Ασφαλής Χρήση των Επιγραμμικών Τεχνολογιών

Δοξαριώτης Γιώργος

Πληροφορία στο Διαδίκτυο

- Παγκόσμιος Ιστός: γρήγορη, εύκολη και ανέξοδη πρόσβαση πληροφοριών.
- Μετάβαση από το παθητικό Διαδίκτυο (ο χρήστης ήταν απλός αναγνώστης), στο **«συμμετοχικό» Διαδίκτυο**, ο χρήστης έχει ενεργό ρόλο στην παραγωγή και διακίνηση της διαδικτυακής πληροφορίας.
- Αναπτύχθηκαν εργαλεία, όπως τα blogs, και τα wikis (π.χ. τα άρθρα της Wikipedia).
- Ο νέος τρόπος παραγωγής και πρόσβασης στην πληροφορία προϋποθέτει και αλλαγή στον κριτικό τρόπο που την αξιολογούμε και φιλτράρουμε.

Αξιοπιστία Πληροφορίας στο Διαδίκτυο

- Συνδιαμόρφωση του περιεχομένου του διαδικτύου από τους χρήστες του.
- Παραγωγός της διαδικτυακής πληροφορίας μπορεί να είναι ο οποιοσδήποτε.
- Οι πληροφορίες στο διαδίκτυο μπορεί να είναι ανακριβείς
  - είτε από λάθος
  - είτε σκόπιμα
- Όλο και περισσότεροι ανατρέχουν στο διαδίκτυο για πληροφορίες χρησιμοποιώντας τις μηχανές αναζήτησης.
- Απαιτούνται δεξιότητες ώστε η αναζήτηση να είναι εστιασμένη και να μας οδηγεί σε σωστά αποτελέσματα.

Αξιοπιστία Πληροφορίας στο Διαδίκτυο ΙΙ

- Διαφορά μεταξύ βιβλίου και διαδικτύου (σε αυτό όλοι μπορούν να γίνουν συγγραφείς)
- Αναζητείστε πληροφορίες από περισσότερες από μία πηγές

Blogs (Ιστολόγια)

- Blog: συνδυασμός των λέξεων «web» (ιστός) και «log» που σημαίνει καταχώριση. Εικονικό ημερολόγιο που μπορεί να δημιουργηθεί και να δημοσιευθεί στο Διαδίκτυο πολύ εύκολα από οποιονδήποτε,
- Blogging: η διαδικασία δημιουργίας και φόρτωσης πληροφοριών σε ένα blog,
- Blogger: ο δημιουργός και αρθρογράφος σε ένα blog
- Δωρεάν εγγραφή σε κάποια υπηρεσία που προσφέρει τα απαραίτητα εργαλεία δημιουργία blog, π.χ.
  - Blogger.com
  - Wordpress.com
- Ο δημιουργός ενός blog
  - επιλέγει τη μορφή και το είδος του περιεχομένου που επιθυμεί να αναρτά στο προσωπικό του ιστολόγιο.
  - επιτρέπει ή απαγορεύει την ανάρτηση σχολίων από τρίτους επί των αναρτήσεών του.

Blogs - Προβληματισμοί

- Κίνδυνοι από δημοσιοποίηση προσωπικών δεδομένων
- Αξιοπιστία παρουσιαζόμενων πληροφοριών
- Πνευματικά δικαιώματα περιεχομένου

Blogs - Συμβουλές

- Προσωπικές μας πληροφορίες δεν πρέπει ποτέ να δημοσιεύονται στο Διαδίκτυο.
- Φωτογραφίες μας μπορούν να χρησιμοποιηθούν κακόβουλα.
- Μπορείτε να χρησιμοποιήσετε κάποιο ψευδώνυμο για να προστατεύσετε την ταυτότητά σας.
- Αν σκοπεύετε να δημοσιεύσετε πληροφορίες και εικόνες για τρίτους, πρέπει πρώτα να πάρετε την άδειά τους.
- Ποτέ μη δημοσιεύετε προσβλητικό ή παράνομο υλικό.
- Τα άρθρα στα ιστολόγια συνήθως είναι ανυπόγραφα και υποκειμενικά. Διασταυρώστε τις πληροφορίες τους.
- Περιορίστε την πρόσβαση στο blog σας σε άτομα που έχουν κωδικό πρόσβασης.
- Μπορείτε να αποφύγετε την εμφάνιση του blog σας στα αποτελέσματα μεγάλων μηχανών αναζήτησης.

Πνευματική Ιδιοκτησία

- Ο νόμος προστατεύει τους συντάκτες και τους δημιουργούς αυθεντικής εργασίας.
- Ο δημιουργός έχει αποκλειστικά δικαιώματα στο έργο του σχετικά με την
  - χρήση
  - αντιγραφή
  - και αναπαραγωγή του
- Χρήση έργου προστατευμένου με πνευματικά δικαιώματα μόνο με γραπτή άδεια από τον δημιουργό.
- Οι περισσότεροι ιστοχώροι αναφέρονται ευκρινώς στην πνευματική τους ιδιοκτησία («copyright» ή ©).
- Στο 4ο κεφάλαιο του Ν. 2121/1993 υπάρχουν εξαιρέσεις (περιορισμένα αντίγραφα – συγκεκριμένες χρήσεις) στο αποκλειστικό δικαίωμα του δημιουργού

Ηλεκτρονικά παιχνίδια

- Μέσω ηλεκτρονικού υπολογιστή ή ειδικών παιχνιδομηχανών (κονσόλες) ή φορητών συσκευών ή online μέσω Διαδικτύου
- Ενδεχομένως ακατάλληλο περιεχόμενο
- Υπερβολική ενασχόληση
- Προσβλητική/παράνομη συμπεριφορά ορισμένων παιχτών απέναντι σε άλλους παίχτες
- Παραβίαση της ιδιωτικής ζωής μέσα από την επικοινωνία των χρηστών στο πλαίσιο του παιχνιδιού
- Ενδεχόμενο διασύνδεσης σε ιστοσελίδες ακατάλληλες για ανηλίκους.

Online Παιχνίδια

- Παιχνίδια μέσω φυλλομετρητή: απλά παιχνίδια που παρέχονται δωρεάν σε ιστοσελίδες που στηρίζονται στις διαφημίσεις.
- Διαφημιστικά παιχνίδια
- Παιχνίδια δικτύου που εγκαθίστανται στον Η/Υ και παίζονται σε σύνδεση με το Διαδίκτυο.
- MMORPG («Massively Multiplayer Online Role Playing Games»): δικτυακά παιχνίδια
  - μεγάλος αριθμός παικτών
  - εξελίσσονται ακόμα και αν ο παίκτης δεν συμμετέχει

Online Παιχνίδια – Πιθανά Προβλήματα

- Ακατάλληλο περιεχόμενο
- Έκθεση σε διαφημιστικό υλικό
- Αλληλεπίδραση με άλλους χαρακτήρες
- Υπερβολική ενασχόληση
- Διαταραχή συμπεριφοράς

Τζόγος και Διαδίκτυο

- Κίνδυνος χρηματικής απώλειας
- Εθισμός
- Κίνδυνοι ηλεκτρονικών συναλλαγών
- Πολύωρη παραμονή μπροστά στον Η/Υ
- Ελέγξτε πρώτα τους όρους χρήσης
- Κάντε μια έρευνα στο Διαδίκτυο και ελέγξτε την αξιοπιστία του δικτυακού τόπου

Υπερβολική Ενασχόληση – «Εθισμός» στο Διαδίκτυο

- Κριτήρια υπερβολικής ενασχόλησης
  - Σύνδρομο Απόσυρσης
  - Χρήση Διαδικτύου για αποφυγή συμπτωμάτων απόσυρσης
  - Παραμονή online για μεγάλο χρονικό διάστημα
  - Κατανάλωση υπερβολικού χρόνου / χρήματος σε αγορά λογισμικού, υλικού (HW), κ.λπ.
  - Δυσλειτουργικότητα του ατόμου
  - Συνέχιση χρήσης παρά τα προβλήματα που του δημιουργεί

Επιβλαβές περιεχόμενο

- Σεξουαλικής φύσεως περιεχόμενο
  - πορνογραφία ενηλίκων. Νόμιμη αλλά σοκαριστική και επιβλαβής για παιδιά
  - παράνομη παιδική πορνογραφία.
- Παρότρυνση σε αυτοκαταστροφικές συμπεριφορές
  - Ανορεξία
  - Αυτοκτονία
- Βία, ρατσισμός, ξενοφοβία

Παράνομο - Επιβλαβές Περιεχόμενο Συμβουλές

- Κανένα τεχνικό μέσο δεν είναι 100% αποτελεσματικό.
- Μην αφήνετε τα παιδιά χωρίς επίβλεψη στο σερφάρισμα
- Χρησιμοποιήστε κάποιο εργαλείο γονεϊκού ελέγχου ή φίλτρο περιεχομένου για το Διαδίκτυο λαμβάνοντας πάντα υπόψη την ηλικία και τις ανάγκες του χρήστη.
- Ορίστε ως αρχική σελίδα του φυλομετρητή σας μια σελίδα της επιθυμίας σας. Μην επιτρέπετε σε προγράμματα την αλλαγή της αρχικής σας σελίδας.

Φίλτρα Περιεχομένου / Εργαλεία Γονεϊκού Ελέγχου

- Ελέγχουν την πρόσβαση σε πληροφορίες ή υπηρεσίες στο Διαδίκτυο σύμφωνα με κριτήρια
- Εγκαθίστανται
  - στον Η/Υ του χρήστη
  - σε κεντρικό υπολογιστή κάποιου φορέα (π.χ. proxy server σε μια περιφέρεια) ή
  - στους Η/Υ παρόχου υπηρεσιών Διαδικτύου
- Δυνατές ενέργειες / λειτουργίες
  - προειδοποίηση για προβληματική ιστοσελίδα
  - καταγραφή λεπτομερειών κίνησης ενός χρήστη στο Διαδίκτυο
  - μπλοκάρισμα ύποπτων ιστοχώρων
  - πρόσβαση σε συγκεκριμένες ώρες και ημέρες

Φίλτρα Περιεχομένου / Εργαλεία Γονεϊκού Ελέγχου ΙΙ

- **Λευκές Λίστες** (**white lists**): ιστοσελίδες κατάλληλες για ανηλίκους. Επιτρέπετε η πρόσβαση μόνο σε αυτές.
- Λίστες «Όχι» (**black lists**): ιστοσελίδες που πρέπει να αποφευχθούν. Μπλοκάρεται η πρόσβαση σε αυτές.
- Μπλοκάρισμα ιστοσελίδων με **απαγορευμένες λέξεις**
- Φιλτράρισμα βάσει αυτόματης **ταξινόμησης του περιεχομένου**
- **Αυτοαξιολόγηση** ιστοσελίδων βάσει ετικετών που τοποθετούν οι δημιουργοί τους.Το φίλτρο διαβάζει τις ετικέτες και αποφασίζει αν θα επιτρέψει την πρόσβαση
- Συνδυασμός μεθόδων φιλτραρίσματος

Ηλεκτρονικές Συναλλαγές

- Δυνατότητα διεκπεραίωσης συναλλαγών μέσω Διαδικτύου:
  - **με επιχειρήσεις** (ηλεκτρονικό εμπόριο «e-commerce»)
  - **με το Δημόσιο** (ηλεκτρονική διακυβέρνηση / «e-government»)
  - **με τράπεζες** για πληρωμή λογαριασμών και διεκπεραίωση τραπεζικών εργασιών («e-banking»)

Ηλεκτρονικές Συναλλαγές - Παρεξηγήσεις

- λανθασμένη άποψη ότι κάθε είδους συναλλαγή στο Διαδίκτυο
  - είναι αναξιόπιστη
  - μπορεί να προκαλέσει
    - απώλεια χρημάτων (απάτες) ή
    - κακή χρήση προσωπικών στοιχείων

Ηλεκτρονικές Συναλλαγές - Οφέλη

- Πρόσβαση σε προϊόντα και υπηρεσίες από όλο τον κόσμο
- Πρόσβαση 24 ώρες το 24ωρο
- Μηδενικός χρόνος αναμονής σε ουρές
- Γρηγορότερη εξυπηρέτηση
- Πολλές φορές μικρότερο χρηματικό κόστος
- Εύκολη σύγκριση τιμών
- Ευκολία πρόσβασης στα άτομα με κινητικές δυσκολίες

Ασφαλείς Ηλεκτρονικές Συναλλαγές

- Εξετάστε
  - την αξιοπιστία του δικτυακού τόπου και κατόπιν
  - ελέγξτε τις μεθόδους συναλλαγών που σας παρέχονται

Ηλεκτρονικές Συναλλαγές Αξιοπιστία Δικτυακών Τόπων

- Σαφής προσδιορισμός της εταιρείας και των στοιχείων της
- Τα χαρακτηριστικά του προϊόντος / της υπηρεσίας και οι όροι της εγγύησης είναι σαφή και εύκολα προσβάσιμα
- Οι όροι των συμβάσεων («όροι χρήσης») είναι εύκολα προσβάσιμοι και ξεκάθαροι
- Η τιμή του προϊόντος περιλαμβάνει τυχόν επιπλέον χρεώσεις
- Ο ιστοχώρος παρέχει ασφαλή τρόπο πληρωμής
- Δικαίωμα ανάκλησης της παραγγελίας
- Οι παραγγελίες επιβεβαιώνονται με email
- «Πολιτική απορρήτου» για την χρησιμοποίηση των προσωπικών στοιχεία του χρήστη
- Σε περίπτωση αποριών επικοινωνήστε με την εταιρεία / υπηρεσία τηλεφωνικά ή με e-mail και ζητήστε διευκρινήσεις
- Ερευνήστε τη φήμη της όποιας εταιρείας στο Διαδίκτυο

Ασφαλείς Ηλεκτρονικές Συναλλαγές

- Μόνο μέσω μεθόδων «ασφαλών ηλεκτρονικών συναλλαγών» (**SSL**).
- Η διεύθυνση της ιστοσελίδας όπου καταχωρούμαι προσωπικά μας στοιχεία ή στοιχεία πληρωμής πρέπει να ξεκινά με **https://** («s» από την λέξη «secure», δηλαδή ασφαλές) και όχι απλά με “http://”.
- Στο δεξιό άκρο της γραμμής δ/νσεων του φυλομετρητή θα πρέπει να βρίσκεται ένα κλειστό κίτρινο **λουκέτο**.
  - υποδεικνύει πως η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών που εισάγετε.
- Το πιστοποιητικό ασφαλείας της τοποθεσίας αντιστοιχεί στο όνομα της τοποθεσίας.
- Το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο.
  - Κάντε κλικ στο λουκέτο και επιλέξτε προβολή πιστοποιητικών για να δείτε το πιστοποιητικό ασφαλείας της τοποθεσίας. Ο κάτοχος θα πρέπει να ταυτίζεται με το όνομα της τοποθεσίας.

Ηλεκτρονικές Απάτες

- Phising
- Pharming
- Scams

Απάτες - Phising

- Από το αγγλικό “fishing”/ ψάρεμα.
- Προσπάθεια απόσπασης προσωπικών στοιχείων (τραπεζικοί λογαριασμοί, αριθμοί πιστωτικών καρτών, κ.α.) με κάποιο ψεύτικο πρόσχημα.
- Επιχειρείται με τη αποστολή κάποιου **spam email** (καθώς και με αναδυόμενο παράθυρο ή άμεσο μήνυμα), το οποίο ισχυρίζεται –ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία
- Το e-mail δείχνει αρκετά επίσημο και παραπέμπει με υπερσύνδεσμο σε ιστοσελίδα πανομοιότυπη με την πραγματική
- Κανένας οργανισμός δεν ζητά προσωπικά στοιχεία με e-mail

Απάτες - Pharming (παραπλάνηση)

- Ανακατεύθυνση από μία τοποθεσία (τράπεζες κ.λπ.) σε μία άλλη πανομοιότυπη, που είναι όμως απάτη.
- Μπορεί να ανακατευθυνθείτε σε μία ψεύτικη ιστοσελίδα χωρίς να το γνωρίζετε.
- Προσπαθούν να καταχωρήσετε ευαίσθητα προσωπικά δεδομένα με σκοπό την εξαπάτηση σας.

Απάτες - Scams

- Αποστέλλεται email στο υποψήφιο θύμα.
- Ζητούνται κάποια χρήματα για την ολοκλήρωση κάποιας συναλλαγής.
- Το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.
- π.χ. διεθνή λαχεία, δημοπρασίες, ψεύτικες ευκαιρίες απασχόλησης.

Spam

- Ανεπιθύμητο διαφημιστικό ηλεκτρονικό μήνυμα.
- Τι να κάνετε εάν λάβετε spam;
  - Δεν θα πρέπει να απαντήσετε σε αυτό, να κάνετε κλικ ή να το προωθήσετε.
  - Διαγράψτε το χωρίς να το ανοίξετε ή να κάνετε κλικ σε κάποιο σύνδεσμο μέσα σε αυτό.
- Γιατί είναι ενοχλητικό;
  - Πιθανόν να εμπεριέχει απάτη ή να μολύνει τον υπολογιστή σας με ιό ή άλλο κακόβουλο λογισμικό.
- Προστασία από ανεπιθύμητα μηνύματα:
  - Μην δίνετε σε οποιονδήποτε την ηλεκτρονική σας διεύθυνση.
  - Χρησιμοποιήστε ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων.
  - Ποτέ μην ανοίγετε τα συνημμένα των μηνυμάτων εκτός και αν γνωρίζετε περί τίνος πρόκειται.
  - Αναφέρετε στις αρμόδιες αρχές τους αποστολείς των ανεπιθύμητων μηνυμάτων.

Downloading

- Downloading είναι η διαδικασία λήψης αρχείων, συνήθως από το διαδίκτυο.
- Αυτά τα αρχεία μπορεί να είναι αυτό που αναμένατε, αλλά μπορεί να είναι και εντελώς επικίνδυνα, μολυσμένα με κακόβουλο λογισμικό.
- Κακόβουλο λογισμικό (malware): λογισμικό το οποίο μπορεί να βλάψει τον υπολογιστή σας.
  - Ιοί (πιθανή καταστροφή δεδομένων ή ανεπίτρεπτη πρόσβαση τρίτων στον Η/Υ μας)
  - Trojans (Δούρειο Ίπποι)
  - Worms
  - προγράμματα υποκλοπής (πιθανή αλλαγής συμπεριφοράς του Η/Υ-καθυστερήσεις, απόσπαση κωδικών πρόσβασης κλπ)
  - άλλα ενοχλητικά προγράμματα.

Συμβουλές Ασφαλείας Ι

- Επικαιροποίηση (updates) λειτουργικού συστήματος και λογισμικού υπολογιστών
- Εγκατάσταση Λογισμικού Ασφάλειας (Τείχος Προστασίας - Firewall, Αντιϊκό πρόγραμμα - AntiVirus, Αφαίρεσης Λογισμικού Υποκλοπής - AntiSpyware, κα).
- Ρυθμίστε το Antivirus να εξετάζει e-mail και συνημμένα αρχεία πριν τα ανοίξετε.
- Χρησιμοποιήστε φίλτρο ανεπιθύμητων μηνυμάτων (antispam).
- Αλλαγή προσωρινών κωδικών ασφάλειας (default passwords) και χρήση προσωπικών κωδικών ασφάλειας
- Μη κοινοποίηση κωδικών ασφάλειας σε οποιονδήποτε

Συμβουλές Ασφαλείας ΙΙ

- Μη εκτέλεση και εγκατάσταση αγνώστου λογισμικού από οποιαδήποτε πηγή και εάν προέρχεται αυτό (Web, E-mail, download, κα).
- Πάντα εισάγουμε το URL απευθείας στον εκάστοτε browser
- Αποφύγετε να κάνετε ηλεκτρονικές συναλλαγές από υπολογιστές τρίτων ή δημόσια προσβάσιμους
- Περιορίζουμε τις προσωπικές πληροφορίες που δίνουμε σε ιστοσελίδες κοινωνικής δικτύωσης
- Αξιοποιήστε τη δυνατότητα για πολλαπλούς λογαριασμούς e-mail και στιγμιαίων μηνυμάτων
- Να μην αποθηκεύετε προσωπικούς κωδικούς πρόσβασης στον υπολογιστή
- Χρήση Λιστών ηλεκτρονικών μηνυμάτων (mailing lists)