ΙΟΙ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ο **ιός** του υπολογιστή είναι ένα κομμάτι προγράμματος, το οποίο αντιγράφει τον εαυτό του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου. Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλο τον κόσμο. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό. Σε περίπτωση που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταρρέουν αρχεία εταιρειών, πανεπιστημίων, ακόμα και κυβερνήσεων.

Δούρειοι Ίπποι (Trojan horses)

Πρόκειται για ένα είδος προγράμματος, το οποίο δεν αναπαράγεται και δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του. Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σα να ήταν το αυθεντικό. Όταν ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα χρησιμοποιεί την έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά.

Σκουλήκια (Worms)

Πρόκειται για προγράμματα υπολογιστών τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ. Χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, irc chat κ.ά.). Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα του λογισμικού των υπολογιστών. Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.

Βασικές αρχές προστασίας από ιούς

1. Αντιικό λογισμικό: επιτρέπει την προστασία του χρήστη από το σύνολο σχεδόν των ιών. Ωστόσο, δεν αποτελεί πανάκεια στο πρόβλημα. Με σκοπό την βέλτιστη χρήση του αντιικού λογισμικού θα πρέπει να τηρούνται τα εξής:

- **Τακτική ενημέρωση του λογισμικού:** Καινούριοι ιοί εμφανίζονται επί καθημερινής βάσεως. Το αντιικό λογισμικό γενικά μπορεί να προστατεύσει το χρήστη μόνο από τους ιούς που περιέχονται στη βάση δεδομένων του. Τα περισσότερα σύγχρονα αντιικά λογισμικά ενσωματώνουν για το σκοπό αυτό μηχανισμούς αναβάθμισης της βάσης αυτής, ώστε να έχουν τη δυνατότητα να αντιμετωπίσουν το σύνολο των υπαρχόντων ιών.
- **Συνεχής ενεργοποίηση του λογισμικού:** Τα περισσότερα σύγχρονα αντιικά λογισμικά ενσωματώνουν προγράμματα τα οποία συνεχώς ελέγχουν κάθε αρχείο ή μήνυμα ηλεκτρονικής αλληλογραφίας που ανακτά ο χρήστης, ώστε να εντοπίζουν τον ιό πριν αυτός εκτελεστεί και προσβάλλει το υπολογιστικό σύστημα. Είναι σημαντικό ο χρήστης να μην κλείνει τα προγράμματα αυτά, για οποιοδήποτε λόγο.

2. Τακτική ενημέρωση του λειτουργικού συστήματος: μπορεί να πραγματοποιείται αυτόματα. Η ενημέρωση (update) ελέγχει το λειτουργικό του υπολογιστή σας, καθώς και άλλο λογισμικό, και φροντίζει για την απόκτηση όλων των ενημερωμένων εκδόσεων και κρίσιμων αναβαθμίσεων που χρειάζονται.

3. Προσοχή στα μηνύματα με επισυναπτόμενα: είναι σημαντικό να αποφεύγει κανείς το άνοιγμα αρχείων ή εγγράφων που παραλαμβάνει από γνωστούς ή αγνώστους αποστολείς, είτε μέσω ηλεκτρονικής αλληλογραφίας είτε μέσω άλλων μέσων. Ακόμα και αν ο αποστολέας είναι γνωστός, ελέγξτε προσεκτικά το περιεχόμενο του μηνύματος και αν το θέμα του είναι σχετικό με αυτό που συνήθως συζητάτε. Σε αντίθετη περίπτωση, και ιδίως όταν το μήνυμα περιέχει επισυναπτόμενο, αποφύγετε το άνοιγμα του επισυναπτομένου αρχείου. Ιδιαίτερη προσοχή πρέπει να δίνεται σε μηνύματα που σας προτρέπουν να ανοίξετε κάποιο επισυναπτόμενο και ισχυρίζονται πως προέρχονται από την ομάδα υποστήριξης κάποιου φορέα, τράπεζας, κ.λπ.

4. Εγκατάσταση τείχους προστασίας: η εγκατάσταση και ενεργοποίηση λογισμικού τείχους προστασίας επιτρέπει την προστασία του χρήστη από προβλήματα ασφαλείας του λειτουργικού συστήματος για τα οποία δεν υπάρχει διαθέσιμη ακόμα κάποια κρίσιμη ενημέρωση.

5. Τακτική λήψη αντιγράφων ασφαλείας: σε περίπτωση που ένας ιός, ή οποιοσδήποτε άλλος παράγοντας, προκαλέσει ανεπανόρθωτη καταστροφή στα δεδομένα του χρήστη, η διαθεσιμότητα έγκυρων αντιγράφων ασφαλείας είναι ο μόνος τρόπος επαναφοράς τους.

URLs:
http://www.sch.gr
http://www.besafeonline.org/English/computer_viruses.htm