ΚΕΦΑΛΑΙΟ 16

Ασφάλεια και προστασία στο Διαδίκτυο

Ασφάλεια υπολογιστικού συστήματος

Κακόβουλο λογισμικό

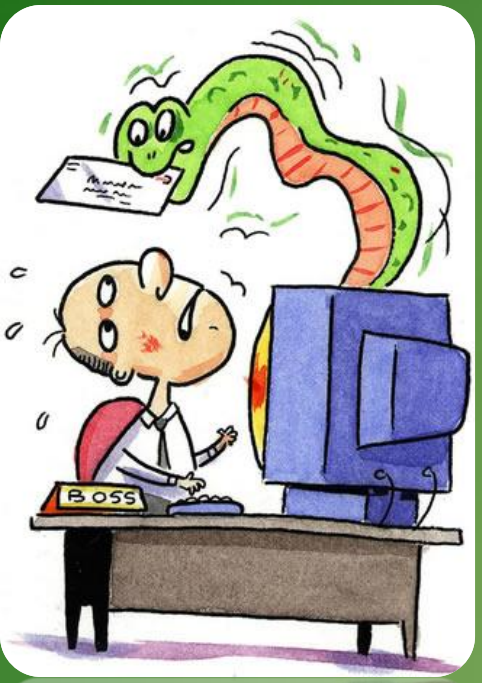
λογισμικό το οποίο εκ προθέσεως διαθέτει τις απαιτούμενες εντολές για να βλάψει ένα υπολογιστικό σύστημα.

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).

- προσκολλάται σε κάποιο πρόγραμμα ή αρχείο και ενεργοποιείται συνήθως μόλις προσπαθήσουμε να τρέξουμε το πρόγραμμα ή να ανοίξουμε το αρχείο.

- 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.
- δε χρειάζεται κάποιο άλλο πρόγραμμα ως όχημα για τη διακίνησή του.
- 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.
- δεν αναπαράγει και δε διαδίδει τον εαυτό του

Λογισμικό Κατασκοπίας (Spyware)

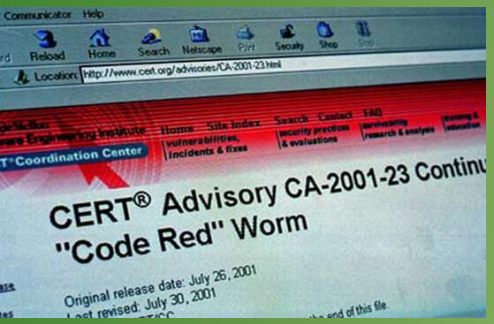
- κακόβουλο πρόγραμμα που προσκολλάται κρυφά σε αρχεία που κατεβάζουμε από το Διαδίκτυο ή κατεβαίνει και εγκαθίσταται αυτόματα σε έναν υπολογιστή κατά την επίσκεψή μας σε μολυσμένες ιστοσελίδες.

- 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.

- μπορεί να αλλάξει την αρχική σελίδα του φυλλομετρητή, να προσθέσει ανεπιθύμητες γραμμές εργαλείων σε αυτόν ή να εμφανίζει συνεχώς παράθυρα με ενοχλητικές διαφημίσεις.

Για την ιστορία…

Ο ιός **I Love You,** ο οποίος έκανε την εμφάνισή του στις 4 Μαΐου 2000, περιείχε ένα κομμάτι κώδικα ως συνημμένο. Οι χρήστες που έκαναν διπλό κλικ στο συνημμένο, επέτρεπαν στον ιό να εκτελεσθεί. Ο κώδικας έστελνε αντίγραφα του εαυτού του σ' όσους βρίσκονταν στο βιβλίο διευθύνσεων του θύματος και μετά άρχιζε να καταστρέφει αρχεία στον υπολογιστή του. Ο ιός προκάλεσε συνολική ζημία της τάξης των 10 δις $ και επηρέασε σχεδόν το 10% των υπολογιστών στον κόσμο.



Το σκουλήκι **Code Red** που αναπαρήγαγε τον εαυτό του πάνω από 250.000 φορές σε εννέα ώρες στις 19 Ιουλίου 2001. Δεν απαιτούσε από εσάς να ανοίξετε ένα συνημμένο ηλεκτρονικό ταχυδρομείο ή να εκτελέσετε ένα αρχείο, απαιτούσε μόνο μια ενεργή σύνδεση στο Internet με την οποία κατέστρεφε την ιστοσελίδα που ανοίξατε εμφανίζοντας ένα κείμενο "Hacked από τους Κινέζους!" Και μέσα σε λιγότερο από μία εβδομάδα, ο "Code Red" έριξε πάνω από 400.000 servers, συμπεριλαμβανομένου εκείνου του Λευκού Οίκου. Προκάλεσε συνολική ζημία ύψους περίπου 2,6 δις $ δολάρια καθώς επηρέασε ένα εκατομμύριο υπολογιστές.

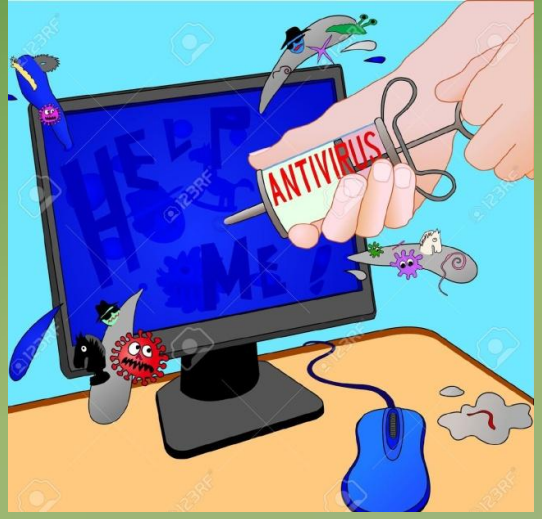
Τρόποι προστασίας από κακόβουλο λογισμικό

- √ 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).

Το λογισμικό προστασίας από ιούς (antivirus) πρέπει να ενημερώνεται τακτικά με πρόσφατους ορισμούς ιών (virus definitions).

Κρατάμε σε τακτά χρονικά διαστήματα αντίγραφα ασφαλείας των αρχείων μας..!!!!!!

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 προ- γράμματα ασφαλείας (οικογένεια προγραμμάτων, με ονομασία όπως Internet Security).

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

Θέματα ασφάλειας και προστασίας στο Διαδίκτυο

Ηλεκτρονικές συναλλαγές

Όταν επισκεπτόμαστε έναν ιστότοπο για ηλεκτρονική συναλλαγή, θα πρέπει αρχικά να ελέγχουμε, όσο είναι αυτό εφικτό, την αξιοπιστία του. Θα πρέπει να υπάρχουν:

- ξεκάθαρος προσδιορισμός του φορέα (δημόσιου ή ιδιωτικού) με το όνομά του, την ιδιότητά του και τα στοιχεία επικοινωνίας του.
- αναλυτικές πληροφορίες για τους όρους χρήσης και ασφάλειας σε ιστότοπους επιχειρήσεων (όροι χρήσης, ασφάλεια συναλλαγών, προσωπικά δεδομένα (πολιτική απορρήτου), διαδικασία υποβολής παραγγελίας, τρόποι πληρωμής και αποστολής, πολιτική επιστροφών)

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 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, οπότε δεν γίνεται πάντα έλεγχος του περιεχομένου των ιστοσελίδων. Το περιεχόμενο μπορεί να είναι παράνομο (περιέχουν προτροπές σε παράνομες πράξεις, οικονομικές απάτες, υλικό εκφοβισμού, συκοφαντική δυσφήμιση, παραβίαση προσωπικών δεδομένων και πνευματικής ιδιοκτησίας, υλικό παιδικής πορνογραφίας κ.ά) και συνάμα επιβλαβές για τα παιδιά, σε άλλες όμως περιπτώσεις νόμιμο αλλά ακατάλληλο για μικρές ηλικίες. Ιδιαίτερη περίπτωση αποτελούν τα ηλεκτρονικά παιχνίδια πολλών χρηστών που παίζονται μέσω του Διαδικτύου.

Επιβάλλεται η χρήση λογισμικού γονικού έλεγχου ή φιλτραρίσματος

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.

safeLine

PEGI Pan European Game Information

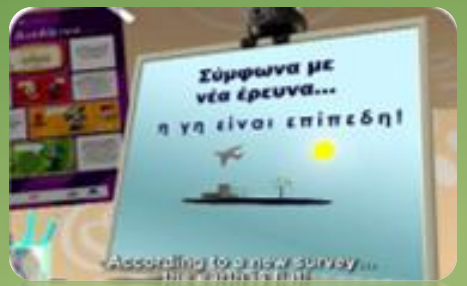
3 7 12 16 18

Επιβλαβή ή ανεπιθύμητα μηνύματα e-mail

- 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. Και 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.

- Η προστασία των ανήλικων χρηστών του Διαδικτύου από ακατάλληλο ή επιβλαβές για αυτούς περιεχόμενο, ή από ακατάλληλη ή επιβλαβή συμπεριφορά.
- Η ενημέρωση των γονέων για τους τρόπους με τους οποίους μπορούν να προστατευθούν αλλά και να προστατεύσουν αποτελεσματικά τα παιδιά τους από τους κινδύνους που εγκυμονούν από τη μη ορθή χρήση των διαδραστικών τεχνολογιών, όπως είναι το Διαδίκτυο ή το κινητό τηλέφωνο.
- Η προώθηση των θετικών πλευρών των διαδραστικών τεχνολογιών, ως εργαλεία της καθημερινής μας ζωής.
- Η εκπαίδευση των εκπαιδευτικών για την ασφαλή χρήση του Διαδικτύου και του κινητού τηλεφώνου, ενημερώνοντας τόσο για τα πολλαπλά οφέλη όσο και για τους πιθανούς κινδύνους, με στόχο τη δημιουργία πολλαπλασιαστικής δράσης μέσα στην τάξη.

Αξιολόγηση πληροφοριών



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.)

- ✓ **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

ΟΡΓΑΝΙΣΜΟΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ
ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ
HELLENIC COPYRIGHT ORGANIZATION
MINISTRY OF CULTURE

Πνευματικό δικαίωμα (copyright) είναι 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.

- η παραβίασή τους θεωρείται άδικη και παράνομη πράξη, και τιμωρείται.
- είναι δύσκολο να αντιμετωπιστεί λόγω της έκτασης και της πολυπλοκότητας του Διαδικτύου.
- αν θέλουμε να χρησιμοποιήσουμε σε εργασία μας υλικό από το Διαδίκτυο, καλό είναι να αναφέρουμε τις πηγές μας.
- ο καθένας προσωπικά θα πρέπει να σέβεται τους δημιουργούς πνευματικών έργων και να δρα έντιμα και ηθικά.

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

⇨ peer to peer networks

Εκτός από την παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών λογισμικού, το παράνομο λογισμικό είναι πιθανό να βλάψει σοβαρά τον υπολογιστή σας (να χάσετε αρχεία ή δεδομένα με την εγκατάστασή του στον υπολογιστή σας, μπορεί να είναι μολυσμένο με κακόβουλο λογισμικό (π.χ. spyware), το παράνομο λογισμικό συνήθως δεν ενημερώνεται με διορθωτικές εκδόσεις για την αντιμετώπιση ευπαθειών και έτσι είναι ευάλωτο σε επιθέσεις εισβολές, δεν παρέχεται τεχνική υποστήριξη, δεν παρέχονται εγχειρίδια χρήσης.

Ιδιωτικότητα και προσωπικά δεδομένα στο Διαδίκτυο

Προσωπικά δεδομένα

Αφορούν στις πληροφορίες που μας χαρακτηρίζουν, όπως:

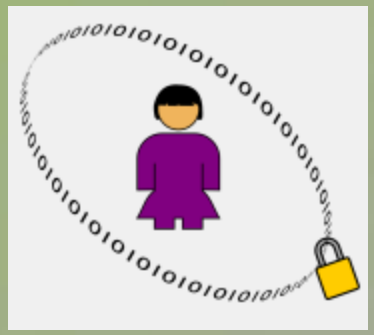
- όνομα, διεύθυνση, τηλέφωνο, φωτογραφίες, ενδιαφέροντα, απόψεις κ.ά.
- διεύθυνση του ηλεκτρονικού ταχυδρομείου καθώς και κωδικοί πρόσβασης που χρησιμοποιούμε.
- θρήσκευμα, πολιτικές πεποιθήσεις ή κατάσταση της υγείας μας.

≈ εγγραφή σε ένα διαδικτυακό κατάστημα

≈ εγγραφή σε ένα διαδικτυακό παιχνίδι

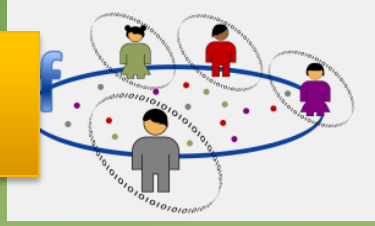
≈ συμμετοχή σε έναν διαγωνισμό

≈ δημιουργία προφίλ σε μια υπηρεσία κοινωνικής δικτύωσης



Αν πέσουν σε λάθος χέρια μπορεί να χρησιμοποιηθούν για δυσφήμιση, παρενόχληση και σε ακραίες περιπτώσεις για υποκλοπή ταυτότητας με δυσάρεστες συνέπειες.

Προστασία προσωπικών δεδομένων



28 ΙΑΝΟΥΑΡΙΟΥ: ΠΑΓΚΟΣΜΙΑ ΗΜΕΡΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- να είμαστε γενικά φειδωλοί με τη δημοσιοποίηση προσωπικών μας δεδομένων σε ιστότοπους και σε υπηρεσίες κοινωνικής δικτύωσης. 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.
- 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.

*** 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**