ΚΕΦΑΛΑΙΟ 16

Ασφάλεια και Προστασία στο Διαδίκτυο

Διδακτικές ενότητες

16.1 Ασφάλεια υπολογιστικού συστήματος
16.2 Θέματα ασφάλειας και προστασίας στο Διαδίκτυο
16.3 Πληροφορίες, πνευματικά δικαιώματα και πειρατεία λογισμικού στο Διαδίκτυο
16.4 Ιδιωτικότητα και προσωπικά δεδομένα στο Διαδίκτυο

Διδακτικοί στόχοι

Σκοπός του κεφαλαίου είναι οι μαθητές να εντοπίζουν και να διαχειρίζονται θέματα ασφάλειας και προστασίας στο Διαδίκτυο.

Οι μαθητές πρέπει να είναι σε θέση:

√ να αναγνωρίζουν τα είδη κακόβουλου λογισμικού.
√ να διακρίνουν τις απαραίτητες εφαρμογές προστασίας από κακόβουλο λογισμικό.
√ να γνωρίζουν τι απαιτείται για ασφαλή διεκπεραίωση ηλεκτρονικών συναλλαγών.
√ να αναγνωρίζουν και να αποφεύγουν επιβλαβές περιεχόμενο στο Διαδίκτυο.
√ να χρησιμοποιούν με ασφάλεια τις υπηρεσίες του Διαδικτύου.
√ να αναζητούν με κριτική σκέψη πληροφορίες στον Παγκόσμιο Ιστό.
√ να διαχειρίζονται σωστά τα θέματα των πνευματικών δικαιωμάτων στο Διαδίκτυο.
√ να προστατεύουν την ιδιωτικότητά τους και τα προσωπικά τους δεδομένα στο Διαδίκτυο.

Ερωτήματα

√ Γνωρίζετε τα είδη κακόβουλου λογισμικού;
√ Ποια προγράμματα ασφαλείας γνωρίζετε;
√ Έχετε κάνει ηλεκτρονικές συναλλαγές;
√ Υπάρχει παράνομο και επιβλαβές περιεχόμενο στο Διαδίκτυο;
√ Υπάρχουν ζητήματα ασφαλείας στη χρήση του ηλεκτρονικού ταχυδρομείου;
√ Υπάρχουν αναληθείς και αναξιόπιστες πληροφορίες στο Διαδίκτυο;
√ Τι είναι η πειρατεία λογισμικού;
√ Πώς μπορείτε να προστατέψετε τα προσωπικά σας δεδομένα στο Διαδίκτυο;

Βασική ορολογία

Κακόβουλο λογισμικό, λογισμικό ασφαλείας, ηλεκτρονικές συναλλαγές, επιβλαβές περιεχόμενο, ηλεκτρονικό ψάρεμα, μηνύματα spam, πνευματικά δικαιώματα, πειρατεία λογισμικού, προσωπικά δεδομένα

Εισαγωγή

Το παρόν κεφάλαιο πραγματεύεται θέματα ασφάλειας και προστασίας στο Διαδίκτυο. Αναφέρεται στο κακόβουλο λογισμικό, στις ηλεκτρονικές συναλλαγές, στο επιβλαβές περιεχόμενο και στους κινδύνους που διατρέχουμε από μηνύματα ηλεκτρονικού ταχυδρομείου. Θα αναδειχθεί η σημασία της αξιολόγησης των πληροφοριών και θα αναλυθεί το θέμα των πνευματικών δικαιωμάτων. Τέλος, θα γίνει αναφορά στην ιδιωτικότητα και στην προστασία των προσωπικών μας δεδομένων στο Διαδίκτυο.

16.1 Ασφάλεια υπολογιστικού συστήματος

Κακόβουλο λογισμικό

Τα δεδομένα και το λογισμικό, τα οποία είναι αποθηκευμένα με τη μορφή αρχείων σε ψηφιακά αποθηκευτικά μέσα, κινδυνεύουν να αλλοιωθούν, να διαγραφούν ή να υποκλαπούν, κυρίως από βλάβες στα αποθηκευτικά μέσα, από κακόβουλο λογισμικό (malware) και από μη εξουσιοδοτημένες παρεμβάσεις κακόβουλων χρηστών («επιθέσεις»). **Κακόβουλο λογισμικό** ονομάζεται το λογισμικό το οποίο εκ προθέσεως διαθέτει τις απαιτούμενες εντολές για να βλάψει ένα υπολογιστικό σύστημα. Επομένως, τίθενται θέματα ασφάλειας και προστασίας στα υπολογιστικά συστήματα.

Εικόνα 16.1. Είδη κακόβουλου λογισμικού.

Υπάρχουν διάφορα είδη κακόβουλου λογισμικού. Τα βασικότερα είναι τα παρακάτω:

- √ **Ιός (virus):** κακόβουλο πρόγραμμα που δημιουργεί προβλήματα στην ομαλή λειτουργία του υπολογιστή μας (π.χ. αδυναμία εκκίνησης, ελάττωση της ταχύτητας επεξεργασίας, προβλήματα στη λειτουργία των εγκατεστημένων εφαρμογών, εμφάνιση ενοχλητικών μηνυμάτων) και στην ασφάλεια των αρχείων μας (π.χ. καταστροφή). Ο ιός προσκολλάται σε κάποιο πρόγραμμα ή αρχείο και ενεργοποιείται συνήθως μόλις προσπαθήσουμε να τρέξουμε το πρόγραμμα ή να ανοίξουμε το αρχείο. Ένας ιός μπορεί να φτάσει στον υπολογιστή μας κυρίως μέσω του Διαδικτύου είτε ως συνημμένο αρχείο σε μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) είτε από την περιήγησή μας ή το κατέβασμα αρχείων από μη ασφαλείς ιστοσελίδες.
- √ **Σκουλήκι (Worm):** βλαβερό πρόγραμμα που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του διαμέσου των δικτύων υπολογιστών. Δεν χρειάζεται κάποιο άλλο πρόγραμμα ως όχημα για τη διακίνησή του. Ένα σκουλήκι δεν είναι τόσο καταστροφικό όπως ένας ιός, επειδή δεν σβήνει αρχεία, αλλά μειώνει την ταχύτητα σύνδεσης στο Διαδίκτυο, μια και στέλνει αντίγραφά του σε άλλους υπολογιστές και καταναλώνει τους πόρους (π.χ. μνήμη) του υπολογιστή που έχει μολύνει κάνοντάς τον πιο αργό.
- √ **Δούρειος ίππος (Trojan horse):** κακόβουλο πρόγραμμα μεταμφιεσμένο σε θεμιτό λογισμικό (π.χ. παιχνίδι, πρόγραμμα ανίχνευσης ιών) που στην πραγματικότητα δρα παρασκηνιακά αναλαμβάνοντας εξ αποστάσεως τον έλεγχο του μολυσμένου υπολογιστή. Μπορεί να διαγράψει αρχεία, να υποκλέψει προσωπικά δεδομένα (π.χ. κωδικούς πρόσβασης) ή να χρησιμοποιήσει τον μολυσμένο υπολογιστή για επίθεση σε άλλους υπολογιστές. Οι δούρειοι ίπποι δεν αναπαράγουν και δεν διαδίδουν τους εαυτούς τους.

Οι συγγραφείς ιών, οι χάκερς (hackers) και άλλα άτομα με κακόβουλες προθέσεις βρίσκουν συνεχώς νέους τρόπους για να επιτεθούν στους στόχους τους.

Οι ιοί διαδίδονται συνήθως από τον έναν υπολογιστή στον άλλο με δύο τρόπους:

α) μέσω φορητού μέσου αποθήκευσης (π.χ. USB flash memory) και
β) μέσω δικτύου υπολογιστών.

Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος λόγω της ευρείας χρήσης του Διαδικτύου. Οι ιοί διαδίδονται γρήγορα μέσω του ηλεκτρονικού ταχυδρομείου (ως συνημμένα αρχεία ή τμήμα αυτού καθαυτού του μηνύματος). Για τον λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν σάρωση των μηνυμάτων και των συνημμένων τους αρχείων.

- **Λογισμικό Κατασκοπίας (Spyware):** κακόβουλο πρόγραμμα που προσκολλάται κρυφά σε αρχεία που κατεβάζουμε από το Διαδίκτυο ή κατεβαίνει και εγκαθίσταται αυτόματα σε έναν υπολογιστή κατά την επίσκεψή μας σε μολυσμένες ιστοσελίδες. Παρακολουθεί τη διαδικτυακή δραστηριότητα του χρήστη του μολυσμένου υπολογιστή (π.χ. ποιους ιστότοπους επισκέπτεται πιο συχνά) και την αποστέλλει σε τρίτους, κυρίως εταιρείες, με σκοπό την αποστολή στοχευμένων διαφημιστικών μηνυμάτων. Ένα πρόγραμμα κατασκοπίας μπορεί να αλλάξει την αρχική σελίδα του φυλλομετρητή, να προσθέσει ανεπιθύμητες γραμμές εργαλείων σε αυτόν ή να εμφανίζει συνεχώς παράθυρα με ενοχλητικές διαφημίσεις.

Εικόνα 16.2. Το spyware παρακολουθεί τη διαδικτυακή μας δραστηριότητα.

Τρόποι προστασίας από κακόβουλο λογισμικό

Για να προστατέψουμε τον υπολογιστή μας από κακόβουλο λογισμικό κατά την περιήγησή μας στο Διαδίκτυο, θα πρέπει να:

- ενημερώνουμε τακτικά το Λειτουργικό Σύστημα και τις εφαρμογές του υπολογιστή μας.
- ρυθμίζουμε κατάλληλα τις επιλογές ασφαλείας του φυλλομετρητή μας.
- προσέχουμε ποιους ιστότοπους επισκεπτόμαστε και ποια αρχεία κατεβάζουμε από το Διαδίκτυο.
- μην ανοίγουμε συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου που μας αποστέλλουν άγνωστοι ή με ύποπτο θέμα.
- έχουμε πάντα εγκατεστημένο στον υπολογιστή μας **λογισμικό ασφαλείας**: λογισμικό προστασίας από ιούς (antivirus) και τείχος προστασίας (firewall). Το **λογισμικό προστασίας από ιούς (antivirus)** πρέπει να ενημερώνεται τακτικά με πρόσφατους ορισμούς ιών (virus definitions). Οι ορισμοί ιών είναι αρχεία που περιέχουν τα ψηφιακά αποτυπώματα γνωστών ιών (virus signatures). Το λογισμικό προστασίας από ιούς για τον εντοπισμό κακόβουλου ή πιθανώς ανεπιθύμητου λογισμικού συγκρίνει το περιεχόμενο των αρχείων με τους ορισμούς των ιών που διαθέτει. Μόλις εντοπίσει μολυσμένο με ιό αρχείο, μας ενημερώνει και στις περισσότερες περιπτώσεις προτείνει επιδιόρθωση, σβήσιμο ή απομόνωσή του.

Επειδή το λογισμικό ασφαλείας δεν μας προστατεύει ποτέ απόλυτα από τους ιούς, χρήσιμο είναι να παίρνουμε σε τακτά χρονικά διαστήματα αντίγραφα ασφαλείας των αρχείων μας.

Οι φορητές συσκευές (έξυπνα κινητά, tablets) μπορούν να μολυνθούν εξίσου από κακόβουλο λογισμικό, γι' αυτό πρέπει και σε αυτές να λαμβάνουμε ανάλογα μέτρα προστασίας.

Το **antivirus** είναι λογισμικό που παρακολουθεί όλες τις online δραστηριότητες και προστατεύει τον υπολογιστή μας από ιούς, worms, trojan horses, spyware και άλλα είδη κακόβουλων προγραμμάτων.

Το **τείχος προστασίας (firewall)** μπορεί να εμποδίσει τους εισβολείς ή το κακόβουλο λογισμικό να αποκτήσουν πρόσβαση στον υπολογιστή μας μέσω του Διαδικτύου. Το firewall μπορεί να παρέχεται από το Λειτουργικό Σύστημα (ενσωματωμένο) ή να εγκαθίσταται ως αυτόνομο πρόγραμμα ή να προσφέρεται μαζί με antivirus και άλλα προγράμματα ασφαλείας (οικογένεια προγραμμάτων, με ονομασία όπως Internet Security).

Ερωτήσεις - Δραστηριότητες

1. Τι κινδύνους διατρέχει ο υπολογιστής σας, αν μολυνθεί από κακόβουλο λογισμικό;
2. Ποια προγράμματα ασφαλείας (antivirus, firewall) είναι εγκατεστημένα στον υπολογιστή σας στο εργαστήριο Πληροφορικής; Δείτε αν είναι ενημερωμένα.
3. Επισκεφθείτε ιστότοπους γνωστών λογισμικών ασφαλείας και αναζητήστε πληροφορίες γι' αυτά (π.χ. AVG http://www.avg.com, Avast http://www.avast.com/el-gr, Norton http://gr.norton.com, ESET http://www.eset.com/gr).

16.2 Θέματα ασφάλειας και προστασίας στο Διαδίκτυο

Ηλεκτρονικές συναλλαγές

Το Διαδίκτυο αποτελεί ένα σύγχρονο μέσο για διεκπεραίωση ποικίλων συναλλαγών με το Δημόσιο, με επιχειρήσεις και με τράπεζες. Τα οφέλη είναι πολλαπλά από την εκμετάλλευση των εφαρμογών ηλεκτρονικών συναλλαγών: γρήγορη εξυπηρέτηση, διαθεσιμότητα των υπηρεσιών σε 24ωρη βάση, εύκολη πρόσβαση σε άτομα με κινητικές δυσκολίες, πιθανή μείωση του κόστους αγοράς αγαθών, εύκολη σύγκριση τιμών και προσφορών από διαφορετικούς προμηθευτές προϊόντων.

Παραδείγματα ηλεκτρονικών συναλλαγών:
α) **δημόσιο** (ηλεκτρονική διακυβέρνηση ή αλλιώς «e-government»): αναζήτηση πιστοποιητικών, φορολογικές συναλλαγές, πληρωμή οφειλών
β) **τράπεζες** («e-banking»): διαχείριση τραπεζικών λογαριασμών, πληρωμή λογαριασμών
γ) **επιχειρήσεις** («e-commerce»): αγοραπωλησίες προϊόντων.

Δυστυχώς όμως, παρά το υψηλό επίπεδο αξιοπιστίας των εφαρμογών ηλεκτρονικών συναλλαγών, υπάρχουν σημαντικά θέματα ασφάλειας που πρέπει να εντοπίζουμε και να διαχειριζόμαστε. Χρειάζεται να αντιλαμβανόμαστε άμεσα αναξιόπιστες υπηρεσίες και προσπάθειες οικονομικής μας εξαπάτησης.

Όταν επισκεπτόμαστε έναν ιστότοπο για ηλεκτρονική συναλλαγή, θα πρέπει αρχικά να ελέγχουμε, όσο είναι αυτό εφικτό, την αξιοπιστία του. Σε έναν αξιόπιστο ιστότοπο υπάρχει ξεκάθαρος προσδιορισμός του φορέα (δημόσιου ή ιδιωτικού) με το όνομά του, την ιδιότητά του και τα στοιχεία επικοινωνίας του. Επίσης, υπάρχουν αναλυτικές πληροφορίες για τους όρους χρήσης και ασφάλειας σε ιστότοπους επιχειρήσεων: όροι χρήσης, ασφάλεια συναλλαγών, προσωπικά δεδομένα (πολιτική απορρήτου), διαδικασία υποβολής παραγγελίας, τρόποι πληρωμής, τρόποι αποστολής, πολιτική επιστροφών.

Το πρωτόκολλο **SSL (Secure Sockets Layer)** παρέχει ασφάλεια κατά τη μετάδοση ευαίσθητων δεδομένων στο Διαδίκτυο. Χρησιμοποιεί μεθόδους κρυπτογράφησης για παροχή απόρρητης επικοινωνίας.

Μία σημαντική παράμετρος στις ηλεκτρονικές συναλλαγές είναι ο ασφαλής τρόπος σύνδεσης και διεκπεραίωσης των εργασιών, για παράδειγμα καταχώριση προσωπικών στοιχείων και στοιχείων πληρωμής (συνήθως δεδομένα πιστωτικής κάρτας). Οι αξιόπιστοι ιστότοποι παρέχουν συναλλαγές μόνο μέσω ασφαλών διαδικασιών, κυρίως με χρήση του πρωτοκόλλου **SSL (Secure Sockets Layer)**. Για να αντιληφθούμε αν παρέχονται τέτοιες διαδικασίες, μπορούμε να κοιτάξουμε τη διεύθυνση της ιστοσελίδας στην οποία βρισκόμαστε. Θα πρέπει να ξεκινάει με **https**:// και

Εικόνα 16.3. Ένδειξη ασφαλούς σύνδεσης σε ιστοσελίδα.

όχι απλά με http://. Το γράμμα **s** προέρχεται από τη λέξη secure (ασφαλής).

Επιβλαβές περιεχόμενο

Στο Διαδίκτυο διακινούνται ιδέες, πληροφορίες και οπτικοακουστικό υλικό με μεγάλη ευκολία και ταχύτητα. Σε πολλές περιπτώσεις δεν είναι εύκολος και δεν πραγματοποιείται έλεγχος του περιεχομένου των ιστοσελίδων. Είναι δυνατό σε κάποιες περιπτώσεις το περιεχόμενο να είναι παράνομο και συνάμα επιβλαβές για τα παιδιά, σε άλλες όμως περιπτώσεις νόμιμο αλλά ακατάλληλο για μικρές ηλικίες. Βάσει της νομοθεσίας, παράνομοι θεωρούνται οι ιστότοποι που περιέχουν προτροπές σε παράνομες πράξεις, οικονομικές απάτες, υλικό εκφοβισμού, συκοφαντική δυσφήμιση, παραβίαση προσωπικών δεδομένων και πνευματικής ιδιοκτησίας, υλικό παιδικής πορνογραφίας κ.ά. Μία λύση στον έλεγχο του περιεχομένου αποτελεί η χρήση λογισμικού γονικού έλεγχου ή φιλτραρίσματος.

Ιδιαίτερη περίπτωση αποτελούν τα ηλεκτρονικά παιχνίδια πολλών χρηστών που παίζονται μέσω του Διαδικτύου. Εκτός από τα προβλήματα που απορρέουν από την υπερβολική ενασχόληση με τα παιχνίδια αυτά, υπάρχει και ο κίνδυνος έκθεσης των παιδιών σε ακατάλληλο περιεχόμενο (π.χ. βίαιες σκηνές). Οι περισσότερες εταιρείες που δημιουργούν ηλεκτρονικά παιχνίδια συμμετέχουν στο Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Παιχνίδια (PEGI Rating System), το οποίο προσφέρει ετικέτες για τον χαρακτηρισμό της καταλληλότητας των παιχνιδιών με βάση την ηλικία και το περιεχόμενο.

Επιβλαβή ή ανεπιθύμητα μηνύματα e-mail

Το ηλεκτρονικό ταχυδρομείο αποτελεί αναμφισβήτητα μία από τις πιο χρήσιμες υπηρεσίες του Διαδικτύου. Δυστυχώς όμως υπάρχουν και οι παρακάτω αρνητικές πλευρές:

- √ μετάδοση ιών: μέσω μολυσμένων συνημμένων αρχείων.
- √ ηλεκτρονικό ψάρεμα (phishing): ένα e-mail, το οποίο φαινομενικά προέρχεται από μια γνωστή και αξιόπιστη εταιρεία, αποστέλλεται σε μεγάλο αριθμό διευθύνσεων ηλεκτρονικού ταχυδρομείου. Το e-mail αυτό μπορεί να παραπέμπει τον παραλήπτη σε έναν πλαστό ιστότοπο όπου πρέπει να δώσει τα προσωπικά του στοιχεία (π.χ. κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας).
- √ ανεπιθύμητα μηνύματα spam: το ηλεκτρονικό ισοδύναμο των μαζικών αποστολών διαφημιστικών επιστολών για προώθηση προϊόντων.

Εικόνα 16.4. Μπορείτε να καταγγείλετε παράνομο περιεχόμενο στο Διαδίκτυο.

Τα συστήματα φιλτραρίσματος και τα εργαλεία γονικού ελέγχου είναι προγράμματα που ρυθμίζουν την πρόσβαση σε πληροφορίες ή υπηρεσίες του Διαδικτύου σύμφωνα με καθοριζόμενα κριτήρια.
Μπορούν να εγκατασταθούν στον υπολογιστή του χρήστη, σε ένα κεντρικό υπολογιστή κάποιου φορέα ή στους υπολογιστές ενός παρόχου υπηρεσιών Διαδικτύου (ISP).

Εικόνα 16.5. Οι ετικέτες ηλικιακής κατάταξης σύμφωνα με το σύστημα PEGI.

Εικόνα 16.6. Κάποια μηνύματα spam μπορεί να περιέχουν προσφορές για απάτες ή κακόβουλο λογισμικό.

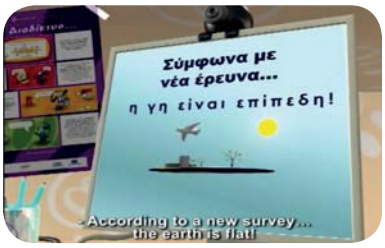
Ερωτήσεις - Δραστηριότητες

1. Διαβάστε στον ιστότοπο www.saferinternet.gr πληροφορίες και συμβουλές για την πρόληψη και αντιμετώπιση των πιο διαδεδομένων ηλεκτρονικών μορφών οικονομικής εξαπάτησης και δημιουργήστε μια παρουσίαση ή ένα ενημερωτικό βίντεο.
2. Έχετε συναντήσει ποτέ παράνομο περιεχόμενο στο Διαδίκτυο; Διερευνήστε και παρουσιάστε κατηγορίες παράνομου περιεχομένου καθώς και τρόπους προστασίας. Ενδεικτική πηγή: www.safeline.gr.
3. Επισκεφθείτε τον ιστότοπο του PEGI (http://pegi.info/gr/), μελετήστε τις επισημάνσεις και, χρησιμοποιώντας το πεδίο Γρήγορη Αναζήτηση, ελέγξτε την καταλληλότητα ενός γνωστού σας ηλεκτρονικού παιχνιδιού (π.χ. World of Warcraft, League of Legends).

16.3 Πληροφορίες, πνευματικά δικαιώματα και πειρατεία λογισμικού στο Διαδίκτυο

Αξιολόγηση πληροφοριών

Ο Παγκόσμιος Ιστός έφερε επανάσταση στον τρόπο που αναζητούμε και αποκτούμε πρόσβαση σε πληροφορίες. Γρήγορα, εύκολα, με ελάχιστο ή καθόλου κόστος, μπορούμε να αντλήσουμε χρήσιμα στοιχεία για τα θέματα που μας ενδιαφέρουν ή μας απασχολούν, και να ενημερωθούμε για τις εξελίξεις σε διάφορους τομείς (πολιτική, οικονομία, τέχνες, ψυχαγωγία, τεχνολογία κ.λπ.). Ταυτόχρονα με την έλευση του Web 2.0 (blogs, wikis, social media) ο χρήστης δεν ανακτά μόνο πληροφορίες από κάποια ιστοσελίδα, αλλά έχει τη δυνατότητα να δημιουργήσει και να διακινήσει το δικό του περιεχόμενο.



Εικόνα 16.7. Παράδειγμα αναξιόπιστης πληροφορίας: η γη είναι επίπεδη! (απόσπασμα από βίντεο της εκστρατείας της δράσης ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου)

Ο σύγχρονος τρόπος άντλησης και διακίνησης πληροφοριών απαιτεί φιλτράρισμά τους και κριτική αξιοποίησή τους. Αναμφισβήτητα δεν είναι όλες οι πληροφορίες που καταχωρίζονται στο Διαδίκτυο αξιόπιστες και έγκυρες. Πολλές πληροφορίες δεν είναι μόνο αναληθείς ή εσφαλμένες, αλλά μπορεί να είναι και επικίνδυνες (προπαγανδιστικές, παραπλανητικές). Συνεπώς, η κρίση του χρήστη σε ό,τι αφορά σε κάθε διαθέσιμη πληροφορία αναρτημένη στο Διαδίκτυο είναι απαραίτητη. Μερικές χρήσιμες πρακτικές συμβουλές που μπορούμε να ακολουθήσουμε είναι οι παρακάτω:

- √ διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και με άλλες πηγές, π.χ. άλλους ιστότοπους, βιβλία, εγκυκλοπαίδειες.
- √ αναζητούμε πληροφορίες σε έγκυρους ιστότοπους, π.χ. έγκριτες ψηφιακές βιβλιοθήκες, Πανεπιστήμια, γνωστούς οργανισμούς, φορείς και ιδρύματα.
- √ αξιολογούμε την αξιοπιστία των ιστοσελίδων που επισκεπτόμαστε με έλεγχο του συγγραφέα τους, του σκοπού τους (π.χ. ενημερωτικός, εμπορικός), των βιβλιογραφικών παραπομπών, της δημοφιλίας, της ένδειξης ανανέωσης, ακόμα και της ορθογραφίας και αισθητικής τους.

Πνευματικά δικαιώματα

Πνευματικό δικαίωμα είναι, όπως είδαμε και στο κεφάλαιο 4, το δικαίωμα που αποκτά κάποιος πάνω σε ένα πρωτότυπο πνευματικό δημιούργημα, π.χ. μουσική, συγγραφικό έργο, εικαστικό έργο, θεατρικό έργο, οπτικοακουστικό έργο, λογισμικό κ.λπ. Πνευματική ιδιοκτησία είναι το σύνολο των εξουσιών που δίνει ο νόμος στον ιδιοκτήτη ενός πνευματικού έργου (συγγραφέα, συνθέτη, προγραμματιστή κ.λπ.) να προστατεύσει, να διαχειριστεί και να αμειφθεί ακόμη από τρίτους, όταν εκείνοι εκμεταλλεύονται την πνευματική του περιουσία.

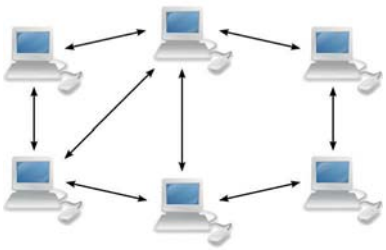
Στο Διαδίκτυο το ψηφιακό υλικό (κείμενα, εικόνες, μουσική, βίντεο κ.λπ.) που αναρτάται ή διακινείται προστατεύεται εξίσου από τη νομοθεσία περί πνευματικής ιδιοκτησίας. Μάλιστα οι περισσότεροι ιστότοποι περιέχουν αναλυτική αναφορά στην πνευματική τους ιδιοκτησία (copyright). Αν θέλουμε να χρησιμοποιήσουμε σε εργασία μας υλικό από το Διαδίκτυο, θα χρειαστεί πολλές φορές να ενημερώσουμε τον δημιουργό του και να ζητήσουμε την έγγραφη έγκρισή του. Σε περιπτώσεις που δεν γίνεται ρητή αναφορά σε πνευματικά δικαιώματα καλό είναι να αναφέρουμε τις πηγές μας.

Εικόνα 16.8. Στον ιστότοπο του Οργανισμού Πνευματικής Ιδιοκτησίας (http://opi.gr/) μπορείτε να βρείτε αναλυτικές πληροφορίες για το θέμα της πνευματικής ιδιοκτησίας.

Η προώθηση μέσω του Διαδικτύου παράνομων αντιγράφων έργων πνευματικής ιδιοκτησίας (π.χ. μουσικής, ταινιών, ηλεκτρονικών βιβλίων, προγραμμάτων) θεωρείται άδικη και παράνομη πράξη, και τιμωρείται. Το ζήτημα των πνευματικών δικαιωμάτων είναι δύσκολο να αντιμετωπιστεί λόγω της έκτασης και της πολυπλοκότητας του Διαδικτύου. Ο καθένας προσωπικά θα πρέπει να σέβεται τους δημιουργούς πνευματικών έργων και να δρα έντιμα και ηθικά.

Πειρατεία λογισμικού

Η πειρατεία λογισμικού αφορά στην παράνομη αντιγραφή και χρήση προγραμμάτων χωρίς την άδεια του δημιουργού τους και στην παράνομη αναπαραγωγή και διάθεση αντιγράφων προγραμμάτων με κίνητρο το οικονομικό όφελος. Το Διαδίκτυο αποτελεί το κυριότερο μέσο διακίνησης πειρατικού λογισμικού είτε μέσω ιστότοπων είτε μέσω ομότιμων δικτύων διαμοιρασμού αρχείων (peer to peer networks).



Εικόνα 16.9. Ομότιμα δίκτυα (peer to peer networks) χρησιμοποιούνται συνήθως για τη διακίνηση πειρατικού λογισμικού και παράνομων αντιγράφων αρχείων μουσικής και ταινιών.

Εκτός από την παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών λογισμικού, το παράνομο λογισμικό είναι πιθανό να βλάψει σοβαρά τον υπολογιστή σας. Πιο συγκεκριμένα:

- √ είναι πιθανό να χάσετε αρχεία ή δεδομένα με την εγκατάστασή του στον υπολογιστή σας
- √ το παράνομο λογισμικό μπορεί να είναι μολυσμένο με κα-

κόβουλο λογισμικό (π.χ. spyware)
- √ το παράνομο λογισμικό συνήθως δεν ενημερώνεται με διορθωτικές εκδόσεις για την αντιμετώπιση ευπαθειών και έτσι είναι ευάλωτο σε επιθέσεις εισβολέων
- √ δεν παρέχεται τεχνική υποστήριξη
- √ δεν παρέχονται εγχειρίδια χρήσης.

Ερωτήσεις - Δραστηριότητες

1. Γιατί πρέπει να αξιολογούμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο;
2. Τι προβλήματα μπορεί να μας δημιουργήσει η εγκατάσταση πειρατικού λογισμικού στον υπολογιστή μας;

16.4 Ιδιωτικότητα και προσωπικά δεδομένα στο Διαδίκτυο

Προσωπικά δεδομένα

Προσωπικά δεδομένα είναι και η διεύθυνση του ηλεκτρονικού μας ταχυδρομείου καθώς και οι κωδικοί πρόσβασης που χρησιμοποιούμε για την πρόσβασή μας σε υπηρεσίες του Διαδικτύου.

Ένα σημαντικό θέμα που πρέπει να έχουν υπόψη τους οι χρήστες και οι διαχειριστές των υπηρεσιών του Διαδικτύου είναι η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Η προστασία αυτή αποτελεί θεμελιώδες ανθρώπινο δικαίωμα και ρυθμίζεται από σχετική νομοθεσία. Η ιδιωτική μας ζωή είναι πολύτιμη και τη διατηρούμε υπό έλεγχο στο Διαδίκτυο μόνο με συνετή, προσεκτική και ελεγχόμενη χρήση των προσωπικών μας δεδομένων. Πρέπει να επιλέγουμε ποιες πληροφορίες κρατάμε για τον εαυτό μας και ποιες δίνουμε στους άλλους.

Ως προσωπικά δεδομένα μπορούμε να ορίσουμε τις πληροφορίες που μας χαρακτηρίζουν, όπως για παράδειγμα το όνομά μας, η διεύθυνσή μας, το τηλέφωνό μας, οι φωτογραφίες μας, τα ενδιαφέροντά μας, οι απόψεις μας κ.ά. Τα προσωπικά δεδομένα αφορούν και σε άλλα, ιδιαίτερα ευαίσθητα, στοιχεία της ιδιωτικής μας ζωής, όπως το θρήσκευμά μας, οι πολιτικές μας πεποιθήσεις ή η κατάσταση της υγείας μας.

Εικόνα 16.10. Για αναλυτικές πληροφορίες επισκεφθείτε τον ιστότοπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα http://www.dpa.gr/

Αρκετές δραστηριότητες στο Διαδίκτυο βασίζονται στην επεξεργασία των προσωπικών μας δεδομένων, για παράδειγμα:

- √ εγγραφή σε ένα διαδικτυακό κατάστημα
- √ εγγραφή σε ένα διαδικτυακό παιχνίδι
- √ συμμετοχή σε έναν διαγωνισμό
- √ δημιουργία προφίλ σε μια υπηρεσία κοινωνικής δικτύωσης

Έχετε αναρωτηθεί για την πιθανότητα τα προσωπικά μας δεδομένα να πέσουν σε λάθος χέρια; Στην περίπτωση αυτή είναι δυνατό να χρησιμοποιηθούν για δυσφήμιση, παρενόχληση και σε ακραίες περιπτώσεις για υποκλοπή ταυτότητας με δυσάρεστες συνέπειες.

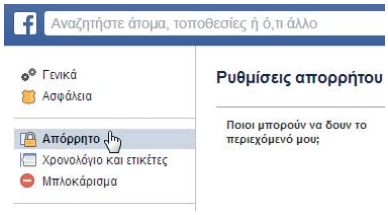
Ως βασικός κανόνας ισχύει ότι, για να χρησιμοποιήσει κάποιος τα προσωπικά μας δεδομένα για έναν συγκεκριμένο σκοπό, πρέπει να έχει εξασφαλίσει τη συγκατάθεσή μας. Πρέπει να γνωρίζουμε την ακριβή ταυτότητά του, τον σκοπό για τον οποίο τα χρειάζεται και ποιος θα έχει πρόσβαση σε αυτά.

Προστασία προσωπικών δεδομένων

Για να διατηρήσουμε προστατευμένα τα προσωπικά μας δεδομένα, καλό είναι να ακολουθούμε τις παρακάτω συμβουλές:

- √ να είμαστε γενικά φειδωλοί με τη δημοσιοποίηση προσωπικών μας δεδομένων σε ιστότοπους και σε υπηρεσίες κοινωνικής δικτύωσης. Κάθε στοιχείο που «ανεβάζουμε» στο Διαδίκτυο είναι δυνατό να υποπέσει στην αντίληψη οποιουδήποτε. Επιπρόσθετα, η δραστηριότητά μας στο Διαδίκτυο μπορεί να αφήσει ίχνη που δύσκολα σβήνουν, για παράδειγμα μια δημοσιοποιημένη φωτογραφία μας δύσκολα «κατεβαίνει».
- √ να αποφεύγουμε την εγγραφή μας σε άγνωστους και αμφιβόλου σκοπού ιστότοπους. Πρέπει να διαβάζουμε την πολιτική απορρήτου (privacy policy) των ιστοσελίδων που επισκεπτόμαστε, ώστε να ενημερωνόμαστε για το πώς θα χρησιμοποιήσουν τα προσωπικά μας δεδομένα και για το αν εγκαθιστούν cookies στον υπολογιστή μας.
- √ να χρησιμοποιούμε ψευδώνυμο στα chat rooms και να μην αποκαλύπτουμε ποτέ προσωπικά δεδομένα στους συνομιλητές μας.
- √ να επιλέγουμε «ισχυρούς» κωδικούς πρόσβασης (passwords) για τη σύνδεσή μας σε υπηρεσίες του Διαδικτύου.
- √ να έχουμε εγκατεστημένο λογισμικό ασφαλείας στον υπολογιστή μας, μια και το κακόβουλο λογισμικό μπορεί να υποκλέψει προσωπικά μας δεδομένα.

Τα **cookies** είναι μικρά αρχεία με πληροφορίες που μια ιστοσελίδα αποθηκεύει στον υπολογιστή ενός χρήστη, ώστε κάθε φορά που ο χρήστης συνδέεται στην ιστοσελίδα, η τελευταία να ανακτά τις εν λόγω πληροφορίες και να προσφέρει στον χρήστη σχετικές με αυτές υπηρεσίες.



Εικόνα 16.11. Ρυθμίσεις απορρήτου στο Facebook

Ερωτήσεις - Δραστηριότητες

1. Με χρήση μιας μηχανής αναζήτησης αναζητήστε πληροφορίες για τον εαυτό σας.
2. Τι προσωπικά σας δεδομένα έχετε δώσει κατά καιρούς σε διάφορους ιστότοπους;
3. Γιατί είναι σημαντικό να προστατεύουμε την ιδιωτική μας ζωή στο διαδίκτυο; Πώς μπορούμε να το πετύχουμε;
4. Επισκεφθείτε έναν γνωστό σας ιστότοπο και διαβάστε την πολιτική απορρήτου που ακολουθεί.