

7ο ΓΥΜΝΑΣΙΟ ΛΑΡΙΣΑΣ – Α ΤΑΞΗ

ΕΡΓΑΣΙΕΣ

ΠΛΗΡΟΦΟΡΙΚΗΣ

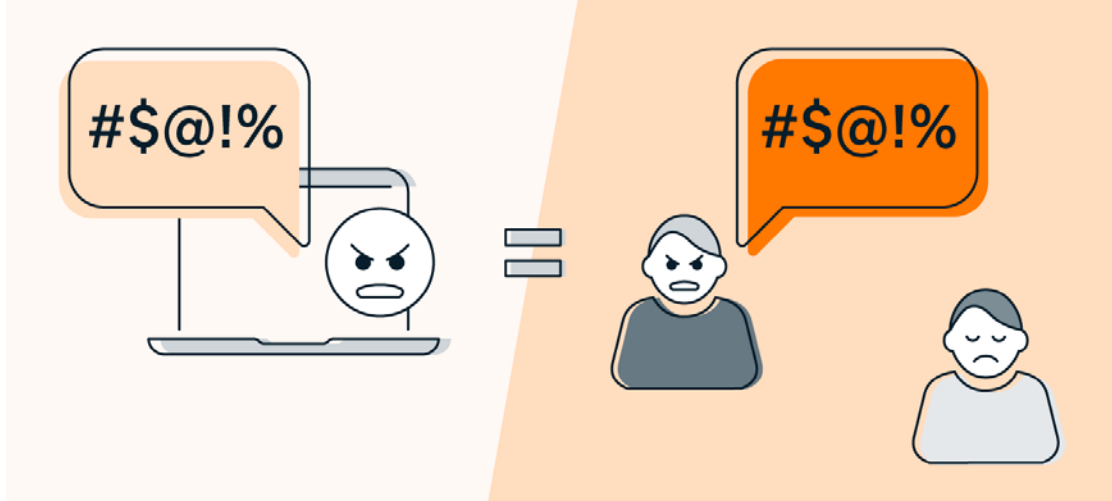
ΜΑΘΗΤΩΝ ΤΟΥ Α5α

2021-2022

NETIQUETTE και SPAM	3
Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο	3
Βασικοί κανόνες	3
Συμβολή στην τήρηση του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο (προσωπική ευθύνη των χρηστών)	4
Σπαμ (spam)	4
Αντιμετώπιση	5
Πηγές	7
Πως να αποφύγετε τα Scam Sites	8
Τι είναι η διαδικτυακή απάτη;	8
Τύποι του Scamming;	8
Πως να το αποφύγετε;	9
Συμπέρασμα	9
PHISHING	10
Πηγές	11
Τι είναι προσωπικά δεδομένα και τι ευαίσθητα προσωπικά δεδομένα;	12
Ορισμός	12
Νομοθεσία	13
Προστασία Δεδομένων	14
ΑΝΤΙΜΕΤΩΠΙΣΗ	14
Πηγές	14
Τι είναι το τρολ	16
Από που βγαίνει η λέξη τρολ	16
ΕΠΙΠΤΩΣΕΙΣ	17
ΑΝΤΙΜΕΤΩΠΙΣΗ	18

NETIQUETTE και SPAM

Μαρία Ρημαγμού / Αλέξια Νικούλη/Δήμητρα Νίκου /Κάτια Πίσσα



Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο

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.

Η ερμηνεία και οι εφαρμογές του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο ποικίλλουν από κοινότητα σε κοινότητα..

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.[6] «Netiquette» Επίσης ένα βιβλίο αναφέρει ότι πρέπει να είμαστε ευγενικοί όταν ο συνομιλητής

μας κάνει λάθος και ιδιαίτερα προσεκτικοί όταν προβαίνουμε σε διορθώσεις σε σχόλια άλλων προσώπων.[7]

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 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 (προσωπική ευθύνη των χρηστών)

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.[8]

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.

Σημαντική όμως είναι και η συμβολή των εταιρειών ή οργανισμών που ενσωματώνουν την τήρηση του Κώδικα δεοντολογικής συμπεριφοράς στο Διαδίκτυο στην πολιτική εταιρικής κοινωνικής ευθύνης που ακολουθούν.

Σπαμ (spam)

Σπαμ (spam) ονομάζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων, εξωτερικών συνδέσμων ή άλλων, σε μια προσπάθεια προώθησης προϊόντων ή ιδεών. Λόγω του χαμηλού κόστους αποστολής, η αποστολή γίνεται σε μεγάλο αριθμό αποδεκτών. Πρόκειται για παγκόσμιο φαινόμενο και υπάρχουν εκτιμήσεις για επτά τρισεκατομμύρια ανεπιθύμητα μηνύματα spam στο 2011. Σε αρκετές χώρες η αποστολή σπαμ διώκεται δικαστικά.

Ο όρος spam προέρχεται από το εμπορικό όνομα αμερικανικού προϊόντος κρέατος σε κονσέρβα στη δεκαετία του 1960 το οποίο εισαγόταν στη Μεγάλη Βρετανία σε μεγάλες

ποσότητες. Το 1970, οι Μόντυ Πάιθονς έγραψαν το σκετς Σπαμ ως μέρος της εκπομπής Το υπτάμενο τσίρκο των Μόντυ Πάιθονς όπου μια ομάδα Βίκινγκς επαναλάμβαναν δυνατά ένα τραγούδι με μόνα λόγια το «σπαμ σπαμ σπαμ...ωραίο σπαμ...εξαίρετο σπαμ». Στη συνέχεια, στη δεκαετία του 1980 οι εταιρείες αποστολής τέτοιων μηνυμάτων τα ονόμαζαν SPAM ως ακρωνύμιο του Sales Promotion and Marketing (Προώθηση Πωλήσεων και Μάρκετιν). Αργότερα η χρήση του επεκτάθηκε και το 1998 το New Oxford Dictionary of English [1]το περιέλαβε με την έννοια των «ασχέτων ή μη αποδεκτών μηνυμάτων που στέλνονται στο Ίντερνετ σε μεγάλο αριθμό ομάδων ειδήσεων ή χρηστών»

Αντιμετώπιση

Η αναγκαιότητα για την αντιμετώπιση του spam εντοπίζεται στα ακόλουθα σημεία:

Είναι φαινόμενο δυσάρεστο, ενοχλητικό και απαράδεκτο από τους παραλήπτες. Πολλές φορές προβάλλει αμφібολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων κ.λπ. Άλλα μηνύματα περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.

Οδηγεί σε κατάχρηση πόρων του Διαδικτύου. Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με δέσμευση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στους εξυπηρετητές ηλεκτρονικής 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 τα οποία μπορεί να είναι ιοί ή δούρειοι ίπποι, οι οποίοι 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 διασυνδεδεμένα στο Διαδίκτυο.

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:

Χρησιμοποιείτε λογισμικό προστασίας από τους ιούς (Antivirus) με δυνατότητα αυτόματης ανανέωσης για τους τελευταίους ιούς.

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»).

Τέλος μπορείτε να χρησιμοποιήσετε ειδικό λογισμικό τύπου firewall για την προστασία του δικτύου σας ή του μεμονωμένου υπολογιστή σας.

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.

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 Project (Spam and Open Relay Blocking System), στο σύνδεσμο: *Spam Fighting FAQ > Spam Prevention > (Ενότητα) Filtering*.

Η λειτουργία εξειδικευμένων προγραμμάτων για την αντιμετώπιση του spam απαιτεί τη λήψη όλου του όγκου των ενοχλητικών μηνυμάτων τοπικά στον υπολογιστή του χρήστη. Άρα, αν πρόκειται για τηλεφωνική σύνδεση, δε βελτιώνεται η επιβάρυνση της γραμμής σύνδεσης με το Διαδίκτυο και δε μειώνεται η καθυστέρηση και ο εκνευρισμός του χρήστη.

Βέβαια υπάρχουν φίλτρα τα οποία μπορούν να εφαρμοστούν στην

πλευρά του εξυπηρετητή ηλεκτρονικού ταχυδρομείου πριν την είσοδο των μηνυμάτων στο γραμματοκιβωτίου του χρήστη, αλλά για να εφαρμοστούν αυτά απαιτείται υποστήριξη του Παροχέα Υπηρεσιών Διαδικτύου (ISP), ο οποίος μπορεί να παρέχει τη συγκεκριμένη προστασία με όρους και προϋποθέσεις που αυτός επιλέγει.

Πηγές

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

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

<http://www.sch.gr/spam>

<http://www.de.sorbs.net>

<http://www2.e-yliko.gr/safety/smail3.htm>

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

Πως να αποφύγετε τα Scam Sites

Πλιάκας Κωνσταντίνος, Βασίλης Σπανός, Μάριος Πουλάνας



Τι είναι η διαδικτυακή απάτη;

Με απλά λόγια, η διαδικτυακή απάτη – επίσης γνωστή και ως απάτη στο ηλεκτρονικό εμπόριο – συμβαίνει όταν κάποιος χρησιμοποιεί κλεμμένες ή ψευδείς πληροφορίες για να πραγματοποιήσει μια ηλεκτρονική αγορά.

Τύποι του Scamming;

Το νούμερο 1 scam αυτήν την στιγμή είναι το phishing. Οι διαδικτυακοί κλέφτες ελπίζουν πως θα πετύχουν κάποιον αφελή χρήστη στέλνοντας του phishing emails. Μέσα σε αυτά τα e-mail θα υπάρχει κάποιος σύνδεσμος ο οποίος θα οδηγεί σε μία μολυσμένη ιστοσελίδα, κάποιο spyware ή θα έχει ένα rootkit έτοιμο να σας κάνει μεγάλη ζημιά. Μέσω το phishing, ο

χάκερ να κλειδώσει τον λογαριασμό σας, αλλά επίσης μπορεί να σας κλέψει:

- Τα προσωπικά σας δεδομένα
- Τα προσωπικά σας τραπεζικά στοιχεία
- Σημαντικά αρχεία του υπολογιστή σας
- Κωδικούς πρόσβασης στα Social Media, κ.α.
- Δείτε μερικά Tips Προστασίας από Phishing

Ψεύτικο Antivirus

Πάρα πολλοί scammers θα προσπαθήσουν να σας πουλήσουν ψεύτικα Antivirus, γνωστά και ως scareware. Αυτό θα γίνει με τον απλό τρόπο να εμφανιστεί ένα banner σε μία ιστοσελίδα που έχετε επισκεφθεί η οποία θα λέει πως έχετε κολλήσει κάποιον ιό στον υπολογιστή σας και πως πρέπει να κατεβάσετε κάποιο

antivirus για να το εξαφανίσετε. Να θυμάστε πάντα πως δεν μπορεί να σας πει οτιδήποτε άλλο εκτός του δικού σας antivirus αν έχετε ιό στην συσκευή σας.

Social Media Scam

Έχετε στο νου σας πως μερικές σελίδες των Social Media μπορεί σε κάποιο post τους να έχουν κάποιον σύνδεσμο, ο οποίος μπορεί να οδηγεί κάπου...επικίνδυνα!

Scam Κοινωνικής Μηχανικής

Κοινωνική Μηχανική είναι ο τρόπος κατά τον οποίο οι κυβερνοεγκληματίες έρχονται σε επαφή με τον άνθρωπο, με σκοπό να του εξαγάγουν πληροφορίες για να βρουν κάποιον κωδικό τους ή κάποια πληροφορία.

Πως να το αποφύγετε;

Στις μέρες μας, τα scam site έχουν δημιουργήσει αρκετή ένταση όχι μόνο στην Ελλάδα, αλλά και σε παγκόσμιο επίπεδο.

Σε γενικές γραμμές, οι ιστοσελίδες αυτές μοιάζουν αισθητικά με τα αληθινά, όμως έχουν κάποιες πολύ βασικές διαφορές, όπου αυτές είναι:

- **Προέλευση του συνδέσμου**

Από κάπου βρήκατε το ψεύτικο site, τώρα είτε είναι από ένα phishing email, είτε σε μήνυμα τηλεφώνου, να προσέξετε τι λέει καλά το μήνυμα αυτό και από που είναι. Αν λάβετε κάποιο e-mail το οποίο θα σας λέει να αλλάξετε τον κωδικό του **e-banking** σας, ή του λογαριασμού στο **PayPal** ή στο **Netflix**, να

θυμηθείτε αν το έχετε ζητήσει εσείς! Μην κλικάρετε στον σύνδεσμο.

- **URL**

Ελέγξτε το URL της ιστοσελίδας που πάτε να μπειτε, καθώς αν το παρατηρήσετε καλά, θα είναι λίγο διαφορετικό από το αληθινό. Μπορεί να έχει ένα γράμμα επιπλέον, ή να αλλάζει το **top-level domain** του.

- **SSL**

Δώστε βάση στην ιστοσελίδα να έχει το σύμβολο του ασφαλούς πιστοποιητικού που βρίσκεται αριστερά από το URL σας. Αυτό θα σας δείξει πως η συγκεκριμένη ιστοσελίδα είναι ασφαλής και πως δεν θα υποκλαπούν τα προσωπικά σας δεδομένα.

- **Παρουσιαστικό**

Η ψεύτικη ιστοσελίδα σε σχέση με την αληθινή μπορεί να μην έχει σχεδόν καμία διαφορά αισθητικά, γι' αυτό θα πρέπει να έχετε στο νου σας να προσέχετε καλά τις λεπτομέρειες και να μην τις προσπερνάτε γρήγορα. Οι διαφορές μπορεί να είναι μικρές, τύπου η γραμματοσειρά ή αν σας ζητάει έναν κωδικό σε μία άλλη σελίδα από αυτήν που θα έπρεπε να είναι το Sign-In.

Συμπέρασμα

Το scam είναι κάτι πολύ συχνό στις μέρες μας, αλλά επικίνδυνο για όλους. Μερικές φορές όμως, που γυρνάμε κουρασμένοι από την δουλειά ή την ασχολία μας μπορεί να μην προσέξουμε που θα πατήσουμε

και έτσι να χάσουμε τα αρχεία μας, ή να μας κλέψει ένας εγκληματίας τα τραπεζικά μας στοιχεία.

Ή και όχι.

PHISHING



Οι απάτες στον κόσμο του Internet είναι ένα σύνηθες φαινόμενο. Είναι πολλοί οι τρόποι που μπορεί να πέσει κανείς θύμα *"phishing"*, όμως η πιο κλασσική περίπτωση είναι η παραπλάνηση του χρήστη μέσω email.

Με τον καιρό οι πάροχοι των mail έχουν αυξήσει τα μέτρα ασφαλείας τους και τα ύποπτα email πάνε αυτόματα στα *«spam»*. Οι *"scammers"* όμως δεν το βάζουν ποτέ κάτω! Όσο αυξάνεται η ασφάλεια, τόσο αυξάνεται και η δυσκολία στο να αναγνωρίσει κανείς ένα *παραπλανητικό email*.

Σύμφωνα με το FBI το 2018 το συνολικό ποσό από **εταιρείες που εξαπατήθηκαν** φτάνει τα **12 δισεκατομμύρια δολάρια**. Για αυτό το λόγο πρέπει να μάθουμε να αναγνωρίζουμε αυτά τα email, από τις μικρές λεπτομέρειες που τα προδίδουν. Σας παρουσιάζουμε **10 tips** ή στοιχεία που αποδεικνύουν ένα mail-απάτη:

1. Μην εμπιστεύεστε το όνομα του αποστολέα

Μια γνωστή τακτική των *"scammers"* είναι βάζουν ως όνομα αποστολέα το όνομα κάποιας γνωστής εταιρείας. Όπως βλέπετε στο παρακάτω παράδειγμα, το mail στάλθηκε από το **My Bank** καθώς ο καθένας μπορεί να έχει όποιο όνομα επιθυμεί.

2. Παρατηρήστε με προσοχή το «Θέμα»

Τα περισσότερα από αυτά τα mail αποσκοπούν στο να δημιουργήσουν άγχος στο χρήστη, ώστε να τον εξαπατήσουν. Αυτό σημαίνει πως το θέμα του mail μπορεί να σας λέει για **πληρωμή που εκκρεμεί**, για κάποιο **πρόβλημα του υπολογιστή** σας ή έναν **ιό**.

3. Κοιτάξτε προσεκτικά το email, αλλά μην κάνετε κλικ!

Η πιο καλή πρακτική που σας προτείνουμε είναι να κοιτάξετε με προσοχή το mail, όμως προσέξτε μην πατήσετε κανέναν σύνδεσμο. Μπορεί να μεταβείτε σε σελίδες που περιέχουν ιούς.

4. Ελέγξτε την ορθογραφία του mail

Όπως διαβάζετε προσεκτικά το mail, πρέπει να έχετε στο νου σας την ορθογραφία και τα συντακτικά λάθη του κειμένου και των συνδέσμων που έχουν.

5. Αναλύστε τον χαιρετισμό

Στον χαιρετισμό του mail μπορεί να αναφέρεται το όνομα σας ή «Αγαπητέ πελάτη μας..».

6. Μην δίνεται τα προσωπικά σας στοιχεία

Να θυμάστε πως καμία τράπεζα δεν θα σας ζητήσει τα προσωπικά σας στοιχεία μέσω mail. Αντίστοιχα πρέπει να είστε 100% σίγουροι σε ποιον δίνετε τα προσωπικά σας στοιχεία στο διαδίκτυο.

7. Ελέγξτε την υπογραφή του αποστολέα

Ένα έγκυρο mail πρέπει να έχει και μια έγκυρη υπογραφή του αποστολέα. Διαβάστε προσεκτικά την υπογραφή του και εστιάστε στα στοιχεία επικοινωνίας. Μπορείτε να τα επαληθεύσετε με μια απλή αναζήτηση.

8. Μην κάνετε κλικ τα συνημμένα αρχεία

Ποτέ δεν πρέπει να ανοίξετε ή να κατεβάσετε τα επισυναπτόμενα αρχεία από ένα ύποπτο mail. Ωστόσο αν τα αρχεία αυτά έχουν περίεργα ονόματα, είναι άλλο ένα σημάδι *phishing*.

9. Να καθαρίζετε συχνά το mailbox σας

Μέσα στην μέρα δεχόμαστε πολλά email από *προσφορές* και *news letters*. Καλό είναι να

κάνουμε **απεγγραφή** από **όσα mail δεν μας ενδιαφέρουν πραγματικά**.

Όσο έχουμε τον έλεγχο του mailbox μας, μπορούμε να καταλάβουμε ότι ένα email μας στάλθηκε από έναν άγνωστο αποστολέα.

10. Μην πιστεύετε όλα όσα βλέπετε

Πολλές φορές το *θέμα* του mail μπορεί όντως να καταφέρει τον σκοπό του και να μας παραπλανήσει. Εφόσον γίνει αυτό θα πρέπει να γίνουμε πολύ καχύποπτοι και να ακολουθήσουμε τα παραπάνω tips, ώστε να μην κινδυνέψουμε ποτέ από *phishing*

Πηγές

<https://dynamics.microsoft.com/el-gr/ai/fraud-protection/online-ecommerce-fraud/>

<https://www.quantum.gr/qblog/10-tips-gia-na-apofygete-to-phishing/>

<https://bitdefender.gr/blog/scam-guide/>

Τι είναι προσωπικά δεδομένα και τι ευαίσθητα προσωπικά δεδομένα;

Κελλυ Σταματα Μαρια Μακροβασιλη



Ορισμός

"Δεδομένο προσωπικού χαρακτήρα" μπορεί να συνιστά κάθε πληροφορία που αναφέρεται σε ένα ορισμένο πρόσωπο (το υποκείμενο των δεδομένων). Τα προσωπικά δεδομένα διακρίνονται σε απλά και ειδικής κατηγορίας (ευαίσθητα). Ο νομοθέτης παρέχει στα ειδικής κατηγορίας προσωπικά δεδομένα διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και την τήρηση αρχείων που να τα εμπεριέχουν. Τα δεδομένα προσωπικού χαρακτήρα μπορούν, στο πλαίσιο διαμόρφωσης αποθετηρίων και τήρησης των σχετικών αρχείων, είτε να συνίστανται

σε στοιχεία αναγνώρισης είτε να αναφέρονται σε ενδιαφέροντα - συνήθειες/ δεδομένα ακαδημαϊκής δραστηριότητας/ δεδομένα θέσης κ.λπ., τα οποία να συνδέονται με συγκεκριμένο πρόσωπο. Ειδικής κατηγορίας προσωπικά δεδομένα είναι τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Παράδειγμα: Το ονοματεπώνυμο, η διεύθυνση ηλεκτρονικού

ταχυδρομείου (email), η διεύθυνση πρωτοκόλλου διαδικτύου (IP address), τα στοιχεία θέασης/ διαβάσματος αρχείων, τα στοιχεία που αφορούν λήψεις/ παραγγελίες αρχείων ενός ηλεκτρονικού αποθετηρίου αποτελούν προσωπικά δεδομένα. Η πληροφορία περί συμμετοχής ενός συγγραφέα σε συνδικαλιστική οργάνωση συνιστά ειδικής κατηγορίας προσωπικό του δεδομένο.

Προσωπικά δεδομένα στο διαδίκτυο

Οι υπηρεσίες κοινωνικής δικτύωσης που στοχεύουν στη δημιουργία on-line κοινοτήτων από ανθρώπους με κοινά ενδιαφέροντα και δραστηριότητες έχουν γίνει ιδιαίτερως δημοφιλείς στις μέρες μας. Οι υπηρεσίες αυτές προσφέρουν πολλαπλούς τρόπους επικοινωνίας και διάδρασης στους εγγεγραμμένους χρήστες τους που συνήθως προϋποθέτουν τη δημιουργία προσωπικών προφίλ των χρηστών. Οι χρήστες των υπηρεσιών αυτών μπορούν να δημοσιοποιούν και να μοιράζονται προσωπικές πληροφορίες με άλλες ομάδες χρηστών μέσα από το προσωπικό τους προφίλ . Αναμφίβολα οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν μία νέα μορφή εκκοινωνίωσης και επικοινωνίας, ιδιαίτερως ανάμεσα στους νέους αλλά όχι μόνο. Ταυτόχρονα όμως, οι υπηρεσίες αυτές προσδίδουν και μια καινούργια διάσταση στην έννοια του “προσωπικού χώρου”, δημιουργώντας

σοβαρές ανησυχίες για παραβίαση της ιδιωτικότητας των χρηστών τους, των οποίων τα προσωπικά δεδομένα δημοσιοποιούνται στο Διαδίκτυο με πρωτοφανή τρόπο και ποσότητα.

Νομοθεσία

Για την προστασία των προσωπικών δεδομένων στο διαδίκτυο έχει τοποθετηθεί επίσημα η Ευρωπαϊκή Ένωση με ειδική νομοθεσία που ορίζει ότι τα προσωπικά δεδομένα μπορούν να αποτελέσουν αντικείμενο επεξεργασίας μόνο σε ορισμένες περιπτώσεις και υπό ορισμένους όρους.

Οι όροι αυτοί είναι:

- Να έχει δώσει ο χρήστης τη συγκατάθεσή του (πρέπει να έχει ενημερωθεί για τη συλλογή των δεδομένων του)
- Να είναι αναγκαία η επεξεργασία τους για περιπτώσεις όπως αίτηση για θέση εργασίας ή αίτηση χορήγησης δανείου
- Να υπάρχει νομική υποχρέωση για την επεξεργασία τους
- Η επεξεργασία τους να αποτελεί «ζωτικό συμφέρον» για το άτομο, για παράδειγμα στην περίπτωση ατυχήματος ένας γιατρός να μπορεί να έχει πρόσβαση στον φάκελό σας
- Εάν η επεξεργασία είναι αναγκαία για την άσκηση καθηκόντων που εξυπηρετούν το δημόσιο συμφέρον ή για την άσκηση καθηκόντων από

την κυβέρνηση, τις
φορολογικές αρχές, την
αστυνομία ή άλλους
δημόσιους φορείς

Υπάρχουν ωστόσο και κάποια
προσωπικά δεδομένα τα οποία δεν
μπορούν να αποτελέσουν αντικείμενο
επεξεργασίας παρά μόνο σε ειδικές
περιπτώσεις και είναι εκείνα που
αφορούν: τη φυλετική ή την εθνική
καταγωγή, τον σεξουαλικό
προσανατολισμό, τα πολιτικά
φρονήματα, τις θρησκευτικές ή
φιλοσοφικές πεποιθήσεις, τη
συμμετοχή σε συνδικαλιστικές
οργανώσεις ή την υγεία. Οι κανόνες
αυτοί ισχύουν τόσο για τους
δημόσιους όσο και για τους ιδιωτικούς
φορείς.

Προστασία Δεδομένων

Τί γνωρίζουν οι χρήστες στην Ελλάδα
για την προστασία των δεδομένων
τους; Τα προσωπικά σου δεδομένα
είναι όλες οι πληροφορίες που
αναφέρονται σε σένα. Είναι το όνομά
σου, η διεύθυνσή σου, ο αριθμός του
κινητού σου, το σχολείο στο οποίο
πηγαίνεις, τα μέρη όπου συχνάζεις.
Μερικές φορές τα προσωπικά σου
δεδομένα αφορούν ιδιαίτερα
ευαίσθητα στοιχεία της ιδιωτικής σου
ζωής, όπως στο θρήσκευμά σου, στις
πολιτικές σου πεποιθήσεις ή στην
κατάσταση της υγείας σου και άλλα.
Πολλές φορές, ιδιαίτερα στα
κοινωνικά δίκτυα, δημοσιεύεις
δεδομένα σου που μπορούν να
χρησιμοποιηθούν από άτομα που δε
γνωρίζεις με κακόβουλο σκοπό.
Προσεκτικός πρέπει να είσαι όχι μόνο

όταν δημοσιεύεις πληροφορίες για
σένα τον ίδιο αλλά και πληροφορίες
που αφορούν άλλα άτομα. Για να το
κάνεις αυτό θα πρέπει να έχεις
ΠΑΝΤΑ τη συγκατάθεσή
τους. Διατηρώντας τον έλεγχο των
προσωπικών μας δεδομένων
ουσιαστικά διατηρούμε τον έλεγχο
της ιδιωτικής μας ζωής.

ΑΝΤΙΜΕΤΩΠΙΣΗ

Αν χρησιμοποιείτε υπηρεσίες
κοινωνικής δικτύωσης ενδεικτικά
σας προτείνουμε να:

- Είστε προσεκτικοί όταν
δημοσιεύετε προσωπικά
δεδομένα, καθώς όλα όσα
δημοσιεύονται γίνονται
αυτόματα διαθέσιμα στο
Διαδίκτυο.
- Σέβεστε την ιδιωτικότητα
των άλλων και να μην
δημοσιεύετε προσωπικά
δεδομένα τρίτων χωρίς την
συγκατάθεσή τους.
- Χρησιμοποιείτε ρυθμίσεις
φιλικές προς την
ιδιωτικότητα.
- Χρησιμοποιείτε διαφορετικά
αναγνωριστικά και κωδικούς
πρόσβασης από αυτά που
χρησιμοποιείτε σε άλλους
διαδικτυακούς τόπους που
επισκέπτεστε.
- Προσέχετε ώστε να μη δίνετε
κατά λάθος τη συγκατάθεση
σας για διάθεση των
προσωπικών σας δεδομένων
για διαφημιστικούς σκοπούς.

Πηγές

[ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ - ΤΟ ΔΙΑΔΙΚΤΥΟ
\(weebly.com\)](http://www.weebly.com)

Τι είναι προσωπικά δεδομένα και τι
ευαίσθητα προσωπικά δεδομένα;
(heal-link.gr)

[Προσωπικά δεδομένα στο διαδίκτυο](#)
(anavasis.gr)

Τι είναι το τρολ

ΚΩΝ/ΝΟΣ ΡΑΝΤΟΣ , ΝΙΚΟΣ ΣΟΥΛΕΝΗΣ



Στη γλώσσα του διαδικτύου η λέξη τρολ ή καλύτερα internet trol, χρησιμοποιείται για ένα πρόσωπο που έχει στόχο να σπείρει τη διχόνοια σε μια ομάδα ή κοινότητα (πχ σε ένα forum) δημοσιεύοντας καυστικά, εμπρηστικά ή εκτός θέματος σχόλια. Η πράξη αυτή γίνεται εσκεμμένα με πρόθεση να προκαλέσει έντονες συναισθηματικές αντιδράσεις στα μέλη μιας ομάδας εισχωρώντας στη κουβέντα τους. Με αυτόν τον τρόπο διαταράσσει την κανονική ροή της συζήτησης, χωρίς κάποιον ιδιαίτερο λόγο, απλά και μόνο για τη δική του διασκέδαση.

Από που βγαίνει η λέξη τρολ

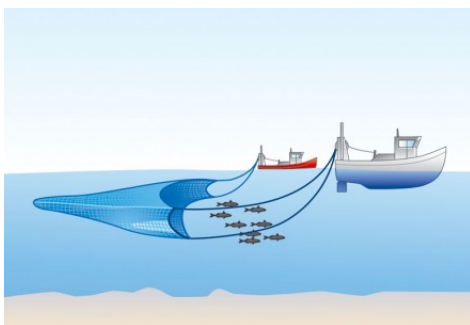
Η ετυμολογική προέλευση της λέξης δεν είναι ξεκάθαρη. Σύμφωνα με μια άποψη προέρχεται από την αρχαία σκανδιναβική λέξη troll που σημαίνει γίγαντας.



Μάλιστα, στην σκανδιναβική παράδοση, η λέξη χρησιμοποιούνταν για να περιγράψει κάποια μυθικά πλάσματα με τη μορφή γίγαντα ή νάνου.

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 τώρα με μία άλλη εκδοχή, η οποία είναι μάλλον και η επικρατέστερη, η λέξη troll προέκυψε από την ομόηχη αγγλική λέξη trawl που σημαίνει τράτα η οποία είναι ένα είδος αλιευτικού δικτύου.

Κι αυτό γιατί το τρολάρισμα βασίζεται εκεί ακριβώς. Το τρολ ρίχνει τα δίκτυα του και τα υποψήφια θύματα "τσιμπάνε" και αντιδρούν δίνοντας του συνεχώς "τροφή" για να συνεχίσει.



Από εκεί βγήκε και η έκφραση "μην δίνετε τροφή στα τρολ", δηλαδή μην ασχολείστε μαζί τους.

Μάλιστα υπάρχει και μια πολύ διάσημη εικόνα για τα τρολς που κυκλοφορεί ευρέως στο internet, το λεγόμενο trollface.



Η εικόνα αυτή που δημιουργήθηκε από τον Carlos Ramirez, στην ουσία είναι ένα παραμορφωμένο πρόσωπο που δείχνει την έκφραση που έχουν τα trolls όταν νευριάζουν τον κόσμο.

ΕΠΙΠΤΩΣΕΙΣ

Η έννοια της λέξης τρολ και των παραγώγων της, μπορεί να σχετίζεται κατά κύριο λόγο με το internet, ωστόσο όμως χρησιμοποιείται και αλλού.

Για παράδειγμα σε μια συζήτηση μεταξύ φίλων, όταν υπάρχει κάποιος που διαταράσσει την ροή της κουβέντας για να αποσπάσει την προσοχή των άλλων με σχόλια εκτός θέματος λέμε ότι αυτός τρολάρει.

Φυσικά το τρολάρισμα μπορεί να γίνει και για κάποιο συγκεκριμένο σκοπό, όπως για παράδειγμα για να αποτραπεί μια συζήτηση που το τρολ για δικούς του λόγους δεν επιθυμεί να γίνει.

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

ΑΝΤΙΜΕΤΩΠΙΣΗ

Σε γενικές γραμμές τα άτομα αυτά δεν είναι ιδιαίτερα επικίνδυνα, αν και κάποιες φορές απειλούν άλλους χρήστες, είναι ωστόσο πολύ ενοχλητικά. Μάλιστα σε ορισμένες περιπτώσεις μπορεί να οδηγήσουν μια κοινότητα ακόμη και σε διάλυση. Πάντως, στις online κοινότητες τα τρολς εντοπίζονται σχετικά γρήγορα και περιθωριοποιούνται από τα μέλη της. Κάπως έτσι σταματάει και η δράση τους. 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 “ταΐσμα” 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.

Επομένως, τώρα που ξέρετε τι είναι τα τρολς μην τα ταΐζετε και να είστε σίγουροι ότι κάποια στιγμή θα σταματήσουν μόνα τους!

<https://www.ipaidia.gr/endiaferouses-eidiseis/ti-simainei-trol-trolaro-kai-trolarisma/>

<https://coolweb.gr/trol-ti-einai/>