



Κεφάλαιο 16

Ασφάλεια και Προστασία στο Διαδίκτυο

16.1 Ασφάλεια υπολογιστικού συστήματος

Κακόβουλο λογισμικό: το λογισμικό το οποίο εκ προθέσεως διαθέτει τις απαιτούμενες εντολές για να βλάψει ένα υπολογιστικό σύστημα. Βασικότερα είδη:

- **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. Μειώνει την ταχύτητα σύνδεσης στο Διαδίκτυο, καταναλώνει τους πόρους (π.χ. μνήμη) του υπολογιστή κάνοντάς τον πιο αργό.
- **Δούρειος ίππος (Trojan horse):** πρόγραμμα μεταμφιεσμένο σε θεμιτό λογισμικό (π.χ. παιχνίδι, πρόγραμμα ανίχνευσης ιών) που αναλαμβάνει τον έλεγχο του μολυσμένου υπολογιστή. Μπορεί να διαγράψει αρχεία, να υποκλέψει προσωπικά δεδομένα (π.χ. κωδικούς πρόσβασης) ή να χρησιμοποιήσει τον υπολογιστή για επίθεση σε άλλους υπολογιστές.
- **Λογισμικό Κατασκοπίας (Spyware):** 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 (π.χ. ποιους ιστότοπους επισκέπτεται πιο συχνά) και την αποστέλλει σε τρίτους, κυρίως εταιρείες, με σκοπό την αποστολή στοχευμένων διαφημιστικών μηνυμάτων. Μπορεί να αλλάξει την αρχική σελίδα του φυλλομετρητή, να προσθέσει ανεπιθύμητες γραμμές εργαλείων σε αυτόν ή να εμφανίζει συνεχώς παράθυρα με ενοχλητικές διαφημίσεις.

16.1 Ασφάλεια υπολογιστικού συστήματος

Τρόποι προστασίας από κακόβουλο λογισμικό:

- 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.
- δεν 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).

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.

16.2 Θέματα ασφάλειας και προστασίας στο Διαδίκτυο

Ηλεκτρονικές συναλλαγές

Πλεονεκτήματα:

- 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.

Μειονεκτήματα:

- υπάρχουν σημαντικά θέματα ασφάλειας

Επιβλαβές περιεχόμενο

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.

Κίνδυνοι από τα **ηλεκτρονικά παιχνίδια** πολλών χρηστών που παίζονται μέσω του **Διαδικτύου**.

- προβλήματα που απορρέουν από την υπερβολική ενασχόληση με τα παιχνίδια αυτά,
- έκθεση των παιδιών σε ακατάλληλο περιεχόμενο (π.χ. βίαιες σκηνές).

16.2 Θέματα ασφάλειας και προστασίας στο Διαδίκτυο

Επιβλαβή ή ανεπιθύμητα μηνύματα **e-mail**

- μετάδοση ιών: μέσω μολυσμένων συνημμένων αρχείων.
- ηλεκτρονικό ψάρεμα (phishing): παραπλέμπει 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.

Αξιολόγηση πληροφοριών - συμβουλές

- 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

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. (<http://opi.gr/>)

Πειρατεία λογισμικού

- παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών λογισμικού,
- είναι πιθανό να χάσετε αρχεία ή δεδομένα με την εγκατάστασή του στον υπολογιστή σας
- μπορεί να είναι μολυσμένο με κακόβουλο λογισμικό (π.χ. spyware)
- συνήθως δεν ενημερώνεται με νέες εκδόσεις και έτσι είναι ευάλωτο σε επιθέσεις εισβολέων
- δεν παρέχεται τεχνική υποστήριξη
- δεν παρέχονται εγχειρίδια χρήσης

Προσωπικά δεδομένα

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, το θρήσκευμά μας, οι πολιτικές μας πεποιθήσεις, η κατάσταση της υγείας μας κ.ά.

Δραστηριότητες στο Διαδίκτυο που βασίζονται στην επεξεργασία των προσωπικών μας δεδομένων:

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

Προστασία προσωπικών δεδομένων – συμβουλές (<http://www.dpa.gr/>):

- να είμαστε γενικά φειδωλοί με τη δημοσιοποίηση προσωπικών μας δεδομένων. Η δραστηριότητά μας στο Διαδίκτυο μπορεί να αφήσει ίχνη που δύσκολα σβήνουν
- να αποφεύγουμε την εγγραφή μας σε άγνωστους και αμφιβόλου σκοπού ιστότοπους.
- 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.