβάλει διάφορα συστήματα που συνδέονται στο Διαδίκτυο.

3.2 Θεσμικό πλαίσιο για την ανεπιθύμητη αλληλογραφία στην Ελλάδα.

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

Σύμφωνα με τις παρ. 1 και 2 του αρ. 11 "Μη ζητηθείσα επικοινωνία": "1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής

προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου. "

Με άλλα λόγια, κάθε ηλεκτρονικό μήνυμα που σας αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση σας, δηλαδή κάθε μήνυμα spam, είναι παράνομο. Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα «opt-in».

Ειδικά για τα μηνύματα ηλεκτρονικού ταχυδρομείου, εξαίρεση αποτελεί, σύμφωνα με την παρ. 3 του αρ. 11, η περίπτωση στην οποία η ηλεκτρονική διεύθυνση του χρήστη αποκτήθηκε από τον αποστολέα νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής. Στην περίπτωση αυτή μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση (σύστημα "opt-out").

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

Ειδικότερα το θεσμικό πλαίσιο που ισχύει σήμερα στην Ελλάδα για την ανεπιθύμητη αλληλογραφία είναι το ακόλουθο:

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

2. "Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις."

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

4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, καθώς και κάθε είδους διαφημιστικούς σκοπούς, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και μια έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας, ή κατά παράβαση του άρθρου 5 ως ισχύει, ή όταν ενθαρρύνονται οι αποδέκτες να επισκεφθούν ιστοσελίδες που παραβιάζουν τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.»

«5. Οι φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν την υποχρέωση να λαμβάνουν τα κατάλληλα μέτρα, που καθορίζονται με κοινή πράξη της Α.Π.Δ.Π.Χ. και της Α.Δ.Α.Ε., για την αποτροπή της μη ζητηθείσας επικοινωνίας. Από τον φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που παραβίασε από αμέλεια την υποχρέωση αυτή καθώς και την υποχρέωση που προβλέπεται στο εδάφιο β` της παραγράφου 2, οι αποδέκτες μη ζητηθείσας επικοινωνίας, έχουν το δικαίωμα να αξιώσουν αποζημίωση για κάθε περιουσιακή ζημία ή χρηματική ικανοποίηση για ηθική βλάβη. Για τη χρηματική ικανοποίηση λόγω ηθικής βλάβης, εφαρμόζεται αναλογικώς η διάταξη της παραγράφου 2 του άρθρου 14 του παρόντος νόμου. Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών δεν υποχρεούται σε αποζημίωση και στη λήψη μέτρων ώστε να μην επαναληφθεί η παραβίαση στο μέλλον εφόσον αποδείξει ότι δεν τον βαρύνει αμέλεια.

6. Εκτός της αποζημίωσης σύμφωνα με το άρθρο 14 του παρόντος νόμου, οι αποδέκτες μη ζητηθείσας επικοινωνίας, καθώς και οι φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν δικαίωμα, σύμφωνα με τη διαδικασία του άρθρου 14 παρ. 3 του παρόντος νόμου, να απαιτήσουν από όποιον παραβιάζει τις υποχρεώσεις που προβλέπονται στις παραγράφους 1 έως 4 του παρόντος άρθρου, να μην επαναλάβει την παραβίαση στο μέλλον, με απειλή χρηματικής ποινής.»

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

«8. Η Α.Π.Δ.Π.Χ. ορίζεται ως αρμόδια αρχή για την εφαρμογή του Κανονισμού 2006/2004/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 364. 9.12.2004) στον τομέα της μη ζητηθείσας επικοινωνίας. Κατά τα λοιπά εφαρμόζεται η κ.υ.α. Ζ1-827/2006 (Β`1086, 9.8.2006), όπως ισχύει.» **[10]**

Απόφαση 59/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Κατόπιν αιτήσεων πέντε προσώπων, που κατήγγειλαν ότι η εταιρία εις βάρος της οποίας διενεργήθηκε ο έλεγχος της Αρχής αποστέλλει μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου στις ηλεκτρονικές τους διευθύνσεις και πιο συγκεκριμένα μηνύματα ηλεκτρονικού ταχυδρομείου (spam) για την προώθηση προϊόντων και υπηρεσιών που παρέχει, η ΑΠΔΠΧ προχώρησε στη διενέργεια ελέγχου της δραστηριότητάς της. Οι καταγγέλλοντες ανέφεραν ότι η εταιρεία δεν ικανοποίησε το αίτημά τους για διαγραφή των ηλεκτρονικών τους διευθύνσεων από τη λίστα παραληπτών της εταιρείας. Η Αρχή, κατά την εξέταση της πρώτης αίτησης, με έγγραφό της απηύθυνε σύσταση προς την εταιρεία, σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 19, καλώντας την να προσαρμόσει τις πρακτικές της, προκειμένου η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου να συνάδει με τις διατάξεις του άρθρου 11 του Ν. 3471/2006. Σε απάντηση του εγγράφου αυτού της Αρχής, η εταιρεία ενημέρωσε την Αρχή ότι συλλέγει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τους συμμετέχοντες στα σεμινάρια που η ίδια διοργανώνει, επισημαίνοντας ότι οι συμμετέχοντες στα σεμινάρια μπορούν να παρέχουν, εκτός από τα δικά τους στοιχεία επικοινωνίας, και διευθύνσεις ηλεκτρονικού ταχυδρομείου φίλων τους, ύστερα από προηγούμενη ενημέρωση και συγκατάθεση των τελευταίων. Τέλος, η εταιρία ανέφερε ότι παρέχει τη δυνατότητα διαγραφής των παραληπτών ηλεκτρονικού ταχυδρομείου από τη λίστα-κατάλογο που διατηρεί. Ακολούθως η Αρχή, κατά την εξέταση των αιτήσεων δυο άλλων αιτούντων, ζήτησε από την εταιρεία, να διευκρινίσει τον τρόπο λήψης συγκατάθεσης των ενδιαφερομένων για την αποστολή ηλεκτρονικής επικοινωνίας, καθώς και το είδος των προσωπικών τους δεδομένων που τηρεί στα αρχεία της, όπως και την προέλευση των δεδομένων αυτών. Επιπρόσθετα, η Αρχή ζήτησε διευκρινίσεις αναφορικά με τη διαδικασία εμπορικής προώθησης την οποία ακολουθεί, τον τρόπο εξασφάλισης της συγκατάθεσης των συνδρομητών των ηλεκτρονικών μέσων επικοινωνίας και τη διαδικασία άσκησης του δικαιώματος αντίρρησης των παραληπτών των διαφημιστικών της μηνυμάτων. Στην συγκεκριμένη περίπτωση η Αρχή εξέτασε τη νομιμότητα της συλλογής διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων προς τον σκοπό της αποστολής αζήτητης ηλεκτρονικής επικοινωνίας από διάφορες πηγές, την ικανοπόηση του δικαιώματος αντίρρησης των παραληπτών ενημερωτικού φυλλαδίου του υπεύθυνου επεξεργασίας και την ικανοποίηση των υποχρεώσεών του αναφορικά με συγκεκριμένες διατάξεις του νόμου 2472/1997 (άρθρα 6 και 10), την αποστολή των μηνυμάτων αζήτητης ηλεκτρονικής επικοινωνίας. Τα πορίσματα στα οποία κατέληξε ήταν ότι η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου τρίτων από τα συνέδρια, στα οποία μετέχει η εταιρεία δεν συνάδει με τη διάταξη του άρθρου 11 παρ. 1 του Ν. 3471/2006, καθόσον δεν εξασφαλίζεται η από τη διάταξη αυτή προβλεπόμενη ρητή συγκατάθεση των τρίτων - κατόχων των διευθύνσεων ηλεκτρονικού ταχυδρομείου. Αντίθετα, στην περίπτωση συλλογής διευθύνσεων από τους συμμετέχοντες στα συνέδρια-σεμινάρια-εκδηλώσεις, η προηγούμενη ρητή συγκατάθεση δίδεται από τους ίδιους τους ενδιαφερόμενους, και επομένως η πρακτική αυτή συνάδει με τη διάταξη του άρθρου 11 παρ. 1 του Ν. 3471/2006. Επίσης, κατά την κρίση της Αρχής η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου των εκθετών στις κλαδικές εκθέσεις δεν συνάδει με τις διατάξεις του άρθρου 11 του Ν.3471/2006, καθόσον σύμφωνα με την παράγραφο 5 του άρθρου αυτού η συγκατάθεση του εκάστοτε αποδέκτη μηνύματος ηλεκτρονικού ταχυδρομείου δεν εξαρτάται από το εάν ο αποδέκτης του μηνύματος ηλεκτρονικού ταχυδρομείου είναι νομικό ή φυσικό πρόσωπο. Η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου από αιτήσεις

που δέχεται η εταιρεία για να συμπεριλάβει μία ή περισσότερες ηλεκτρονικές διευθύνσεις στους αποδέκτες των εντύπων τους δεν συνάδει με τις διατάξεις του άρθρου 11 παρ. 1 του Ν. 3471/2006, σε περίπτωση που στις εν λόγω αιτήσεις περιλαμβάνονται διευθύνσεις ηλεκτρονικού ταχυδρομείου που ανήκουν σε τρίτους. Στην περίπτωση διευθύνσεων, οι οποίες χορηγούνται στην εταιρεία από τους ίδιους, δεν υφίσταται κάποια παράβαση, καθώς πληρούνται οι διατάξεις του άρθρου 11 παρ. 1 του Ν. 3741/2006. Για τους λόγους αυτούς, επεβλήθη στην εταιρία πρόστιμο ύψους 2.000 ευρώ στον υπεύθυνο επεξεργασίας για την παράνομη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου καθώς και πρόστιμο 2.000 ευρώ για αποστολή μη ζητηθείσας εμπορικής επικοινωνίας, χωρίς την προηγούμενη συγκατάθεση των συνδρομητών. **[11]**

Υπ΄αριθμ. 2110/2002 απόφαση του Μονομελούς Πρωτοδικείου Αθηνών.

Έτερο παράδειγμα που αφορά το νομικό πλαίσιο της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, αποτελεί η ως άνω απόφαση του Μονομελούς Πρωτοδικείου Αθηνών. Στην περίπτωση αυτή, ηλεκτρονική εφημερίδα πραγματοποιούσε αποστολή διαφημιστικών μηνυμάτων χωρίς την συγκατάθεση των αποδεκτών. Το Δικαστήριο έκρινε ότι η εφημερίδα έκανε κακή χρήση του Δικτύου της otenet καθώς επρόκειτο για πρόσκληση επίσκεψης της σελίδας της ηλεκτρονικής εφημερίδας και η διαβίβασή της ήταν παράνομη, μη προηγηθείσας της συγκατάθεσης του παραλήπτη και κατ΄ επέκταση η διακοπή από μέρους του παροχέα πρόσβασης της λήψης ηλεκτρονικών μηνυμάτων μπορεί να θεωρηθεί νόμιμη κατά το σκεπτικό της απόφασης, εφόσον παραμένει ελεύθερη η πρόσβαση στην ιστοσελίδα του εκδότη της ηλεκτρονικής εφημερίδας και έτσι δεν εμποδίζεται το δικαίωμα του τελευταίου να εκφράζει και να διαδίδει στοχασμούς του και συνεπώς δεν γεννάται κανένα θέμα περιορισμού της ελευθερίας του τύπου. **[11]**

3.3 Θεσμικό πλαίσιο για την ανεπιθύμητη αλληλογραφία σε άλλα κράτη.

Γενικότερα, σε διεθνή επίπεδο ο νόμος που αφορά τις εμπορικές επικοινωνίες αναφέρει ότι:

Τα κράτη μέλη εξασφαλίζουν ότι οι εμπορικές επικοινωνίες που συνιστούν υπηρεσία της κοινωνίας της πληροφορίας ή αποτελούν μέρος της πληρούν τουλάχιστον τους ακόλουθους όρους:

- η εμπορική επικοινωνία καθώς και το φυσικό ή νομικό πρόσωπο για λογαριασμό του οποίου αυτή γίνεται, πρέπει να είναι σαφώς αναγνωρίσιμα.
- οι διαφημιστικοί διαγωνισμοί ή παιχνίδια, οι προσφορές όπως είναι οι εκπτώσεις, τα πριμ και τα δώρα, εφόσον επιτρέπονται από το κράτος μέλος στο οποίο είναι εγκατεστημένος ο φορέας παροχής υπηρεσιών, πρέπει να είναι σαφώς αναγνωρίσιμοι-

α, η πρόσβαση στους όρους υπό τους οποίους μπορεί κανείς να επωφεληθεί από τις προσφορές πρέπει να είναι εύκολη, οι δε όροι να παρουσιάζονται σαφώς και επακριβώς. Όσο αφορά τη μη ζητηθείσα εμπορική επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου (spam) από φορέα παροχής υπηρεσιών εγκατεστημένο στο έδαφός τους, όσα κράτη-μέλη την επιτρέπουν πρέπει:

- να εξασφαλίζουν ότι είναι σαφώς αναγνωρίσιμη αμέσως μόλις περιέλθει στον παραλήπτη.
- να εξασφαλίζουν την τήρηση μητρώων "επιλογών" για τις μη ζητηθείσες εμπορικές επικοινωνίες, στα οποία μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες και τα οποία συμβουλεύονται τακτά οι φορείς που αναλαμβάνουν τέτοιου είδους επικοινωνίες.

Πιο συγκεκριμένα για το θεσμικό πλαίσιο σε διεθνή επίπεδο, θα αναφέρουμε δειγματικά τι ισχύει σε Μεγάλη Βρετανία, Γερμανία, Η.Π.Α και Κύπρο.

ΜΕΓΑΛΗ ΒΡΕΤΑΝΙΑ

Η ανεξάρτητη αρχή που ρυθμίζει τα σχετικά με την ιδιωτικότητα των πολιτών στην Μεγάλη Βρετανία είναι το Γραφείο Επιτρόπου Πληροφοριών. Όσον αφορά το spamming το Γραφείο Επιτρόπου Πληροφοριών κατέστησε σαφές ότι η ηλεκτρονική επικοινωνία για προώθηση πωλήσεων ή υπηρεσιών είναι επιτρεπτή μόνο εφόσον τα άτομα στα οποία απευθύνεται αυτή, ήτοι οι αποδέκτες έχουν δώσει τη συγκατάθεσή τους, εκτός εάν υπάρχει προηγούμενη συμβατική σχέση που να συνδέει τον αποστολέα με τον αποδέκτη. Η ανεξάρτητη αρχή στην επίσημη ιστοσελίδα της αναφέρει ότι ορισμένα μηνύματα ανεπιθύμητης ηλεκτρονικής αλληλογραφίας προέρχονται έξω από τα γεωγραφικά όρια της Μεγάλης Βρετανίας και καθιστά σαφές ότι η ίδια μπορεί να επιληφθεί αναφορών που αφορούν αποστολείς τέτοιου είδους μηνυμάτων οι οποίοι είναι δυνατόν να αναγνωριστούν εντός της χώρας.

ΓΕΡΜΑΝΙΑ

Το Γερμανικό Συνταγματικό Δικαστήριο ήδη από το 1983 είχε εύστοχα τονίσει το εξής: Είναι αδύνατο να υπάρξει δημοκρατική κοινωνία εάν ο πολίτης δεν γνωρίζει ποιος, πότε και για ποιο στόχο συλλέγει τα προσωπικά του δεδομένα. Η δημοκρατική κοινωνία προϋποθέτει την εμπιστοσύνη του πολίτη και τη διαβεβαίωση ότι δεν είναι «αντικείμενο» αλλά «υποκείμενο» και πως μπορεί ο ίδιος να καθορίζει τη διάθεση των προσωπικών του δεδομένων». Στη Γερμανία η μη αιτηθείσα εμπορική επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου είναι μη επιτρεπτή, εφόσον δεν υφίσταται ούτε εκπεφρασμένη ούτε εικαζόμενη συγκατάθεση του παραλήπτη. Μόνο εάν υπάρχει η προηγούμενη συγκατάθεση του παραλήπτη είναι επιτρεπτή η αποστολή διαφημιστικών e-mail. Συγκεκριμένα υπήρχε περίπτωση όπου στην οποία δεν υπάρχει συγκατάθεση, στον αποδέκτη της αλληλογραφίας προκαλείται ζημία και γεννάται υπέρ του παραλήπτη αξίωση παραλείψεως. Από τη γερμανική νομολογία, το LG Ellwagen δέχτηκε ότι

η μη αιτηθείσα διαφημιστική αλληλογραφία μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, που αποστέλλεται σε πελάτες ανταγωνιστικής επιχείρησης, είναι αθέμιτη ενόσω δεν έχει προηγηθεί συγκατάθεση του παραλήπτη. Άρα, πέρα από τον αποδέκτη της αλληλογραφίας δικαίωμα να ενάγει τον αποστολέα έχει και η θιγόμενη ανταγωνίστρια εταιρία προς παράλειψη και ανόρθωση της επελθούσας ζημίας.

Η.Π.Α.

Όσον αφορά στις ΗΠΑ, υπάρχουν ατελείς κανονιστικές διατάξεις, οι οποίες ως χαρακτηριστικό έχουν ότι επιβάλλουν στους αποστολείς της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας σημαντικά πρόστιμα. Το μέσο πρόστιμο είναι 10$ ανά μήνυμα με μέγιστο τα $25.000 ανά ημέρα. Για επιχειρηματίες μικρής κλίμακας, με περιορισμένους οικονομικούς πόρους, αυτό αποτελεί ένα σοβαρό ή και ριζικό αποτρεπτικό μέσο. Το spamming στις ΗΠΑ, σε αντίθεση με τα κράτη στην ΕΕ, δεν αντιμετωπίζεται μόνον ως παραβίαση ιδιωτικής σφαίρας. Τα αμερικανικά δικαστήρια θεωρούν το spamming παράνομη δραστηριότητα και έχουν κάνει δεκτές αιτήσεις δικαστικής προστασίας κατά των αποστολέων ανεπιθύμητης εμπορικής ηλεκτρονικής αλληλογραφίας. Σε ομοσπονδιακό επίπεδο στις ΗΠΑ δεν υπάρχει ρητή νομοθετική απαγόρευση, ενώ δεκαοκτώ πολιτείες έχουν εισαγάγει ρυθμίσεις για την ανεπιθύμητη ηλεκτρονική αλληλογραφία.

ΚΥΠΡΟΣ

Στην Κύπρο οι διατάξεις σχετικά με την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών μεταφέρθηκαν με τον υπ΄αριθμ. 112 (Ι)/2004) νόμο περί ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών. Το άρθρο 106 του ως άνω νόμου προβλέπει ότι για την αποστολή διαφημιστικών μηνυμάτων για απευθείας εμπορική προώθηση πρέπει να λαμβάνεται εκ των προτέρων η συγκατάθεση των παραληπτών των μηνυμάτων, ήτοι όπως και στην δική μας έννομη τάξη έτσι και στην Κύπρο έχουμε σε ισχύ την αρχή του opt-in. Η μοναδική εξαίρεση που προβλέπεται το σύστημα opt-out είναι η περίπτωση που ο αποστολέας λαμβάνει στοιχεία επαφής του ηλεκτρονικού ταχυδρομείου πελατών του στα πλαίσια πώλησης προϊόντος ή υπηρεσίας. Στην περίπτωση αυτή ο αποστολέας δύναται να χρησιμοποιήσει αυτά τα στοιχεία για απευθείας προώθηση παρόμοιων δικών του προϊόντων ή υπηρεσιών, υπό την προϋπόθεση όμως ότι δίνεται σαφώς και ευδιάκριτα στους πελάτες η δυνατότητα να αντιταχθούν ατελώς και με εύκολο για αυτούς τρόπο. Η αντίστοιχη Αρχή που είναι επιφορτισμένη με την προστασία όσων τα δικαιώματα ενδέχεται να θιγούν από την αποστολή μηνυμάτων spam, ονομάζεται Γραφείο Επιτρόπου Προστασίας Προσωπικών Δεδομένων. Ο Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι αρμόδιος να εξετάζει παράπονα για παράβαση του Νόμου και μπορεί να επιβάλει κυρώσεις σε όσους παρανομούν μεταξύ των οποίων και χρηματική ποινή μέχρι 30000 ευρώ.

4 *Τρόποι αποφυγής και μέτρα προστασίας.*

4.1 Τρόποι αποφυγής, χρήση υπαρχόντων τεχνικών μέτρων προστασίας.

Ενδεικτικά κάποιοι γενικοί τρόποι και τακτικές αποφυγής των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι:

1. Η δημιουργία μίας διεύθυνσης ηλεκτρονικού ταχυδρομείου αποκλειστικά για συναλλαγές στον Ιστό.

2. Η χρήση κάποιας δωρεάν διαδικτυακής υπηρεσίας ηλεκτρονικού ταχυδρομείου, για τη δημιουργία ενός λογαριασμού που μπορεί να χρησιμοποιηθεί στις ηλεκτρονικές συναλλαγές, θεωρείται σημαντική. Με αυτόν τον τρόπο, διασφαλίζεται η διατήρηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου που έχει εκχωρηθεί από τον εκάστοτε πάροχο υπηρεσιών Διαδικτύου (ISP) ή της απόρρητης διεύθυνσης, αν έχει παραχωρηθεί από το επαγγελματικό περιβάλλον.

3. Οι χρήστες οφείλουν να δίνουν την προσωπική τους διεύθυνση ηλεκτρονικού ταχυδρομείου μόνο σε άτομα που εμπιστεύονται.

4. Η καταχώρηση της διεύθυνση ηλεκτρονικού ταχυδρομείου σε μεγάλους καταλόγους του Διαδικτύου, ακόμα και σε προσωπική διαδικτυακή τοποθεσία, μπορεί να «διευκολύνει» τους spammers.

5. Προτείνεται η διεύθυνση ηλεκτρονικού ταχυδρομείου να παραμένει προσωπική.

6. Η χρήση μιας «καμουφλαρισμένης» διεύθυνσης συνιστάται, όταν δίνεται η διεύθυνση του χρήστη σε ομάδα συζήτησης, σε κανάλι συνομιλίας ή σε ηλεκτρονικό πίνακα ανακοινώσεων. Για παράδειγμα, θα μπορούσε να δοθεί μια ηλεκτρονική διεύθυνση ως "s0me0ne@example.c0m" χρησιμοποιώντας "0" (μηδέν) αντί για το "o." Κάποιο πρόσωπο μπορεί να καταλάβει τη διεύθυνση, αλλά τα αυτοματοποιημένα προγράμματα που χρησιμοποιούν οι αποστολείς μηνυμάτων spam, δεν μπορούν.

7. Επιβάλλεται, επίσης, προσοχή στα πλαίσια επιλογών σε διαδικτυακές συναλλαγές.

8. Κατά την αγορά αντικειμένων από το Διαδίκτυο, οι εταιρείες συνήθως προσθέτουν ένα πλαίσιο επιλογής (προεπιλεγμένο!), το οποίο υποδεικνύει ότι συμφωνεί ο πελάτης να πωληθεί ή να δοθεί η διεύθυνση του ηλεκτρονικού ταχυδρομείου του σε «υπεύθυνα πρόσωπα». Η αποεπιλογή της κρίνεται αναγκαία.

9. Έλεγχος στις πολιτικές απορρήτου των διαδικτυακών τοποθεσιών.

10. Σε περιπτώσεις εγγραφής σε υπηρεσίες που βασίζονται στον Ιστό, όπως ηλεκτρονικές τραπεζικές συναλλαγές, αγορές ή δελτία ενημέρωσης, πρέπει να εξετάζεται προσεκτικά η πολιτική απορρήτου, προτού αποκαλυφθεί η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη. Η πολιτική απορρήτου θα εξηγεί τους όρους και τις περιπτώσεις σχετικά με το εάν ή το πώς η τοποθεσία θα κοινοποιήσει τα δεδομένα του. Εάν δεν διαβάσει μάλιστα κάποια δήλωση, πιθανόν να "συμφωνήσει" στην κοινοποίηση των προσωπικών του δεδομένων, χωρίς να το γνωρίζει.

11. Εάν κάποια διαδικτυακή τοποθεσία δεν διαθέτει δήλωση απορρήτου, ο χρήστης οφείλει να επικοινωνήσει πρώτα με τους ιδιοκτήτες της τοποθεσίας, προτού κοινοποιήσει σημαντικές πληροφορίες.

12. Εάν η διαδικτυακή τοποθεσία δεν εξηγεί τον τρόπο με τον οποίο θα χρησιμοποιήσει τα προσωπικά δεδομένα, ο χρήστης δεν υποχρεούται να τα δώσει. Πρέπει να γνωστοποιηθεί πως πολλές εταιρείες - ακόμη και νόμιμες - ενδέχεται να κοινοποιήσουν τα προσωπικά δεδομένα με ανεπιθύμητους, πολλές φορές, τρόπους. **[12]**

Τρόποι προστασίας.

Γενικά μπορούμε να πούμε ότι υπάρχουν δύο τρόποι προστασίας από spam:

1. Μέσω εφαρμογών spam blockers και

2. Με τη χρήση spam φίλτρων.

Παρακάτω θα αναφερθούμε σε αυτούς τους δύο τρόπους και τη προστασία που παρέχουν στους χρήστες έναντι του spam.

Το spam blocker μπορεί να αποδειχθεί ένας αποτελεσματικός τρόπος για την καταπολέμηση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Αυτού του είδους το λογισμικό διαφέρει από τα προγράμματα spam filter, αφού μπλοκάρει όλα σχεδόν τα εισερχόμενα spam μηνύματα. Στην πραγματικότητα δηλαδή, πρόκειται για ένα σύστημα το οποίο αποτρέπει τη λήψη μηνυμάτων spam. Συνήθως, αποτρέπει ένα ποσοστό 90% ανεπιθύμητων μηνυμάτων να φθάσουν στο ηλεκτρονικό ταχυδρομείο ενός χρήστη, που μπορεί να περιέχουν ποικίλους ιούς ή άλλα κακόβουλα λογισμικά. Η απόδοση σε μερικά συστήματα μπορεί να φθάσει και το 99%. Πώς δουλεύει, όμως μία εφαρμογή spam blocker; Μία τέτοια εφαρμογή λειτουργεί μέσω του διακομιστή που είναι υπεύθυνος για το ηλεκτρονικό ταχυδρομείο, ελέγχοντας το λογαριασμό ενός χρήστη για ανεπιθύμητα μηνύματα και σβήνοντάς τα, ώστε αυτά να μην παραδοθούν. Όταν ψάχνουμε για ένα spam blocker, θα πρέπει να ελέγξουμε να είναι συμβατό με τη υπηρεσία ηλεκτρονικού ταχυδρομείου που διαθέτουμε, να

έχει μεγάλο ποσοστό αποτροπής ανεπιθύμητων μηνυμάτων, να είναι εύκολο στην εγκατάσταση, αλλά και το κόστος αγοράς του. Μερικά από τα πλεονεκτήματα εγκατάστασης και χρήσης μιας εφαρμογής spam blocking είναι ότι εγκαθίσταται σχετικά εύκολα και δε χρειάζεται περαιτέρω διαμόρφωση για να λειτουργήσει, επιτρέπει στο να διατηρήσει την διεύθυνση ηλεκτρονικού ταχυδρομείου που διαθέτει, ενώ επειδή σβήνει τα spam μηνύματα, ελαχιστοποιεί το χρόνο που ο χρήστης ασχολείται με αυτά καθώς και τη πιθανότητα να μολυνθεί ο υπολογιστής από κάποιο κακόβουλο λογισμικό.

Μία άλλη λύση για την αντιμετώπιση των ανεπιθύμητων μηνυμάτων, είναι η χρήση των λεγόμενων spam φίλτρων. Ένα τέτοιο φίλτρο είναι ένα λογισμικό το οποίο μπορεί και μπλοκάρει τα ανεπιθύμητα μηνύματα με τρεις βασικούς τρόπους:

1. Με την εγκαθίδρυση λευκών και μαύρων λιστών (white/black lists): οι οποίες μπορούν και δημιουργούν μία λίστα με αποδεκτές διευθύνσεις, όπου όλα τα μηνύματα από αυτές γίνονται δεκτά, και μία λίστα με ανεπιθύμητες διευθύνσεις, όπου τα μηνύματα που λαμβάνονται από αυτές αποθηκεύονται σε ένα ξεχωριστό κατάλογο.
2. Μπλοκάρισμα των λεγόμενων «sporm»: τα spam φίλτρα μπορούν και μπλοκάρουν ένα μεγάλο ποσοστό από spam που είναι σχετικά με πορνογραφία, καθώς επίσης και εισερχόμενα μηνύματα τα οποία έχουν περιεχόμενο σχετικό με ενηλίκους, όπως εικόνες ή κείμενα.
3. Οργάνωση των μηνυμάτων: αυτές οι εφαρμογές επιτρέπουν στους χρήστες να δημιουργήσουν φακέλους, ώστε να μπορούν να αποθηκεύονται μηνύματα ανάλογα με τη κατηγορία στην οποία ανήκουν (από φίλους, οικονομικά, προσωπικά, σχετικά με παιχνίδια). Τα εισερχόμενα μηνύματα αυτόματα κατηγοριοποιούνται στον κατάλληλο φάκελο, ώστε ο χρήστης να μπορέσει να διαλέξει ποια θα διαβάσει. Αυτό που θα πρέπει να τονιστεί είναι ότι ο χρήστης είναι αυτός που θέτει τα διάφορα φίλτρα, ανάλογα με τους κανόνες που επιλέγει, ώστε να γίνει η κατηγοριοποίηση των εισερχόμενων μηνυμάτων.

Μία σημαντική διαφορά του spam blocker από το spam filter είναι πως μέσω του spam filter έχουμε την οργάνωση των μηνυμάτων σε καταλόγους ανάλογα με το περιεχόμενο, ώστε ο χρήστης να δει μετά τι χρειάζεται και να απαντήσει ή να σβήσει όσα δε χρειάζεται. Παράλληλα, ένα πρόγραμμα spam blocker σβήνει όλα τα εισερχόμενα spam μηνύματα διευκολύνοντας τον χρήστη.

Η αντιμετώπιση, συνεπώς, ενός μεγάλου αριθμού ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου μπορεί να πραγματοποιηθεί μέσα από τη προσεκτική παρακολούθηση και ανακάλυψη κάποιων βασικών χαρακτηριστικών που έχουν τα spam μηνύματα, είτε στη διεύθυνση του αποστολέα, είτε μέσα στο κείμενο.

Γενικότερα το nextnet (ιστοσελίδα που παρέχει δωρεάν διαδικτυακές υπηρεσίες) αναφέρει ότι:

Επειδή στην εποχή μας το κυβερνοέγκλημα έχει πάρει σοβαρές διαστάσεις και οι κυβερνοεγκληματίες γίνονται ολοένα και πιο εφευρετικοί στις προσπάθειες τους να σου

αποσπάσουν ευαίσθητα δεδομένα ή να σε προκαλέσουν να κάνεις κλικ σε έναν fake σύνδεσμο που βρίσκεται μέσα σε κάποιο μήνυμα email πρέπει να είμαστε πολύ προσεκτικοί με την ηλεκτρονική αλληλογραφία.

Κακόβουλά μηνύματα email

Ένα κακόβουλο email που έρχεται στο γραμματοκιβώτιο σου μοιάζει σαν να προέρχεται από κάποιο πιστωτικό ίδρυμα, μια κρατική υπηρεσία ή ένα μεγάλο site ηλεκτρονικού εμπορίου αλλά και από οποιαδήποτε εταιρία ή οργανισμό. Συνήθως σε προτρέπει να ενεργήσεις γρήγορα π.χ. λέγοντας σου ότι ο λογαριασμός σου έχει μπλοκαριστεί και ότι πρέπει να κάνεις κλικ σε έναν σύνδεσμο για να τον ξεμπλοκάρεις.

Αν εντοπίσεις κάποιο τέτοιο μήνυμα email στα εισερχόμενά σου και δεν μπορείς να πεις με σιγουριά αν είναι κακόβουλο ή όχι τότε το καλύτερο που έχεις να κάνεις είναι να επικοινωνήσεις με την εταιρία από την οποία φαίνεται ότι προέρχεται το μήνυμα. Για την επικοινωνία αυτή χρησιμοποίησε στοιχεία που έχεις ήδη από πριν (όπως μια απόδειξη προηγούμενης αγοράς, ένα τηλέφωνο στο πίσω μέρος μιας πιστωτικής κάρτας κλπ.). Μην επικοινωνείς με την εταιρία με στοιχεία που υπάρχουν στο ύποπτο μήνυμα email. Αν δεν έχεις στοιχεία επικοινωνίας τότε ψάξε για την εταιρία στο διαδίκτυο αλλά επαναλαμβάνοντας χωρίς να χρησιμοποιήσεις στοιχεία που δίνονται στο ύποπτο μήνυμα.

Μηνύματα spam

Τα spam emails (ανεπιθύμητη αλληλογραφία) είναι πια τόσο διαδεδομένα που οι περισσότεροι χρήστες του διαδικτύου έχουν συμβιβαστεί με το γεγονός ότι υπάρχουν. Με τον όρο μήνυμα spam εννοούμε ένα μήνυμα email που έρχεται χωρίς να το περιμένεις, ένα μήνυμα που τις περισσότερες φορές είναι ανεπιθύμητο. Για την αποστολή του μηνύματος χρησιμοποιούνται ειδικά λογισμικά μαζικής αποστολής email (mass mailing software). Μερικοί τρόποι για να αντιμετωπίσεις το spam είναι:

- **Ενεργοποίησε φίλτρα spam στο λογαριασμό σου email**
  Οι περισσότεροι παροχείς δωρεάν email (όπως το Gmail, το Yahoo mail ή το Hotmail) έχουν ήδη ενσωματωμένα φίλτρα ανεπιθύμητης αλληλογραφίας (spam filters) για το περιορισμό των μηνυμάτων spam. Αν έχεις δικό σου διακομιστή και όνομα τομέα και έχεις αντίστοιχη διεύθυνση email τότε μέσα από το πρόγραμμα ανάγνωσης των emails σου θα μπορείς να ενεργοποιήσεις spam filters. Προσοχή όμως στις ρυθμίσεις που θα πραγματοποιήσεις έτσι ώστε να μπλοκάρεις μόνο τα μηνύματα spam και όχι κάποιο άλλο μήνυμα που θέλεις να λάβεις.
- **Ανέφερε τα μηνύματα spam**
  Οι παροχείς δωρεάν email αλλά και τα προγράμματα ανάγνωσης μηνυμάτων (email πελατών) σου δίνουν την ευκαιρία να "μαρκάρεις" ένα μήνυμα ως spam ή να κάνεις αναφορά spam. Μόλις εντοπίσεις κάποιο μήνυμα spam καλό είναι να το "μαρκάρεις" ή να το αναφέρεις έτσι ώστε να αποφύγεις να λαμβάνεις τέτοια μηνύματα κατευθείαν στο γραμματοκιβώτιο σου. Τα μηνύματα spam τότε θα καταλήγουν στο φάκελο ανεπιθύμητης αλληλογραφίας (spam folder ή junk folder).
- **Προστάτεψε την διεύθυνση email σου**
  Μη μοιράζεσαι την διεύθυνση email σου με τον οποιονδήποτε. Κρύψε την από τα

προφίλ σου στα κοινωνικά δίκτυα ή μοιράσου την με συγκεκριμένους. Αν έχεις ιστοσελίδα, ένα μέτρο πρόληψης είναι να μην κάνεις τη διεύθυνση email σου ορατή αλλά να έχεις μια φόρμα επικοινωνίας (contact form) για να επικοινωνούν οι επισκέπτες της ιστοσελίδας σου μαζί σου. **[13]**

4.2 Εφαρμογή μη τεχνικών μέτρων προστασίας.

Εκτός βέβαια από τα τεχνικά και οργανωτικά μέτρα προστασίας που πρέπει να περιλαμβάνουν οι επιχειρήσεις, οι οργανισμοί, τα κράτη και όλη γενικά η παγκόσμια κοινωνία, που είναι υπεύθυνη για την αντιμετώπιση αυτού του προβλήματος, είναι και τα μη τεχνικά μέτρα προστασίας. Το κυριότερο από αυτά μπορούμε να πούμε ότι είναι η επιβολή τέλους (πληρωμή) στις υπηρεσίες ηλεκτρονικών ταχυδρομείων. Μπορεί να αναρωτηθεί κάποιος, γιατί τα ανεπιθύμητα μηνύματα εδρεύουν κατά κύριο λόγο στις εφαρμογές ηλεκτρονικών ταχυδρομείων και όχι π.χ. στα μηνύματα κινητών, στις κλήσεις κινητών ή στα μηνύματα των "παραδοσιακών" ταχυδρομείων;

Η απάντηση είναι απλή. Διότι όλες οι υπόλοιπες υπηρεσίες, που αναφέραμε, κοστίζουν χρήματα σε κάποιους, οι οποίοι είναι κατά κύριο λόγο οι αποστολείς. Οπότε από το να στείλει κάποιος ένα ανεπιθύμητο μήνυμα μέσω κάποιας κινητής τηλεφωνίας, το οποίο θα του κοστίσει και πόσο μάλλον όταν πρόκεινται για ανεπιθύμητη αλληλογραφία όπου υπάρχει μαζική αποστολή και όχι μεμονωμένη, γιατί να μην το στείλει μέσω μιας δωρεάν υπηρεσίας που τυγχάνει να είναι και λιγότερο ανιχνεύσιμη; Έτσι λοιπόν αν κάποιος εκτιμούσε την αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου με ένα κόστος χ, όσο μικρό και αν ήταν αυτό, αμέσως θα ελαχιστοποιούταν η ανεπιθύμητη αλληλογραφία κατά πολύ. Αυτό θα συνέβαινε διότι, ενώ για κάποιον που θα ήθελε πραγματικά να επικοινωνήσει μέσω ηλεκτρονικού ταχυδρομείου δεν θα του κόστιζε πολύ, αντίθετα με εκείνον που θα ήθελε να αποστείλει μαζικά ανεπιθύμητα μηνύματα ηλεκτρονικής αλληλογραφίας. Μπορούμε να πούμε ότι είναι ένα μέτρο προστασίας που μπορεί να ελαττώσει την ανεπιθύμητη αλληλογραφία σε βαθμό τουλάχιστον 30%. Ένα απλό παράδειγμα μπορεί να υπάρξει σε μία ανεπιθύμητη αλληλογραφία για εμπορική χρήση. Για παράδειγμα, έστω ότι μια επιχείρηση θέλει να διαφημίσει τα προϊόντα της. Εφόσον δεν υπάρχει πληρωμή στις υπηρεσίες ηλεκτρονικού ταχυδρομείου, η συγκεκριμένη εταιρία στέλνει ανεπιθύμητα εμπορικά μηνύματα σε όλες τις επαφές της, ή ακόμα σε μία λίστα επαφών που έχει αγοράσει ή αποκτήσει μέσω μιας άλλης εταιρίας. Η συγκεκριμένη διαφήμιση της κοστίζει πολύ λιγότερο, από την δημιουργία διαφημιστικών φυλλαδίων, τηλεφωνικών κλήσεων ή μηνυμάτων ή προβολής των προϊόντων σε μέσα μαζικής ενημέρωσης. Αν όμως, έπρεπε να της κοστίσει αντίστοιχα το ηλεκτρονικό μήνυμα, πολλές θα ήταν αυτές που θα επέλεγαν τους άλλους τρόπους διαφήμισης. Ένα άλλο παράδειγμα είναι τα μαζικά ανεπιθύμητα μηνύματα που στέλνουν κάποιοι ώστε να μπορέσουν να πουλήσουν κάποια προϊόντα. Το θέμα στην συγκεκριμένοι περίπτωση

είναι ότι, αυτοί οι ανεπιθύμητοι αποστολείς στέλνουν μηνύματα μαζικής αλληλογραφίας, με την προϋπόθεση ότι έστω και ένας από όλους αυτούς τους παραλήπτες να αγοράσουν το προϊόν τους, αυτοί να είναι κερδισμένοι. Αν όμως αυτοί οι αποστολείς έπρεπε να πληρώσουν κάποια χρήματα για την αποστολή των μηνυμάτων αυτών, θα ήταν και πάλι κερδισμένοι με την ελάχιστη αγορά που θα γινόταν; Επίσης οι αποστολείς των ανεπιθύμητων μηνυμάτων, τύπου phishing, θα ήταν κερδισμένοι αν τους κόστιζαν οι αποστολές των μηνυμάτων αυτών; Φυσικά και όχι. Δηλαδή, αυτοί οι αποστολείς, στέλνουν τέτοιου είδους μηνύματα με την σκέψη ότι κάποιος χρήστης θα ξεγελαστεί, με το εκάστοτε σύνδεσμο ή διεύθυνση, και έτσι θα μπορέσουν να υποκλέψουν διάφορες ευαίσθητες πληροφορίες. Αν ο χρήστης αυτός δεν ξεγελαστεί τελικά; Αν ο χρήστης αυτός δεν διαθέτει ευαίσθητες ή προσωπικές πληροφορίες στο υπολογιστικό του σύστημα (υπολογιστή, τηλέφωνο κ.τ.λ.); Μπορεί να πάρει κάποιος τόσο μεγάλο ρίσκο, χωρίς να ξέρει αν θα πάρει απάντηση ή και να πάρει αν θα βρει κάτι; Έτσι λοιπόν, φαίνεται ότι το συγκεκριμένο μη τεχνικό μέτρο θα ήταν πολύ σημαντικό και δραστικό στην άμεση αντιμετώπιση των ανεπιθύμητων μηνυμάτων. Αλλά είναι γεγονός, ότι υπάρχουν ακόμα σοβαρότερα προβλήματα με την εφαρμογή του μέτρου αυτού σε άλλους τομείς σε σύγκριση με τα προβλήματα που λύνονται εφαρμόζοντάς το.

- Πώς μπορεί όμως να προστατευθεί γενικότερα ένας οργανισμός ή μια επιχείρηση;

Τα καλά νέα είναι ότι μπορεί να σταματήσει μία απάτη μέσω email πριν αυτή πετύχει. Η καλύτερη άμυνα συνδυάζει ανθρώπους, διαδικασίες και τεχνολογία – και χρειάζονται και τα τρία. Μπορούμε δηλαδή να αποφύγουμε την απάτη μέσω email με μία τρίπτυχη προσέγγιση:

- **Ενημέρωση και εκπαίδευση** του προσωπικού σχετικά με την απάτη μέσω email. Η εκπαίδευση μπορεί να βοηθήσει τους ανθρώπους να αναγνωρίζουν τα σημάδια ενός email-απάτη και να ακολουθούν τις βέλτιστες πρακτικές ώστε να μην πέφτουν στην παγίδα της απάτης μέσω email.
- **Διαδικασίες και πολιτικές** για τις εργασίες που γίνονται μέσω email. Χρησιμοποιώντας τις κατάλληλες διαδικασίες και πολιτικές, μπορούν να βοηθήσουν τους ανθρώπους να διαχειρίζονται με ασφάλεια τα αιτήματα μέσω email.
- **Εξελιγμένη προστασία** κατά απειλών που εμποδίζει τα email-απάτες πριν φτάσουν στα inbox των υπαλλήλων. Αυτή η προστασία θα πρέπει επίσης να εμποδίζει τους υπαλλήλους σας από το διαμοιρασμό ευαίσθητων πληροφοριών, σε περίπτωση που εξαπατηθούν για να επικοινωνήσουν με τους επιτιθέμενους. Μία αποτελεσματική λύση, πρέπει να περιλαμβάνει δύο ισχυρές δυνατότητες. Να ανιχνεύει και να εμποδίζει την απάτη μέσω email στο email gateway και επίσης να επαληθεύει την αυθεντικότητα των email της εταιρείας στα gateways των συνεργατών και στους λογαριασμούς email των πελατών. Η κατάλληλη τεχνολογία είναι απαραίτητη για την ανίχνευση και την εμπόδιση των επιθέσεων πριν αυτές φτάσουν στους ανθρώπους. (αναφέρεται σε τεχνικό μέτρο προστασίας)

Εκπαίδευση. Η εκπαίδευση ασφάλειας σχετικά με τις απάτες μέσω email, και την κυβερνοασφάλεια γενικά, μπορεί να βοηθήσει μια επιχείρηση να αποφύγει τις επιθέσεις και να ελαχιστοποιήσει τις επιδράσεις κάποιας επιτυχημένης επίθεσης. Όσα περισσότερα γνωρίζουν οι

άνθρωποι, τόσο καλύτερες θα είναι οι πιθανότητες για μία ισχυρή άμυνα. Η εκπαίδευση πρέπει να καλύπτει το χώρο των απειλών, τις νεότερες τεχνικές social engineering, και πως να εντοπίζουν τα emails-απάτες. Πρέπει να φροντιστεί ώστε οι άνθρωποι να γνωρίζουν τις συνήθεις λειτουργικές διαδικασίες και πολιτικές της εταιρείας, σχετικά με το πως τα στελέχη, οι συνεργάτες και οι πελάτες, αιτούνται χρήματα και ευαίσθητα δεδομένα. Όσο είναι δυνατό, πρέπει να συμπεριληφθούν στην εκπαίδευση, πραγματικές περιπτώσεις απάτης μέσω email ώστε να κατανοήσουν πως οι στρατηγικές επίθεσης υλοποιούνται σε πραγματικές συνθήκες.

Διαδικασίες. Τα emails- απάτες social engineering είναι σχεδιασμένα με αληθοφάνεια. Ακόμα και οι καλύτεροι υπάλληλοι μπορούν να ξεγελαστούν από μία καλοσχεδιασμένη και καλώς υλοποιημένη απάτη μέσω email. Γι’ αυτό και μία ξεκάθαρη, αυστηρή διαδικασία διαχείρισης και ελέγχου των αιτημάτων μέσω email μπορούν να παρέχουν καίριο προπύργιο εναντίον τους. Σκεφτείτε το ενδεχόμενο να εφαρμόσετε εσωτερικούς ελέγχους οικονομικών και αγορών, που θα βασίζονται σε διαδικασία επαλήθευσης με δύο ή περισσότερα βήματα.

5

Γενική αξιολόγηση-

Συμπεράσματα

Όπως φαίνεται επομένως, οι διάφοροι τρόποι αποστολής ανεπιθύμητης αλληλογραφίας με διαφημιστικό κυρίως περιεχόμενο, όπου δεν τυγχάνει ζήτησης από τον παραλήπτη και αποστέλλεται αυθαίρετα χωρίς κάποια συγκατάθεση μεγεθύνεται συνεχώς. Δεν πρέπει να φαντάζει περίεργο το γεγονός ότι τα περισσότερα μηνύματα τέτοιου τύπου, όλοι μας λίγο πολύ τα έχουμε λάβει. Η εξέλιξη αυτή ήταν δεδομένη, αν σκεφτεί κάποιος ότι πολύ απλά μπορούμε και δίνουμε σχεδόν παντού την ηλεκτρονική μας διεύθυνση, όπως π.χ. στην αγορά ενός προϊόντος μέσω διαδικτύου, στην ανάγκη να γίνουμε συνδρομητές σε κάποιες ιστοσελίδες, ακόμα και τα κοινοποιούμε στα μέσα κοινωνικής δικτύωσης χωρίς κάποιον ιδιαίτερο λόγο. Από την άλλη πλευρά, υπάρχει και η απαιτούμενη βοήθεια από τις διαφημιζόμενες επιχειρήσεις, οι οποίες μας βοηθούν με την υποστήριξή τους αφού μειώνουν το κόστος της προαγωγής του αντικειμένου της δραστηριότητά τους. Αντιθέτως, το κόστος είναι πολύ λιγότερο, με τον τρόπο της ανεπιθύμητης αλληλογραφίας από άλλους τρόπους διαφήμισης. Στο περισσότερο μέρος της εργασίας, έγινε λόγος για τις πολλαπλές απειλές που εμπεριέχονται στα μηνύματα αυτά αλλά και για τις επιπτώσεις που μπορεί να υπάρχουν από τα μηνύματα αυτά στους τελικούς χρήστες, στους οργανισμούς, στις επιχειρήσεις και γενικά στον ιδιωτικό τομέα. Έπειτα αναφερθήκαμε στο θεσμικό πλαίσιο που υπάρχει στην Ελλάδα σχετικά με το θέμα αυτό, καθώς επίσης έγινε και μία συνοπτική περιγραφή δύο σημαντικών παραδειγμάτων καταγγελιών ανεπιθύμητης αλληλογραφίας, όπου και πήραν σοβαρές διαστάσεις τα θέματα αυτά. Έτσι επομένως, φαίνεται ότι έχει γίνει μεγάλη προσπάθεια ώστε να αντιμετωπιστεί ικανοποιητικά το πρόβλημα αυτό. Βέβαια, παρά την μεγάλη προσπάθεια που έχει γίνει, δεν είναι σωστό να πούμε ότι το θέμα έχει λυθεί ή έχει μειωθεί δραστικά. Ακόμα παραμένει ένα μείζον πρόβλημα. Φαίνεται, δηλαδή ότι είναι ένα πρόβλημα σύγχρονης τεχνολογίας, αρκετά νέο, τόσο για το νομικό πλαίσιο, όσο και για το θεσμικό. Αλλά αυτό δεν παύει να σημαίνει ότι δεν μπορεί να καταπολεμηθεί. Πάντα υπάρχει τρόπος αντιμετώπισης προβλημάτων που αφορούν όλη την κοινωνία. Εκτός της χώρας μας βέβαια, υπάρχει ένα δυνατότερο θεσμικό πλαίσιο για το πρόβλημα της ανεπιθύμητης αλληλογραφίας, για το οποίο γίνεται σταδιακή εφαρμογή στην χώρα μας, όπως και σε άλλες χώρες. Επισημάναμε επίσης, γενικότερα και τον τρόπο αντιμετώπισης καθώς επίσης και το νομικό πλαίσιο τεσσάρων άλλων χωρών. Ακόμα αξίζει να σημειωθεί ότι, οι ραγδαίες τεχνολογικές εξελίξεις φαντάζουν αδύνατον στην γρήγορη αντιμετώπισή τους από θεσμικά και νομικά πλαίσια. Επιπλέον, αναφερθήκαμε στα διάφορα τεχνικά αλλά και μη τεχνικά μέτρα προστασίας που υπάρχουν ή θα μπορούσαν να υπάρξουν για την αντιμετώπιση αυτού του προβλήματος. Οπότε, μπορούμε να πούμε ότι παράλληλα με την προσπάθεια που κάνουν οι φορείς αυτών των υπηρεσιών που χρησιμοποιούνται μέσω διαδικτύου και ξεχωριστά από τα θεσμικά και

νομικά πλαίσια που υπάρχουν σε κάθε χώρα, είναι σημαντική η ανάγκη των μηχανισμών άμυνας και προστασίας, αλλά και ενημέρωσης των ίδιων των τελικών χρηστών στην πρόληψη αλλά κυρίως στην αντιμετώπιση του προβλήματος της ανεπιθύμητης αλληλογραφίας.

6 *Αναφορές*

1) 1992-2020 ESET, spol. S. r. o. Τι είναι spam, πως μπορούμε να το αναγνωρίζουμε και πως μπορούμε να προστατεύουμε από αυτό.

2) Valsa Raj Uchamballi, Sabyasachi Chakrabarty & Basudev Saha, (2005). Department of Information Technology, Ministry of Communications and Information Technology Govt. of India. In: An Overview of SPAM: Impact and Countermeasures, 16 March 2005.

3) Itsecuritypro (2018), Ασφάλεια Email.. οι απάτες, οι επιθέσεις & οι τρόποι προστασίας, 16 July 2018.

4) "Email harvesting is the process of obtaining lists of email addresses using various methods for use in bulk email or other purposes usually grouped as spam", http://en.wikipedia.org/wiki/E-mail_address_harvesting.

5) Η διαφημιστική εταιρία "Double Click" που δραστηριοποιείται στο Internet, αγόρασε τη βάση δεδομένων της εταιρίας "Abacus Direct", η οποία περιείχε εκατομμύρια προσωπικών δεδομένων αμερικανών καταναλωτών. Υπό την απειλή των καταναλωτών να προσφύγουν στην Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission, FTC), η "Double Click" δεσμεύτηκε ότι θα ενημερώνει τους αποδέκτες των διαφημιστικών της μηνυμάτων για τους σκοπούς του άμεσου marketing και θα τους παρέχει το δικαίωμα να δηλώνουν ότι δεν επιθυμούν να λαμβάνουν τέτοια ηλεκτρονικά μηνύματα.

   Η. Καστανάς, Ίντερνετ και προστασία των προσωπικών δεδομένων, ΔτΑ 11/2001, σελ. 717.

6) Data mining, a branch of computer science and artificial intelligence, is the process of extracting patterns from data. Data mining is an increasingly important tool by modern business to transform data into business intelligence giving an informational advantage. It is currently used in a wide range of profiling practices such as marketing (…)", http://en.wikipedia.org/wiki/Data_mining

7) https://freestuff.gr/forums/viewtopic.php?p=416440&416440

8) Λαλίνα Φαφούτη (2008), Εφημερίδα: Το Βήμα. Η απειλή των spam, November 2008

9) BIZtech.gr (2014), Malware, spam και phishing, οι απειλές που αντιμετωπίζουν συχνότερα οι εταιρίες.

10) Lawspot (2006). Νόμος 3471/2006. Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, Άρθρο 11, 28 Ιουνίου 2006.

11) Hellenic Data Protection Authority. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

12) Γιάννης Παλιούρης (2018).e-parenting. In: Spam και Scam emails. Πώς να προστατευτούμε;, 04 March 2018

13) Hellenic Data Protection Authority. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ανεπιθύμητες ηλεκτρονικές επικοινωνίες- SPAM.

14) Robert J. Hall (1999), AT&T Labs Technical Report 99.9.1 AT&T Proprietary AT&T Corp., 1999.In: A countermeasure to Duplicate-detecting Anti-spam techniques.

15) Christofer P. Lueg (2007), Webology, Volume 4. In: Mystery Meat revisited: Spam, AntiSpam Measures and Digital Redlining, March 2007.

16) Internet society (2015), The challenge of spam. In: An internet Society Public Policy Briefing, 30 October 2015.

17) Alena Kimakova & Reza Rajabiun (2008) MIT Spam Conference. In: The dangerous Economics of Spam Control, June 2008

18) Top Sec Cloud Solutions. Blended Threat Protection and Phishing Simulation Service.

19) Information Commissioner's Office (2018). Your data matters. What are spam email, what does the law say, and what can I do if l'm getting unwanted marketing emails.