

2022

7ο ΓΥΜΝΑΣΙΟ
ΛΑΡΙΣΑΣ

Τμήμα Α4

[ΘΕΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ]

Ομαδικές εργασίες των μαθητών του
τμήματος Α4α.

ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	3
Βασικοί κανόνες.....	3
Συμβολή στην τήρηση του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο	4
Πηγές	4
ΑΠΑΤΕΣ-SCAM	5
Οι απάτες	5
Απατηλά μηνύματα με email και SMS	5
Πώς να προστατευτείτε:	6
Πηγές	6
TROLLS	7
Τρολ και τρολάρισμα.....	7
Η ψυχολογία του Τρολ	8
Αντιμετώπιση του τρολ.....	9
Πηγές	9
ΤΙ ΕΙΝΑΙ ΤΟ SPAM;.....	10
Ορισμός.....	10
Ποιοι είναι οι τύποι του;.....	10
Ποια είναι η ιστορία του SPAM;.....	10
Πως να το εντοπίσετε το SPAM;	11
Αντιμετώπιση	11
Πηγές	13

ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΝΣΤΑΣΙΑ ΜΕΡΕΝΤΙΤΗ ΡΑΦΑΕΛΑ ΜΠΑΜΠΑΚΟΥ ΕΡΗ ΜΑΙΜΑΡΗ



Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο (στη διεθνή βιβλιογραφία: netiquette) ονομάζεται το σύνολο των κανόνων που ορίζουν την αποδεκτή συμπεριφορά μεταξύ δύο ή περισσότερων χρηστών του Διαδικτύου κατά την ηλεκτρονική τους επικοινωνία. Ο Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο στοχεύει στην καθιέρωση συμβάσεων ευγένειας και αλληλοσεβασμού, καθώς και στην πιο αποδοτική αλληλεπίδραση μεταξύ των χρηστών. Ο χαρακτήρας των κανόνων που τον απαρτίζουν είναι εθιμοτυπικός και κατά συνέπεια η μη υπακοή σε αυτούς δεν επιφέρει νομικές κυρώσεις.

Βασικοί κανόνες

Οι κανόνες του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο διαφέρουν από κοινότητα σε κοινότητα και τροποποιούνται ανάλογα με τη φύση του μέσου επικοινωνίας. Ωστόσο,

υπάρχουν ορισμένοι κοινοί κανόνες (γενικοί και ειδικοί) που αναφέρονται σε πρότυπα αποδεκτής συμπεριφοράς, σε θέματα ιδιωτικότητας και σε ζητήματα σωστής σύνταξης του ηλεκτρονικού γραπτού λόγου.

Ενδεικτικά, οι πιο γνωστοί γενικοί κανόνες αναφέρονται στην τήρηση μίας μετριοπαθούς στάσης κατά την ηλεκτρονική επικοινωνία, στο σεβασμό του ιδιωτικού χώρου και χρόνου του συνομιλητή μας, στη σωστή διαχείριση της ανωνυμίας μας, στην αποφυγή προσωπικών προστριβών και στη συγκαταβατικότητα προς άλλους χρήστες. Συγκεκριμένα για τον τελευταίο κανόνα, η Virginia Shea στο βιβλίο της «Netiquette» αναφέρει ότι πρέπει να είμαστε ευγενικοί όταν ο συνομιλητής μας κάνει λάθος και ιδιαίτερα προσεκτικοί όταν προβαίνουμε σε διορθώσεις σε σχόλια άλλων προσώπων.

Για την αποστολή ηλεκτρονικού ταχυδρομείου όμως και γενικότερα για τη σύνταξη του ηλεκτρονικού γραπτού λόγου, διαμορφώθηκαν ειδικοί κανόνες, από τους οποίους οι πιο γνωστοί είναι οι εξής:

- αποφυγή αποστολής ανεπιθύμητης αλληλογραφίας (spam ή junk mail)
- σεβασμός στα προσωπικά δεδομένα των παραληπτών
- όχι στη χρήση κεφαλαίων γραμμάτων, που ερμηνεύονται ως υψωμένος τόνος φωνής
- όχι στην προώθηση προσωπικού ηλεκτρονικού ταχυδρομείου σε λίστες συζητήσεων
- προσοχή στις κοινοποιήσεις (cc), στις κρυφές κοινοποιήσεις (bcc), στο χωρισμό των παραγράφων και στα ορθογραφικά – συντακτικά λάθη

Η συχνή παραβίαση των δύο πρώτων κανόνων συνιστά χαρακτηριστικό της εποχής μας, αφού η μαζική αποστολή ανεπιθύμητης αλληλογραφίας (Spamming) αποτελεί διαδεδομένη διαφημιστική πρακτική.

Συμβολή στην τήρηση του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο

Η τήρηση του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο εναπόκειται πρώτα και κύρια στη θέληση του χρήστη. Ωστόσο, σήμερα οι περισσότερες εταιρείες παροχής υπηρεσιών Διαδικτύου ενθαρρύνουν την εφαρμογή των κανόνων, υιοθετώντας πολιτικές αποδεκτής χρήσης που οριοθετούν τις επιτρεπόμενες και μη επιτρεπόμενες δραστηριότητες των

χρηστών, καθώς και τους κανόνες κατά την μεταξύ τους επικοινωνία.

Η παραβίαση των όρων χρήσης μπορεί να επιφέρει μη δημοσίευση ή και διαγραφή των προσβλητικών σχολίων, αποκλεισμό του χρήστη από μία ομάδα συζήτησης ή ακόμα και αναστολή των προνομίων χρήσης.

Πηγές

<https://el.wikipedia.org/wiki/Netiquette>

ΑΠΑΤΕΣ-SCAM

ΔΗΜΗΤΡΗΣ ΚΩΤΣΗΣ, ΝΙΚΟΣ ΜΑΤΟΣ, ΧΡΗΣΤΟΣ ΝΑΤΣΙΚΟΥ



Οι απάτες

Ένα τέχνασμα απάτης ή εμπιστοσύνης είναι μια προσπάθεια εξαπάτησης ενός ατόμου ή μιας ομάδας κερδίζοντας την εμπιστοσύνη τους.

Η απάτη μπορεί επίσης να αναφέρεται σε:

To Phishing είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί.

Αν ήταν εφικτό να αποδώσουμε τον όρο στα Ελληνικά, θα μπορούσαμε κάλλιστα να το αποκαλέσουμε 'Ηλεκτρονικό Ψάρεμα', κι αυτό γιατί αγγλικός όρος δεν απέχει πολύ από αυτό. Ο όρος Phishing, που πρωτοχρησιμοποιήθηκε από τον χάκερ Khan C Smith και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα των χάκερς, προέρχεται από το αγγλικό 'fishing' (ψάρεμα), καθώς η

διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες, θυμίζει την διαδικασία του δολώματος στο ψάρεμα. Μία άλλη εξήγηση σε αυτό είναι πως οι πρώτοι phishers, χρησιμοποιούσαν στα chat rooms τον html κωδικό `<><` που παραπέμπει σε ψάρι, διότι αυτός ο κωδικός δεν ήταν εύκολο να ανιχνευθεί ή να φιλτραριστεί αφού είναι ο πιο βασικός στην Html. Η αλλαγή του γράμματος f σε ph, πιθανότατα να είναι τυχαία ή να χρησιμοποιήθηκε από τους hackers για την απόκρυψη των ιχνών τους, αλλά σύμφωνα με κάποιους, έχει να κάνει με τον παλαιότερο όρο 'phreaking' ή 'phone freaking'. **To phreaking** είναι η ενέργεια μη εξουσιοδοτημένου χειρισμού τηλεφωνικών δικτύων.

Απατηλά μηνύματα με email και SMS

Οι απατεώνες στέλνουν απατηλά email ή SMS προσποιούμενοι ότι αποστολέας είναι η τράπεζα των παραληπτών. Σε αυτά τα μηνύματα συνήθως αναφέρουν ότι «έχει

παρατηρηθεί ύποπτη δραστηριότητα» στον λογαριασμό ή την κάρτα του αποδέκτη ή ότι «έχει κλειδωθεί ή απενεργοποιηθεί» ο λογαριασμός ή η κάρτα του.

Τα μηνύματα δίνουν κάποιον σύνδεσμο και προτρέπουν τους αποδέκτες να ακολουθήσουν αμέσως τις οδηγίες που υπάρχουν σε αυτόν για να λυθεί το πρόβλημά τους.

Ωστόσο, ο σύνδεσμος οδηγεί σε απατηλή ιστοσελίδα πανομοιότυπη με αυτήν της τράπεζας των παραληπτών. Οι παραλήπτες δεν αντιλαμβάνονται τη διαφορά κι έτσι συμπληρώνουν τους κωδικούς e-Banking τους, τα στοιχεία των πιστωτικών καρτών τους αλλά και τους Κωδικούς μιας Χρήσης (OTP) που λαμβάνουν εκείνη τη στιγμή και απαιτούνται για την έγκριση συναλλαγών.

Αυτή η πρακτική ονομάζεται phishing ή ηλεκτρονικό ψάρεμα.

Πώς να προστατευτείτε:

Πρέπει να είστε ιδιαίτερα επιφυλακτικοί με μηνύματα που σας ενημερώνουν για δήθεν προβλήματα με λογαριασμούς, κάρτες ή το e-Banking σας.

Εάν υποψιάζεστε ότι υπάρχει κάποιο ζήτημα με λογαριασμούς ή κάρτες σας, μεταβείτε απευθείας στο e-Banking ή το Eurobank Mobile App χωρίς να ακολουθήσετε κάποιον σύνδεσμο.

Παρατηρήστε εάν το μήνυμα είναι προσωποποιημένο ή εάν έχει λάθη και ανακρίβειες. Τα απατηλά μηνύματα αποστέλλονται μαζικά και δεν αναγράφουν το όνομα του πελάτη ούτε τον λογαριασμό που έχει το πρόβλημα. Επιπλέον, συνήθως υπάρχουν ορθογραφικά ή συντακτικά λάθη. Αυτά είναι ενδείξεις ότι πρόκειται για απάτη.

Να ελέγχετε προσεκτικά την περιγραφή των μηνυμάτων (SMS, Viber) που λαμβάνετε μαζί με τον Κωδικό μιας Χρήσης (OTP) για την έγκριση συναλλαγών.

Ενεργοποιήστε υπηρεσίες ειδοποιήσεων για να ενημερώνεστε για την κίνηση προϊόντων σας. Έτσι θα λαμβάνετε email ή SMS αμέσως μόλις πραγματοποιηθεί μια συναλλαγή σε λογαριασμό ή κάρτα σας.

Πηγές

<https://www.eurobank.gr/el/prostasia-apo-diadiktuakes-apates>

<https://help.steampowered.com/el/faqs/view/70E6-991B-233B-A37B>

TROLLS

Ντανταλής Γιώργος , Κωστής Θωμάς , Μακρής Θοδωρής



Στη γλώσσα του Διαδικτύου η λέξη **τρολ (troll)** περιγράφει κάποιον χρήστη του Ίντερνετ με πονηρά προκλητικές, σκόπιμα ανόητες ή επιτηδευμένα εκτός θέματος θέσεις και απόψεις σε μία online ανοιχτή κοινότητα, όπως ένα φόρουμ συζήτησης, mailing list, chat room ή [μπλογκ](#), με πρωταρχική πρόθεση να προκαλέσει και να ερεθίσει άλλους χρήστες ή με κάθε τρόπο να επιφέρει διαταραχή σε μια διαδικτυακή συζήτηση για οποιοδήποτε θέμα και να πετύχει μια αλυσίδα αντιδράσεων από άλλους χρήστες. Η συμπεριφορά αυτή που λέγεται **τρολάρισμα (trolling)** πολλές φορές συνοδεύεται από αμφιλεγόμενη διαμάχη των υπολοίπων περί του σκοπού του.

Η σύγχρονη χρήση του όρου φαίνεται ότι εμφανίστηκε για πρώτη φορά στο Διαδίκτυο στα τέλη της δεκαετίας του

1980, αλλά η πιο γνωστή καταγεγραμμένη αναφορά προέρχεται από συζήτηση του 1991.

Σύμφωνα με αυτή την έννοια, Troll είναι αυτός που κάνει *trolling*, αγγλική λέξη που αναφέρεται σε σύρσιμο του δολώματος μέσα στο νερό κατά την τεχνική της αλιείας θύννου (τόννου) και ξιφία, παρόμοια με την [συρτή](#).

Η λέξη παραπέμπει επίσης και στα [τρολλ](#) (trolls), δαιμόνια πλάσματα που παρουσιάζονται στη σκανδιναβική λαογραφία. Τα τρολλ είναι πλάσματα αντίστοιχα των [Καλικάντζαρων](#) της ελληνικής λαογραφίας που με την σειρά της πηγάζει από την αρχαιοελληνική δοξασία περί «δαιμονίων». Σύμφωνα με την σύγχρονη δοξασία οι Καλικάντζαροι εμφανίζονται κατά το Δωδεκάημερο 25 Δεκεμβρίου - 6 Ιανουαρίου.

Τρολ και τρολάρισμα

- Τρολ είναι αυτός που έχει σκοπό να κάνει κακό σε μια διαδικτυακή κοινότητα, προκαλώντας αναταραχή.
- Το **τρολάρισμα** είναι αποτέλεσμα συμπεριφοράς, όχι απαραίτητα με κακό σκοπό από τους φανερά εμπλεκόμενους, μια κατάσταση στην οποία μπορεί να έρθει η αλληλεπίδραση των χρηστών. Το τρολάρισμα κάνει την εμφάνισή του υπό διάφορες συνθήκες, όπως:

1. Λόγω ενός πονηρού τρολ, στα κατώματα του οποίου ανταποκρίνονται, ανυποψίαστα, αδαείς χρήστες.
2. Λόγω κάποιου αδαούς που παρασύρεται, ακούσια, σε συμπεριφορά αγανάκτησης.

Η ψυχολογία του Τρολ

Έρευνα των канаδών Erin Buckels, Paul Trapnell και Delroy Paulhus, οι οποίοι πήραν συνέντευξη από 1200 τρολ, βρήκε υψηλή συσχέτιση με τον σαδισμό, ψυχοπάθεια και μακιαβελλισμό. Ο σαδισμός σημαίνει πως αντλεί ευχαρίστηση με το να προκαλεί κακό στους άλλους, η ψυχοπάθεια είναι ψυχιατρική νόσος, αντικοινωνική διαταραχή προσωπικότητας και ο μακιαβελλισμός σημαίνει πως του αρέσει να εξαπατά και δεν έχει αισθήματα.

Ένα ιδιαίτερα επίμονο και ενοχλητικό τρολ μπορεί να αποτρέψει άλλους χρήστες από το να συμμετάσχουν σ' έναν κοινό διάλογο, ενώ μπορεί να προκαλέσει ακόμα και τη διάλυση

μιας διαδικτυακής κοινότητας. Αν ένα τρολ αγνοηθεί από την υπόλοιπη κοινότητα (πρόκειται συνήθως για το πιο αποτελεσματικό μέτρο), συνήθως αρχίζει να παράγει όλο και πιο ενοχλητικά και προσβλητικά μηνύματα με μόνο στόχο να προκαλέσει αντίδραση. Αν αυτή δεν έρθει, τότε το τρολ συνήθως εγκαταλείπει την κοινότητα.

Η συμμετοχή ή απάντηση σε συζήτηση που συμμετέχει το τρολ, σατιρικά περιγράφεται ως "τάισμα" του τρολ, γι' αυτό και υπάρχει η συνήθης παραίνεση «μην ταΐζετε τα τρολ» (Αγγλ. "Don't feed the trolls") ώστε να μην προκληθούν αντιδράσεις που θα ικανοποιήσουν το τρολ, ή περαιτέρω δυσάρεστες τροπές.

Εκτός από την αδιαφορία, σε πολλές περιπτώσεις υπάρχουν χρήσιμα τεχνικά μέσα για την καταπολέμηση ενός χρήστη - τρολ, όπως η άμεση αφαίρεση των μηνυμάτων του, η τεχνική με κατάλληλα φίλτρα προστασίας ώστε αυτά να καθίστανται αυτομάτως αόρατα, ή η [φραγή](#) του, αν υπάρχει αυτή η δυνατότητα ώστε να μην έχει τη δυνατότητα να γράψει απολύτως τίποτα. Σε chat rooms οι διαχειριστές ("operators" ή "moderators") έχουν τη δυνατότητα να απομακρύνουν το τρολ από ένα "δωμάτιο" συζήτησης (kick) ή και να του απαγορεύσουν την επανείσοδο (ban). Δραστικότερη είναι η μέθοδος κατά την οποία το τρολ τίθεται αμέσως εκτός chat room με την απλή είσοδό του σε αυτό με συγκεκριμένο ψευδώνυμο ή από συγκεκριμένη IP (akick). Τέλος, αν η περίπτωση του τρολ είναι πολύ «βαριά», δεν του επιτρέπεται καν η σύνδεση με το διακομιστή (K-lined)

Αντιμετώπιση του τρολ

Ένα ιδιαίτερα επίμονο και ενοχλητικό τρολ μπορεί να αποτρέψει άλλους χρήστες από το να συμμετάσχουν σ' έναν κοινό διάλογο, ενώ μπορεί να προκαλέσει ακόμα και τη διάλυση μιας διαδικτυακής κοινότητας. Αν ένα τρολ αγνοηθεί από την υπόλοιπη κοινότητα (πρόκειται συνήθως για το πιο αποτελεσματικό μέτρο), συνήθως αρχίζει να παράγει όλο και πιο ενοχλητικά και προσβλητικά μηνύματα με μόνο στόχο να προκαλέσει αντίδραση. Αν αυτή δεν έρθει, τότε το τρολ συνήθως εγκαταλείπει την κοινότητα.

Η συμμετοχή ή απάντηση σε συζήτηση που συμμετέχει το τρολ, σατιρικά περιγράφεται ως "τάισμα" του τρολ, γι' αυτό και υπάρχει η συνήθης παραίνεση «μην ταΐζετε τα τρολ» (Αγγλ. "Don't feed the trolls") ώστε να μην προκληθούν αντιδράσεις που θα ικανοποιήσουν το τρολ, ή περαιτέρω δυσάρεστες τροπές.

Εκτός από την αδιαφορία, σε πολλές περιπτώσεις υπάρχουν χρήσιμα τεχνικά μέσα για την καταπολέμηση ενός χρήστη - τρολ, όπως η άμεση αφαίρεση των μηνυμάτων του, η τεχνική με κατάλληλα φίλτρα προστασίας ώστε αυτά να καθίστανται αυτομάτως αόρατα, ή η φραγή του, αν υπάρχει αυτή η δυνατότητα ώστε να μην έχει τη δυνατότητα να γράψει απολύτως τίποτα. Σε chat rooms οι διαχειριστές ("operators" ή "moderators") έχουν τη δυνατότητα να απομακρύνουν το τρολ από ένα "δωμάτιο" συζήτησης (kick) ή και να του απαγορεύσουν την επανείσοδο (ban). Δραστικότερη είναι η μέθοδος κατά την οποία το τρολ

τίθεται αμέσως εκτός chat room με την απλή είσοδό του σε αυτό με συγκεκριμένο ψευδώνυμο ή από συγκεκριμένη IP (akick). Τέλος, αν η περίπτωση του τρολ είναι πολύ «βαριά», δεν του επιτρέπεται καν η σύνδεση με το διακομιστή (K-lined).

Πηγές

[https://el.wikipedia.org/wiki/%CE%A4%CF%81%CE%BF%CE%BB_\(%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF\)](https://el.wikipedia.org/wiki/%CE%A4%CF%81%CE%BF%CE%BB_(%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF))

ΤΙ ΕΙΝΑΙ ΤΟ SPAM;

Θάνος Μπαζαΐτης, Άγγελος Μπούζας, Κωνσταντίνος Νταΐτση



Ορισμός

SPAM ή αλλιώς Sending and Posting Advertisement in Mass σημαίνει η αποστολή ηλεκτρονικών μηνυμάτων σε έναν τεράστιο αριθμό ανθρώπων, δηλαδή η μαζική διαφήμιση. Όμως, γιατί είναι τόσο κακιά τεχνική και όλοι την αντιπαθούμε;

Η απάντηση είναι απλή. Το μεγαλύτερο πρόβλημα στο ανεπιθύμητα μηνύματα είναι πως είναι εντελώς απρόσωπα και δεν έχουν καμία επαφή με τον πελάτη.

Το SPAM δημιουργεί μεγάλο πρόβλημα σε έναν χρήστη, καθώς σε έναν άνθρωπο ο οποίος δεν ενδιαφέρεται για ένα συγκεκριμένο προϊόν, όταν του στέλνουν συνεχώς e-

mail για αυτό, το αποτέλεσμα είναι να τον εκνευρίζουν.

Ποιοι είναι οι τύποι του;

Το SPAM χωρίζεται σε δύο κατηγορίες:

– **Στο SPIM:** Το οποίο αναφέρεται στο Spam το οποίο αφορά τα μηνύματα μέσω πλατφόρμων Social Media.

– **Στο SPIT:** Το οποίο έχει να κάνει με τα μηνύματα μέσω τηλεφώνου.

Ποια είναι η ιστορία του SPAM;

Η ιστορία του SPAM, να λέμε την αλήθεια δεν είναι ακριβής, όμως υπάρχουν κάποιοι μύθοι που κυκλοφορούν.

Ο πιο γνωστός από όλους είναι αυτός με την ιστορία του Monty Python, ενός γκρουπ από κωμικούς στην Αγγλία, στο οποίο υπήρχε μία σκηνή κατά την οποία βρίσκονται σε ένα εστιατόριο και θέλουν να προωθήσουν ένα καπνιστό χοιρινό, οπότε σε κάθε πιάτο που έφερναν, έβαζαν δίπλα και ένα κομμάτι καπνιστό χοιρινό.

Πως να το εντοπίσετε το SPAM;

Κοιτάξτε, πολλές φορές μπορεί να είναι δύσκολο να διακρίνετε το SPAM εάν είναι σωστά στημένο, εκτός φυσικά αν έχετε κάποια λύση κυβερνοασφαλείας που έχει λειτουργία anti-spam.

Αλλά, εάν δεν έχετε κάποια αξιόπιστη λύση, μπορείτε να διακρίνετε το SPAM, από:

1. Μηνύματα από κάποιον που δεν γνωρίζετε.
2. E-mails με θέματα που δεν έχετε σχέση.
3. Προσφορές από εταιρείες που δεν ενδιαφέρεστε.
4. Διαφημίσεις με υπερβολικά πλεονεκτήματα.
5. Ψεύτικα νέα που σας ζητούν να τα κοινοποιήσετε.
6. Newsletter από ιστοσελίδες που δεν γνωρίζετε.
7. E-mails που ξεκινούν συζήτηση, π.χ. "Γεια, με θυμάσαι;".

8. Μηνύματα με συνδέσμους (link)
9. Emails που λένε ότι δεν είναι SPAM.

Αντιμετώπιση

Ακολουθεί μία σειρά από μέτρα για την αποφυγή της ανεπιθύμητης αλληλογραφίας:

- Μη δημοσιεύετε την e-mail διεύθυνσή σας. Βάζοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μια ιστοσελίδα είναι σχεδόν σίγουρο ότι σύντομα θα δείτε μηνύματα spam στο γραμματοκιβώτιό σας (βλ. «Προβλήματα από τη δημοσίευση e-mail διευθύνσεων στους δικτυακούς τόπους»).
- Μη δίνετε την e-mail διεύθυνσή σας σε οργανισμούς που δεν εμπιστεύεστε. Να είστε προσεκτικοί όταν επισκέπτεστε διάφορους δικτυακούς τόπους και ζητείται η συμπλήρωση προσωπικών στοιχείων επικοινωνίας, όπως το e-mail (π.χ. για να εγγραφείτε, ή για να προβείτε σε λήψη κάποιου αρχείου, κ.λπ.). Αν είστε αναγκασμένοι να κάνετε κάτι τέτοιο διαβάστε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας του συγκεκριμένου οργανισμού.
- Εναλλακτική e-mail διεύθυνση. Για τις περιπτώσεις που απαιτείται να δώσετε την e-mail διεύθυνσή σας και δεν είστε σίγουροι για το πώς αυτή

θα χρησιμοποιηθεί, μπορείτε να ανοίξετε έναν άλλο λογαριασμό e-mail σε κάποιον από τους φορείς που παρέχουν δωρεάν Web-mail λογαριασμούς (in.gr, yahoo, gmail, κ.ά.). Έτσι δε θα είστε αναγκασμένοι να δημοσιοποιείτε την κανονική διεύθυνσή σας.

- Μην απαντάτε στο spam. Μην απαντάτε σε spam μηνύματα όταν υπάρχει σχετική προτροπή σε αυτά, ούτε ακόμα και για τη διαγραφή σας από τις λίστες παραληπτών τους. Μία τέτοια απάντηση θα έχει ως αποτέλεσμα: α) να ελεγχθεί η εγκυρότητα της e-mail διεύθυνσής σας και να γίνει στόχος αποστολής επιπλέον spam μηνυμάτων, β) να χάνετε το χρόνο σας και να σπαταλάτε δικτυακούς πόρους χωρίς λόγο, αφού δεν αλλάζει κάτι.
- Αναφέρετε τα μηνύματα spam που λαμβάνετε. Υπάρχουν σχετικές υπηρεσίες του Διαδικτύου η οποίες συντηρούν λίστες από spammers. Τις λίστες αυτές αξιοποιούν πολλοί εξυπηρετητές ηλεκτρονικού ταχυδρομείου για τον περιορισμό του spam που φθάνει στους χρήστες.
- Διαδώστε τη γνώση σας και την εμπειρία σας σε σχέση με το spam. Μιλήστε στους χρήστες του δικτύου σας, μαθητές, εκπαιδευτικούς, διοικητικό προσωπικό, στην οικογένειά σας και τους φίλους σας για αυτό το θέμα και την αντιμετώπισή του. Είναι αρκετά συνηθισμένο οι

spammers να συγκεντρώνουν e-mail διευθύνσεις από τις απαντήσεις χρηστών του Διαδικτύου.

- Ελέγξτε τα συστήματά σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή. Μεταξύ των άλλων:
 1. Χρησιμοποιείτε λογισμικό προστασίας από τους ιούς (Antivirus) με δυνατότητα αυτόματης ανανέωσης για τους τελευταίους ιούς.
 2. Ενεργοποιείτε τις δυνατότητες προστασίας που διαθέτουν τα σύγχρονα συστήματα (π.χ. στα Windows XP ενεργοποιείτε από τις «Ιδιότητες» της σύνδεσής σας στο δίκτυο, στην καρτέλα «Για προχωρημένους», το «Τείχος προστασίας των Windows»).
 3. Τέλος μπορείτε να χρησιμοποιήσετε ειδικό λογισμικό τύπου firewall για την προστασία του δικτύου σας ή του μεμονωμένου υπολογιστή σας.
 4. **Χρήση προγραμμάτων αλληλογραφίας με δυνατότητα εντοπισμού της ανεπιθύμητης αλληλογραφίας.** Τα σύγχρονα προγράμματα αλληλογραφίας όπως το Microsoft Outlook 2003, Mozilla mail, κ.λπ. επιτρέπουν τον αυτόματο εντοπισμό και το φιλτράρισμα του spam. Χρησιμοποιούν διάφορες τεχνικές, η πιο γνωστή από

τις οποίες είναι η Bayesian filtering και διάφορες παραλλαγές. Τα προγράμματα αυτά επιτρέπουν το διαχωρισμό του spam σε ξεχωριστό φάκελο (π.χ. Junk Email στο Microsoft Outlook) ή επιτρέπουν στο χρήστη την οριστική διαγραφή των μηνυμάτων που χαρακτηρίζονται ως spam. Ο χαρακτηρισμός μπορεί να γίνει είτε μέσω black lists (οι οποίες δεν επιτρέπουν την παραλαβή μηνυμάτων από χρήστες που υπάρχουν σε αυτές) και white lists (οι οποίες επιτρέπουν την παραλαβή μηνυμάτων μόνο από χρήστες που υπάρχουν σε αυτές), είτε και με φιλτράρισμα βάσει του περιεχομένου των μηνυμάτων χρησιμοποιώντας

χαρακτηριστικές λέξεις-κλειδιά.

5. **Χρήση εξειδικευμένων προγραμμάτων φιλτραρίσματος.** Επιπλέον υπάρχει μια σειρά από εξειδικευμένα εμπορικά αλλά και ελεύθερα προγράμματα spam φίλτρων. Λίστα τέτοιων προγραμμάτων μπορείτε να βρείτε στο δικτυακό τόπο του SORBS

Πηγές

https://bitdefender.gr/blog/spam_ti_e_inai/

<https://el.wikipedia.org/wiki/%CE%A3%CF%80%CE%B1%CE%BC>

<http://dide.ilei.sch.gr/keplinet/tech/spam.php>