Discovering Computers Enhanced Edition ©2017

Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Security, Ethics, and Privacy

Γιατί μιλάμε για την ασφάλεια;

- Κακόβουλο λογισμικό (botnets, trojans, rootkits),….
- Παράνομη εισβολή σε συστήματα, (Hacking, cracking…),
- Μη εξουσιοδοτημένη πρόσβαση σε πληροφορία (read, write)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DOS, DDOS).
- Επιθέσεις Πλαστοπροσωπίας (Spoofing / Masquerading), Κλοπή Ταυτότητας (Identity Theft)
- Υποκλοπές Επικοινωνιών, Πρόσβαση σε προσωπικά δεδομένα
- Μη ζητηθείσα επικοινωνία (spam), «Ηλ. Ψάρεμα» (Phishing)
- Ηλεκτρονικό έγκλημα (cyber-crime), παιδική πορνογραφία,…
- Παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας
- …

Ασφάλεια – Ορισμοί

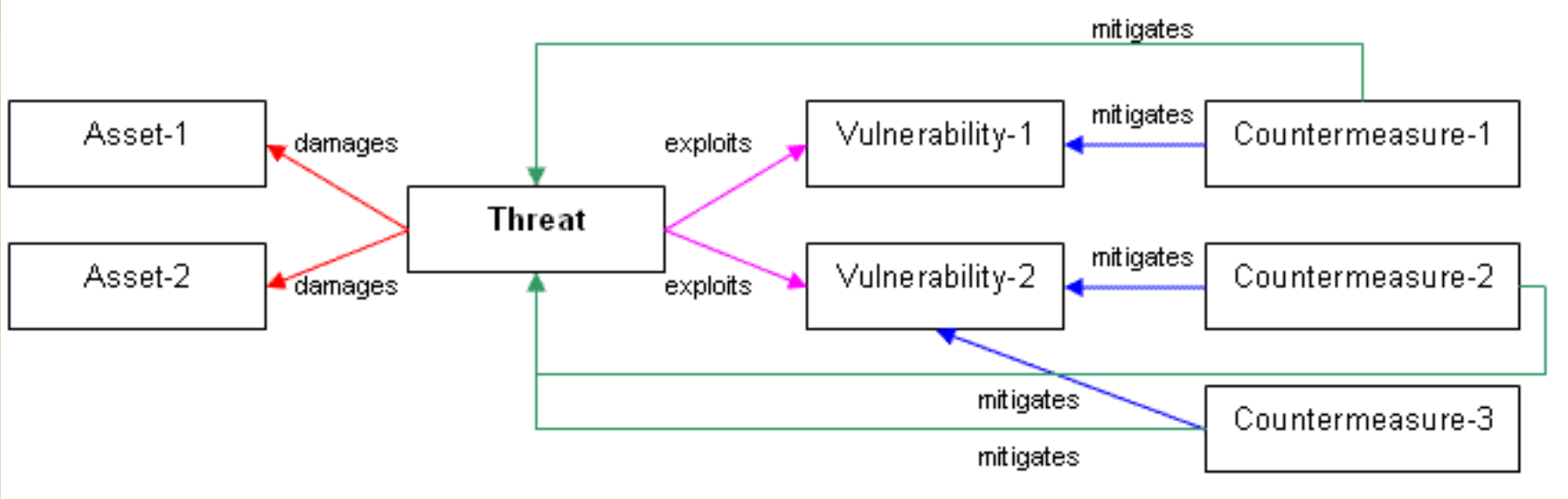
- Security: (Oxford Dictionary)
  - Freedom from danger or anxiety
- Ασφάλεια: (Μπαμπινιώτης)
  - Η κατάσταση στην οποία … αισθάνεται κανείς ότι δεν απειλείται.
  - Η αποτροπή κινδύνου ή απειλής…
- Ασφάλεια (Security) & Ασφάλεια (Safety)
  - Security: Προστασία έναντι εχθρού
  - Safety: Προστασία έναντι σφαλμάτων, λαθών, ατυχημάτων, παραλείψεων

Γιατί είναι σημαντική η ασφάλεια των ΠΣ???

- Γιατί τα πληροφοριακά συστήματα είναι ευπαθή σε καταστροφή, σφάλματα και κακή χρήση;
- Ποια είναι η επιχειρηματική αξία της ασφάλειας και του ελέγχου;
- Ποια είναι τα συστατικά στοιχεία ενός οργανωσιακού πλαισίου δράσης για την ασφάλεια και τον έλεγχο;

Τι σημαίνει «Ασφαλές Σύστημα»;

Θεώρηση από τη σκοπιά της «Ανάλυσης και Διαχείρισης Κινδύνων»



http://www.ptatechnologies.com/PTA3.htm

Κίνδυνοι ψηφιακής ασφάλειας

- **Κίνδυνος ψηφιακής ασφάλειας (digital security risk)** είναι οποιοδήποτε συμβάν ή ενέργεια που θα μπορούσε να προκαλέσει απώλεια ή ζημιά σε υλικό, λογισμικό, δεδομένα, πληροφορίες ή δυνατότητες επεξεργασίας υπολογιστή ή κινητής συσκευής
- Κάθε παράνομη πράξη που συνεπάγεται τη χρήση υπολογιστή ή συναφών συσκευών αναφέρεται γενικά ως έγκλημα στον υπολογιστή.
- Το έγκλημα στον κυβερνοχώρο (**cybercrime**)είναι μια διαδικτυακή ή διαδικτυακή παράνομη πράξη

Κίνδυνοι ψηφιακής ασφάλειας

Page 213
Figure 5-1

Κίνδυνοι ψηφιακής ασφάλειας

Hacker

Cracker

Script kiddie

Επιχειρηματικοί κατάσκοποι

Corporate spies

Ανήθικοι εργαζόμενοι
Unethical employees

Κυβερνοεκβιαστής
Cyberextortionist

Κυβερνοτρομοκράτης
Cyberterrorist

Ενδεικτικός Πίνακας Απειλών

	Απειλή
1.	Πλαστοπροσωπία Χρήστη από κακόβουλους Εσωτερικούς Χρήστες
2.	Πλαστοπροσωπία Χρήστη από κακόβουλους Συνεργάτες
3.	Πλαστοπροσωπία Χρήστη από κακόβουλους Εξωτερικούς Χρήστες
4.	Μη εξουσιοδοτημένη χρήση Εφαρμογής
5.	Παρακολούθηση Επικοινωνίας
6.	Παραποίηση Επικοινωνίας
7.	Αποποίηση πράξης από Χρήστη
8.	Αποτυχία Επικοινωνίας
9.	Είσοδος κακόβουλου κώδικα (virus, Trojan, spam, hoaxes κτλ)
10.	Τυχαίο λάθος δρομολόγησης επικοινωνίας
11.	Εσκεμμένη τροποποίηση δρομολόγησης επικοινωνίας
12.	Λανθασμένη χρήση συστήματος
13.	Τεχνική βλάβη υπολογιστή
14.	Βλάβη κλιματισμού
15.	Βλάβη λογισμικού συστήματος
16.	Βλάβη λογισμικού διαχείρισης δικτύου
17.	Λάθος διαχείρισης συστήματος ή δικτύου
18.	Λάθος συντήρησης υλικού (hardware)
19.	Λάθος συντήρησης λογισμικού (software)
20.	Έλλειψη προσωπικού
21.	Τεχνική βλάβη εγκατάστασης (παροχή ρεύματος, τηλεφώνου κτλ)
22.	Τεχνική βλάβη εκτυπωτών
23.	Τεχνική βλάβη δικτυακού εξοπλισμού (hub, router, switch κτλ)
24.	Τεχνική βλάβη Gateway
25.	Τεχνική βλάβη συστήματος ελέγχου πρόσβασης (firewall)
26.	Τεχνική βλάβη συστήματος εντοπισμού εισβολών (IDS)
27.	Τεχνική βλάβη υπολογιστή διαχείρισης δικτύου ή λειτουργιών
28.	Τεχνική βλάβη υπηρεσίας πρόσβασης διαδικτύου (Internet access)
29.	Τεχνική βλάβη άλλης δικτυακής υπηρεσίας (ftp, web mail κτλ)
30.	Τεχνική βλάβη υπηρεσίας e-mail
31.	Βλάβη λογισμικού εφαρμογών (application software)
32.	Λάθος χειρισμού δεδομένων

Επιθέσεις στο Διαδίκτυο και το δίκτυο

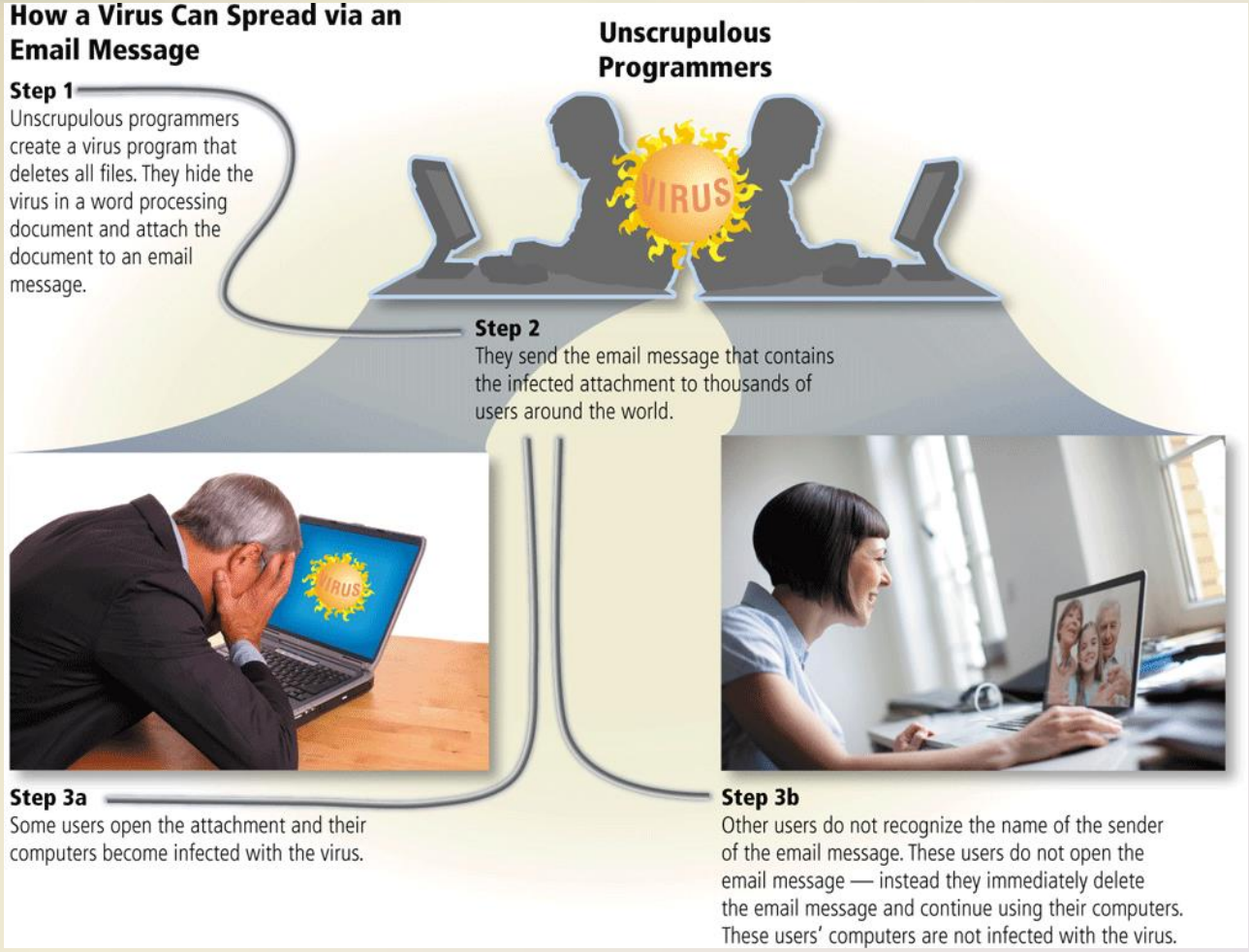
- Οι πληροφορίες που μεταδίδονται μέσω δικτύων έχουν υψηλότερο βαθμό κινδύνου για την ασφάλεια από τις πληροφορίες που διατηρούνται στις εγκαταστάσεις ενός οργανισμού
- Malware, σύντομη έφραση για κακόβουλο λογισμικό, αποτελείται από προγράμματα που ενεργούν χωρίς τη γνώση του χρήστη και να τροποποιήσει σκόπιμα τις λειτουργίες των υπολογιστών και κινητών συσκευών
-

Table 5-1 Common Types of Malware

Type	Description
Virus	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission.
Worm	A program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer, device, or network.
Trojan horse	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
Rootkit	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device.
Spyware	A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
Adware	A program that displays an online advertisement in a banner, pop-up window, or pop-under window on webpages, email messages, or other Internet services.

Page 215
Table 5-1

Επιθέσεις στο Διαδίκτυο και το δίκτυο



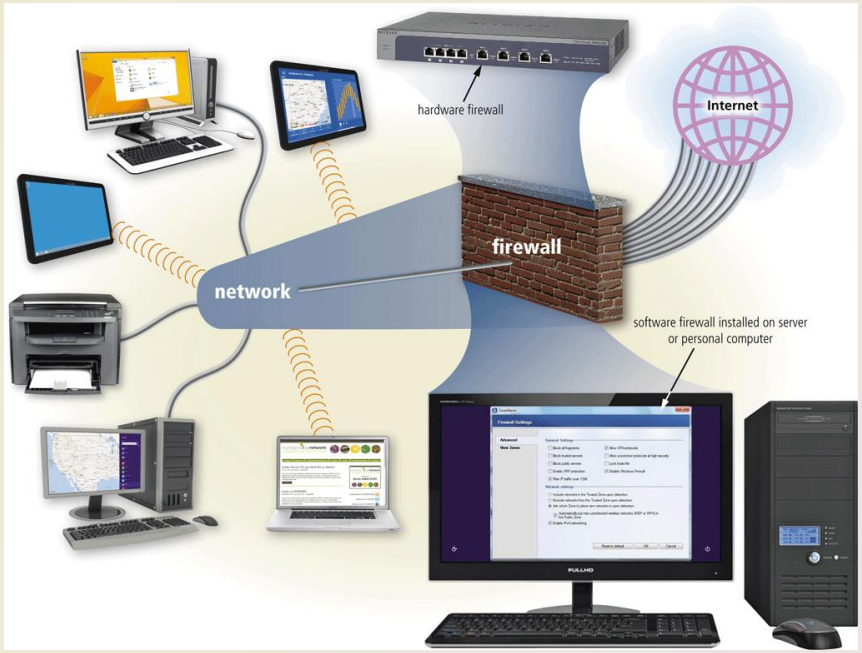
Page 215
Figure 5-2

Επιθέσεις στο Διαδίκτυο και το δίκτυο

- Ένα botnet είναι μια ομάδα υπολογιστών ή κινητών συσκευών που έχουν παραβιαστεί και είναι συνδεδεμένες σε ένα δίκτυο
- Ένας υπολογιστής ή μια συσκευή που έχει παραβιαστεί είναι γνωστή ως ζόμπι
- Μια επίθεση άρνησης υπηρεσίας (επίθεση DoS) διαταράσσει την πρόσβαση του υπολογιστή σε μια υπηρεσία Internet
- Κατανεμημένη επίθεση DoS (επίθεση DDoS)
- Η πίσω πόρτα (back door) είναι ένα πρόγραμμα ή ένα σύνολο οδηγιών σε ένα πρόγραμμα που επιτρέπουν στους χρήστες να παρακάμπτουν τα στοιχεία ελέγχου ασφαλείας
- Η πλαστογράφηση (spoofing) είναι μια τεχνική που χρησιμοποιούν οι εισβολείς για να κάνουν τη μετάδοση του δικτύου τους ή του Διαδικτύου να φαίνεται νόμιμη
-

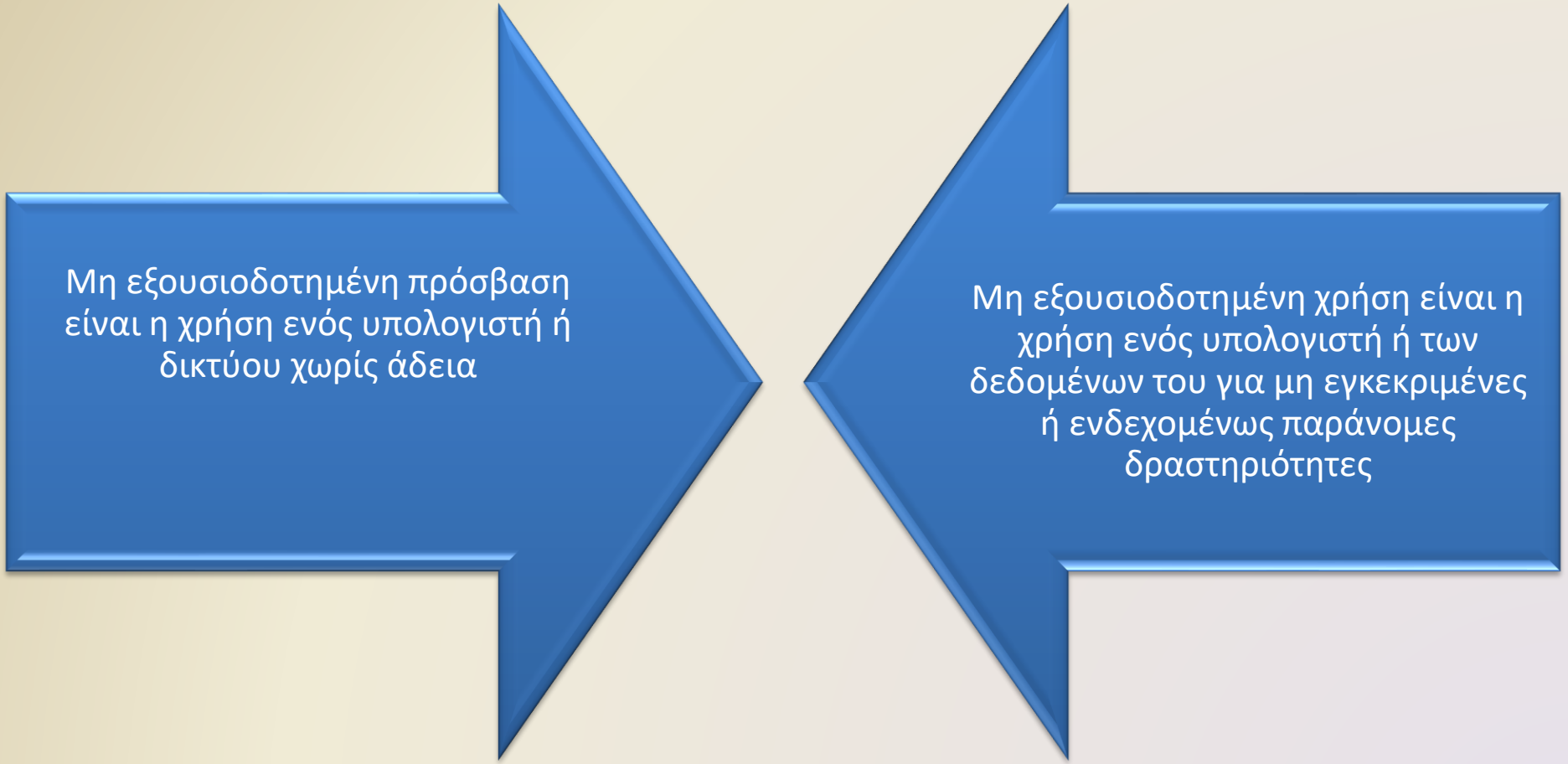
Επιθέσεις στο Διαδίκτυο και το δίκτυο

- Το τείχος προστασίας (firewall) είναι υλικό ή/και λογισμικό που προστατεύει τους πόρους ενός δικτύου από εισβολή
-



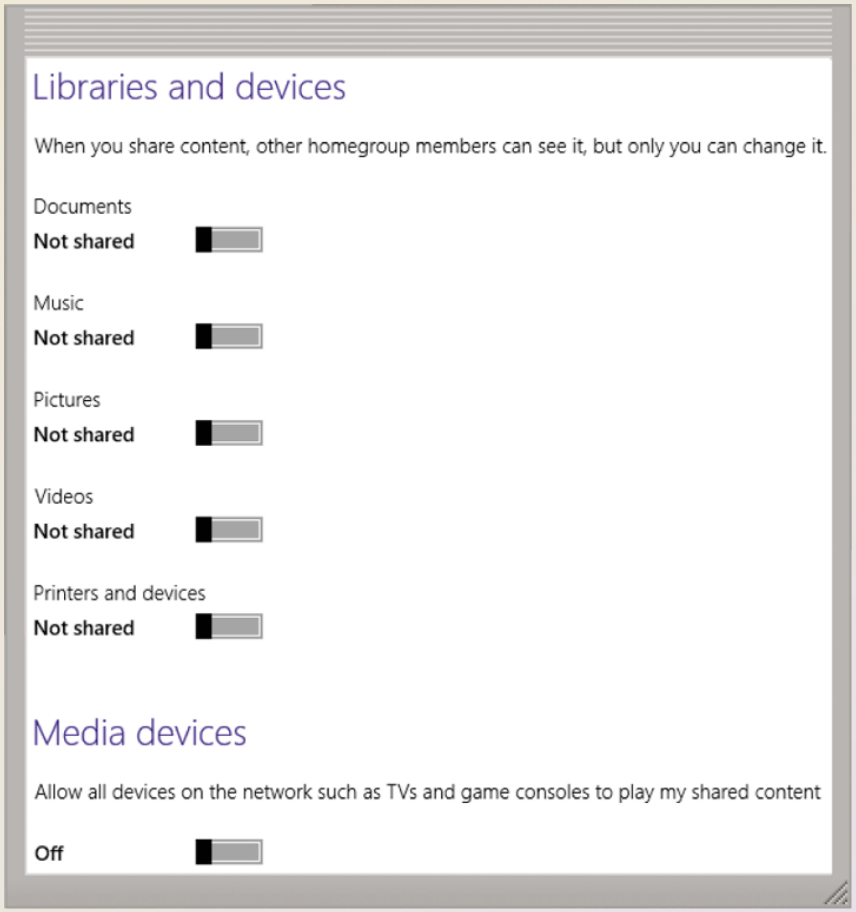
Pages 219 - 220
Figure 5-4

Μη εξουσιοδοτημένη πρόσβαση και χρήση



Μη εξουσιοδοτημένη πρόσβαση και χρήση

- Οι οργανισμοί λαμβάνουν διάφορα μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και χρήσης
- Πολιτική αποδεκτής χρήσης
- Απενεργοποίηση κοινής χρήσης αρχείων και εκτυπωτών



Page 221
Figure 5-5

Μη εξουσιοδοτημένη πρόσβαση και χρήση

- Τα στοιχεία ελέγχου της πρόσβασης καθορίζουν ποιος μπορεί να έχει πρόσβαση σε έναν υπολογιστή, μια συσκευή ή ένα δίκτυο, πότε μπορούν να έχουν πρόσβαση σε αυτό? και τι ενέργειες μπορούν να λάβουν κατά την πρόσβαση σε αυτό
- Ο υπολογιστής, η συσκευή ή το δίκτυο θα πρέπει να διατηρούν μια διαδρομή ελέγχου που καταγράφει σε ένα αρχείο τόσο επιτυχημένες όσο και ανεπιτυχείς προσπάθειες πρόσβασης
- Όνομα χρήστη
- Κωδικό πρόσβασης

Pages 222 - 223
Figure 5-6

Μη εξουσιοδοτημένη πρόσβαση και χρήση

- Μια φράση πρόσβασης (passphrase) είναι ένας ιδιωτικός συνδυασμός λέξεων, που συχνά περιέχει μεικτή κεφαλαία και σημεία στίξης, που σχετίζονται με ένα όνομα χρήστη που επιτρέπει την πρόσβαση σε ορισμένους πόρους του υπολογιστή
- Ένα PIN (προσωπικός αναγνωριστικός αριθμός), που μερικές φορές ονομάζεται κωδικός πρόσβασης, είναι ένας αριθμητικός κωδικός πρόσβασης, είτε εκχωρημένος από μια εταιρεία είτε επιλεγμένος από ένα χρήστη
- Ένα possessed object είναι οποιοδήποτε στοιχείο που πρέπει να έχετε ή να μεταφέρετε μαζί σας, προκειμένου να αποκτήσετε πρόσβαση σε έναν υπολογιστή ή μια εγκατάσταση υπολογιστή
- Μια βιομετρική συσκευή ελέγχει την ταυτότητα ενός ατόμου με τη μετάφραση ενός προσωπικού χαρακτηριστικού σε έναν ψηφιακό κώδικα που συγκρίνεται με έναν ψηφιακό κώδικα σε έναν υπολογιστή ή μια κινητή συσκευή που επαληθεύει ένα φυσικό ή συμπεριφοριστικό χαρακτηριστικό
-

Pages 223 - 224

Μη εξουσιοδοτημένη πρόσβαση και χρήση

Συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων

Σύστημα αναγνώρισης προσώπου

Σύστημα γεωμετρίας χεριών

Σύστημα φωνητικής επαλήθευσης

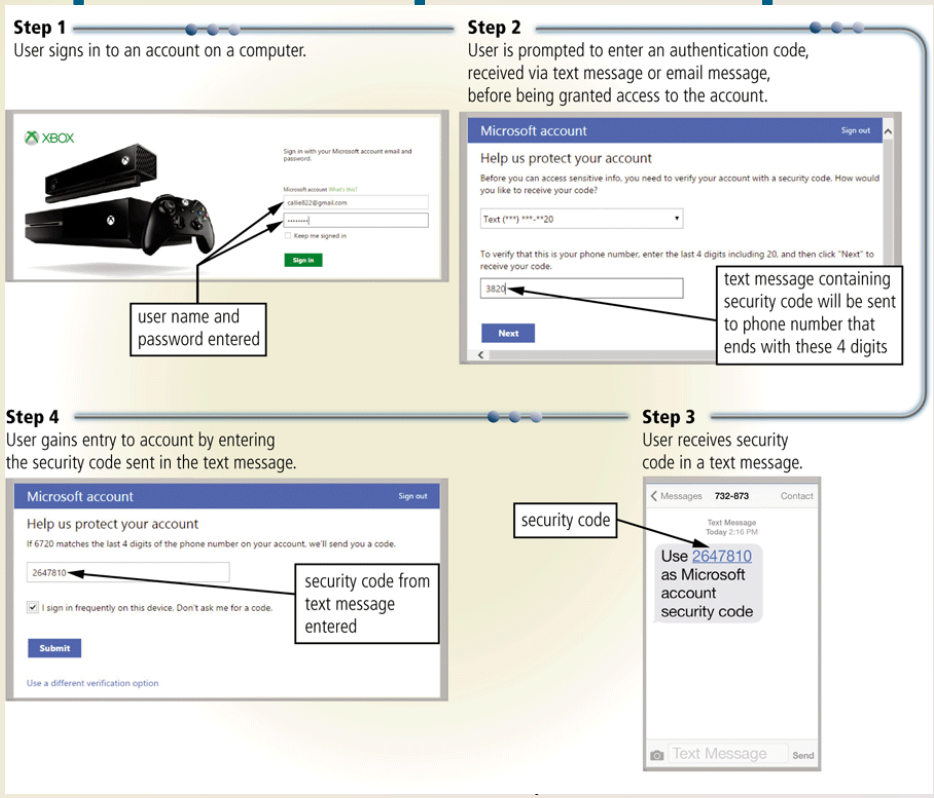
Σύστημα επαλήθευσης υπογραφής

Σύστημα αναγνώρισης ίριδας

Pages 224 – 226
Figures 5-8 – 5-11

Μη εξουσιοδοτημένη πρόσβαση και χρήση

- **Η επαλήθευση σε δύο βήματα χρησιμοποιεί δύο ξεχωριστές μεθόδους, η μία μετά την επόμενη, για να επαληθεύσει την ταυτότητα ενός χρήστη**



Pages 226 – 227
Figure 5-12

Μη εξουσιοδοτημένη πρόσβαση και χρήση

- **Ψηφιακή εγκληματολογία είναι η ανακάλυψη, συλλογή, και ανάλυση των αποδεικτικών στοιχείων που βρέθηκαν σε υπολογιστές και δίκτυα**
- Many areas use digital forensics

Κλοπή λογισμικού

- **Η κλοπή λογισμικού συμβαίνει όταν κάποιος:**
-

Κλέβει media λογισμικού

Διαγράφει σκόπιμα προγράμματα

Καταχωρήσεις ή/και ενεργοποιεί παράνομα ένα πρόγραμμα

Αντιγράφει παράνομα ένα πρόγραμμα

Κλοπή λογισμικού

- Πολλοί κατασκευαστές ενσωματώνουν μια διαδικασία ενεργοποίησης στα προγράμματά τους για να εξασφαλίσουν ότι το λογισμικό δεν είναι εγκατεστημένο σε περισσότερους υπολογιστές από ό, τι νόμιμα άδεια χρήσης
- Κατά τη διάρκεια της ενεργοποίησης του προϊόντος, η οποία διεξάγεται είτε ηλεκτρονικά είτε μέσω τηλεφώνου, οι χρήστες παρέχουν τον αναγνωριστικό αριθμό του προϊόντος λογισμικού για να συσχετίσουν το λογισμικό με τον υπολογιστή ή την κινητή συσκευή στην οποία είναι εγκατεστημένο το λογισμικό

Κλοπή λογισμικού

- Μια άδεια χρήσης είναι το δικαίωμα χρήσης λογισμικού

Typical Conditions of a Single-User License Agreement

You can…

- Install the software on only one computer or device. (Some license agreements allow users to install the software on a specified number of computers and/or mobile devices.)
- Make one copy of the software as a backup.
- Give or sell the software to another individual, but only if the software is removed from the user's computer first.

You cannot…

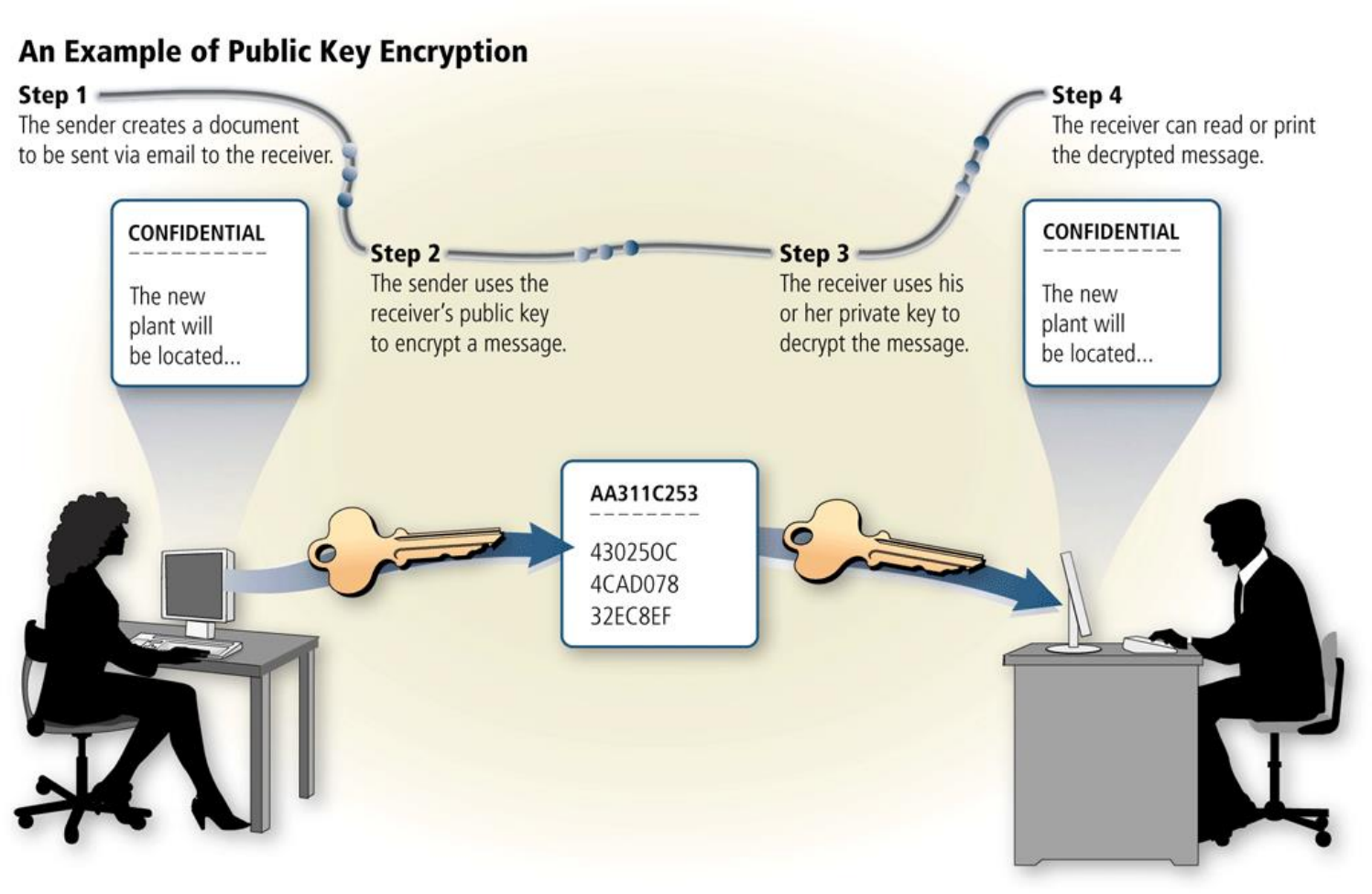
- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues, while continuing to use the software.
- Export the software.
- Rent or lease the software.

Pages 228 – 229
Figure 5-13

Κλοπή Πληροφοριών

- Κλοπή πληροφοριών συμβαίνει όταν κάποιος κλέβει προσωπικές ή εμπιστευτικές πληροφορίες
- Η κρυπτογράφηση είναι μια διαδικασία μετατροπής δεδομένων που είναι αναγνώσιμα από τους ανθρώπους σε κωδικοποιημένους χαρακτήρες για την αποτροπή μη εξουσιοδοτημένης πρόσβασης

Κλοπή Πληροφοριών



Page 230
Figure 5-14

Κλοπή Πληροφοριών

- Μια ψηφιακή υπογραφή είναι ένας κρυπτογραφημένος κώδικας που επισυνάπτεται ένα άτομο, μια τοποθεσία Web ή ένας οργανισμός σε ένα ηλεκτρονικό μήνυμα για την επαλήθευση της ταυτότητας του αποστολέα του μηνύματος
- Συχνά χρησιμοποιείται για να εξασφαλιστεί ότι ένας απατεώνας δεν συμμετέχει σε μια συναλλαγή στο Διαδίκτυο
- Ένα ψηφιακό πιστοποιητικό είναι μια ειδοποίηση που εγγυάται ότι ένας χρήστης ή ένας ιστότοπος είναι νόμιμος
- Μια τοποθεσία Web που χρησιμοποιεί τεχνικές κρυπτογράφησης για την ασφάλεια των δεδομένων της είναι γνωστή ως ασφαλής τοποθεσία
-

Κλοπή Πληροφοριών

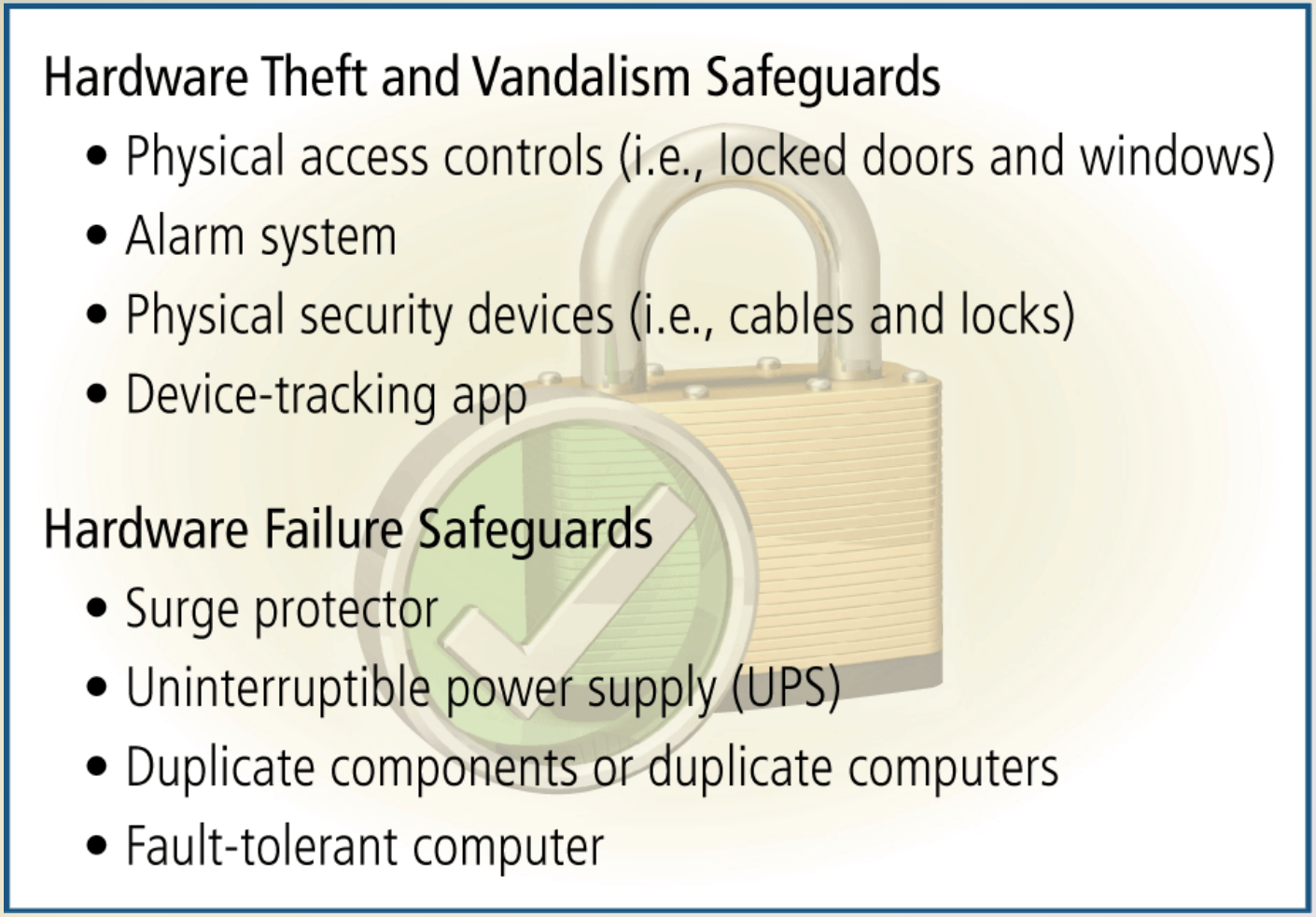
Page 231
Figure 5-15

Κλοπή υλικού, βανδαλισμός και αποτυχία

Η κλοπή υλικού είναι η πράξη της κλοπής ψηφιακού εξοπλισμού

Ο βανδαλισμός υλικού είναι η πράξη της αλλοίωσης ή καταστροφής του ψηφιακού εξοπλισμού

Κλοπή υλικού, βανδαλισμός και αποτυχία



Page 233
Figure 5-16

Δημιουργία αντιγράφων ασφαλείας - Η απόλυτη διασφάλιση

- Ένα αντίγραφο ασφαλείας είναι ένα αντίγραφο ενός αρχείου, προγράμματος ή μέσου που μπορεί να χρησιμοποιηθεί εάν το πρωτότυπο χαθεί, καταστραφεί ή καταστραφεί
- Για να δημιουργήσει αντίγραφο αντιγράφων σε ένα αρχείο σημαίνει να κάνετε ένα αντίγραφο του
- Τα αντίγραφα ασφαλείας εκτός τοποθεσίας αποθηκεύονται σε μια θέση ξεχωριστή από την τοποθεσία του υπολογιστή ή της κινητής συσκευής

Δημιουργία αντιγράφων ασφαλείας - Η απόλυτη διασφάλιση

- Κατηγορίες αντιγράφων ασφαλείας:
- Full
  - Differential
  - Incremental
  - Selective
  - Continuous data protection
  - Cloud

Δημιουργία αντιγράφων ασφαλείας - Η απόλυτη διασφάλιση

Table 5-2 Various Backup Methods

Type of Backup	Description	Advantages	Disadvantages
Full backup	Copies all of the files on media in the computer.	Fastest recovery method. All files are saved.	Longest backup time.
Differential backup	Copies only the files that have changed since the last full backup.	Fast backup method. Requires minimal storage space to back up.	Recovery is time-consuming because the last full backup plus the differential backup are needed.
Incremental backup	Copies only the files that have changed since the last full or incremental backup.	Fastest backup method. Requires minimal storage space to back up. Only most recent changes saved.	Recovery is most time-consuming because the last full backup and all incremental backups since the last full backup are needed.
Selective backup	Users choose which folders and files to include in a backup.	Fast backup method. Provides great flexibility.	Difficult to manage individual file backups. Least manageable of all the backup methods.
Continuous data protection (CDP)	All data is backed up whenever a change is made.	The only real-time backup. Very fast recovery of data.	Very expensive and requires a great amount of storage.
Cloud backup	Files are backed up to the cloud as they change.	Cloud backup provider maintains backup hardware. Files may be retrieved from anywhere with an Internet connection on any device.	Requires an Internet connection, otherwise files are marked for backup when the computer goes back online.

Page 234
Table 5-2

Ασύρματη ασφάλεια

- Η ασύρματη πρόσβαση εγκυμονεί πρόσθετους κινδύνους για την ασφάλεια
- Ορισμένοι δράστες συνδέονται με ασύρματα δίκτυα άλλων για να αποκτήσουν δωρεάν πρόσβαση στο Internet ή εμπιστευτικά δεδομένα
- Άλλοι συνδέονται σε ένα δίκτυο μέσω ενός μη ασφαλούς σημείου ασύρματης πρόσβασης (WAP) ή ενός δρομολογητή συνδυασμού/WAP
-

Page 236
Figure 5-18

Ηθική και Κοινωνία

- **Η τεχνολογική ηθική είναι οι ηθικές κατευθυντήριες γραμμές που διέπουν τη χρήση υπολογιστών, κινητών συσκευών, πληροφοριακών συστημάτων και συναφών τεχνολογιών**
- **Η ακρίβεια των πληροφοριών αποτελεί πρόβλημα**
- **Δεν είναι σωστές όλες οι πληροφορίες στο Internet**
-

Pages 238 - 240
Figure 5-20

Ηθική και Κοινωνία

- Η πνευματική ιδιοκτησία αναφέρεται σε μοναδικά και πρωτότυπα έργα όπως ιδέες, εφευρέσεις, τέχνη, γραπτά, διαδικασίες, ονόματα εταιρειών και προϊόντων και λογότυπα
- Τα δικαιώματα πνευματικής ιδιοκτησίας είναι τα δικαιώματα στα οποία οι δημιουργοί δικαιούνται το έργο τους
- Ένα πνευματικό δικαιώμα προστατεύει κάθε απτή μορφή έκφρασης
- Η διαχείριση ψηφιακών δικαιωμάτων (DRM) είναι μια στρατηγική που έχει σχεδιαστεί για την αποτροπή της παράνομης διανομής ταινιών, μουσικής και άλλου ψηφιακού περιεχομένου

Ηθική και Κοινωνία

- Ένας κώδικας δεοντολογίας είναι μια γραπτή κατευθυντήρια γραμμή που βοηθά να καθοριστεί αν μια προδιαγραφή είναι ηθική / ανήθικη ή επιτρέπεται / δεν επιτρέπεται
-

Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use technology in a way that demonstrates consideration and respect for fellow humans.

Page 241
Figure 5-21

Ηθική και Κοινωνία

- Η πράσινη πληροφορική περιλαμβάνει τη μείωση της ηλεκτρικής ενέργειας και των περιβαλλοντικών αποβλήτων κατά τη χρήση υπολογιστών, κινητών συσκευών και συναφών τεχνολογιών
-

Green Computing Tips

1. Conserve Energy
   a. Use computers and devices that comply with the ENERGY STAR program.
   b. Do not leave a computer or device running overnight.
   c. Turn off the monitor, printer, and other devices when not in use.
2. Reduce Environmental Waste
   a. Use paperless methods to communicate.
   b. Recycle paper and buy recycled paper.
   c. Recycle toner and ink cartridges, computers, mobile devices, printers, and other devices.
   d. Telecommute.
   e. Use videoconferencing and VoIP for meetings.

Page 241
Figure 5-22

Προστασία προσωπικών δεδομένων πληροφοριών

- Η προστασία της ιδιωτικής ζωής των πληροφοριών αναφέρεται στο δικαίωμα των ατόμων και των εταιρειών να αρνούνται ή να περιορίζουν τη συλλογή, τη χρήση και τη διάδοση πληροφοριών σχετικά με αυτά
- Τεράστιες βάσεις δεδομένων αποθηκεύουν δεδομένα σε απευθείας σύνδεση
- Οι τοποθεσίες Web συλλέγουν συχνά δεδομένα σχετικά με εσάς, ώστε να μπορούν να προσαρμόζουν διαφημίσεις και να σας στέλνουν εξατομικευμένα μηνύματα ηλεκτρονικού ταχυδρομείου
- Ορισμένοι εργοδότες παρακολουθούν τη χρήση του υπολογιστή σας και τα μηνύματα ηλεκτρονικού ταχυδρομείου
-

Προστασία προσωπικών δεδομένων πληροφοριών

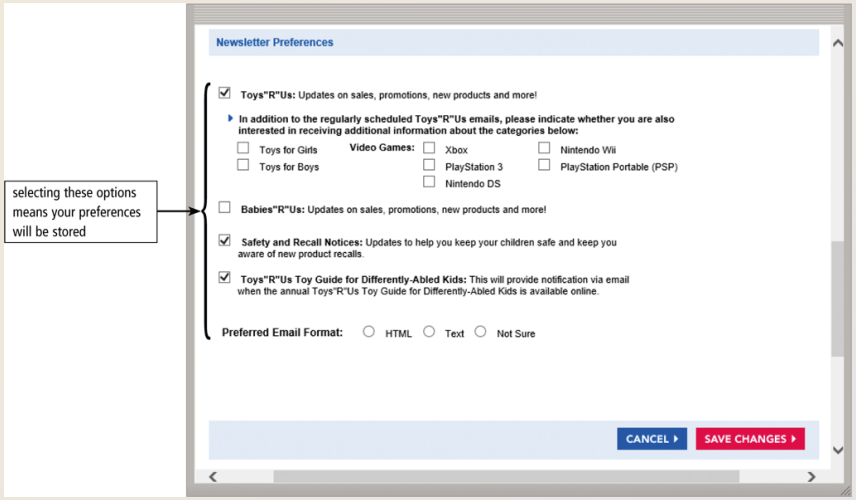
How to Safeguard Personal Information

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your phone number or Social Security number on personal checks.
3. Have an unlisted or unpublished phone number.
4. If you have Caller ID, find out how to block your number from displaying on the receiver's system.
5. Do not write your phone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, phone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to websites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free email account. Use this email address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for email filtering through your ISP or use an anti-spam program.
21. Do not reply to spam for any reason.
22. Surf the web anonymously or through an anonymous website.

Page 242
Figure 5-23

Προστασία προσωπικών δεδομένων πληροφοριών

- Πληροφορίες σχετικά με εσάς μπορούν να αποθηκευτούν σε μια βάση δεδομένων όταν γίνεται:
- Συμπλήρωση έντυπης ή ηλεκτρονικής φόρμας
- Δημιουργία προφίλ σε ηλεκτρονικό κοινωνικό δίκτυο
- Καταχωρήστε εγγύηση προϊόντος
-



Pages 242 - 243
Figure 5-24

Προστασία προσωπικών δεδομένων πληροφοριών

- Ένα cookie είναι ένα μικρό αρχείο κειμένου που αποθηκεύει ένας διακομιστής web στον υπολογιστή σας
- Οι ιστότοποι χρησιμοποιούν cookies για διάφορους

Δυνατότητα εξατομίκευσης

Αποθήκευση ονομάτων χρηστών ή/και κωδικών πρόσβασης

Βοήθεια στις ηλεκτρονικές αγορές

Παρακολούθηση της συχνότητας με την οποία οι χρήστες επισκέπτονται μια τοποθεσία

Διαφημίσεις-στόχοι

Pages 243 - 244

Προστασία προσωπικών δεδομένων πληροφοριών

Page 244
Figure 5-25

Virus(es) Ιοί

- που αναφέρονται σε κρυφές εντολές προγραμμάτων ή δεδομένα τα οποία εκτελούνται ή χρησιμοποιούνται ακουσίως και χωρίς προειδοποίηση από διάφορες διαδικασίες (διάβασμα ενός e-mail).

Worms

- Πρόγραμμα τα οποίο πολλαπλασιάζει τον εαυτό του εισβάλλει σε όσο το δυνατόν περισσότερα συστήματα υπολογιστών.

Trojan Horse

- Πρόγραμμα το οποίο παραμένει ανενεργό μέχρι τη στιγμή που κάποιο γεγονός στο ΠΣ συμβεί (π.χ. εισαγωγή δεδομένου, εκτέλεση προγράμματος, κλπ). Τότε το Trojan horse ενεργοποιείται και εκτελεί τις επιβλαβείς λειτουργίες του.

Salami Slicing

- Πρόγραμμα το οποίο «κλέβει» μικρά ποσά από ηλεκτρονικές συναλλαγές με αποτέλεσμα να γίνεται πολύ αργά αντιληπτό.

Sniffer

- Πρόγραμμα το οποίο ψάχνει για passwords καθώς αυτά «ταξιδεύουν» στο Διαδίκτυο.

Password Cracker

- Πρόγραμμα το οποίο προσπαθεί να «μαντέψει» ένα password.
- Μπορεί να είναι ιδιαίτερα αποτελεσματικό.

Κακόβουλα Applets

- Τα Applets είναι προγράμματα γραμμένα σε Java, τα οποία χρησιμοποιούν τους πόρους του συστήματος του Η/Υ κακόβουλα, π.χ.

- Στέλνει e-mails που δεν έχουμε στείλει με «διάφορα» μηνύματα, διαφοροποιεί προγραμματισμένες συναντήσεις, κλπ.

Spyware

- Μικρά προγράμματα που εγκαθίστανται λαθραία σε υπολογιστές και παρακολουθούν τη δραστηριότητα περιήγησης του χρήστη στον Ιστό και παρουσιάζουν διαφημίσεις

Καταγραφείς πληκτρολογήσεων (Key loggers)

- Καταγράφουν κάθε πληκτρολόγηση του χρήστη για να κλέψουν σειριακούς αριθμούς, κωδικούς πρόσβασης ή να εξαπολύσουν επιθέσεις στο Διαδίκτυο

Παραπλάνηση (Spoofing)

- Παραπλανητική αντιπροσώπευση κάποιου με τη χρήση πλαστών διευθύνσεων ηλεκτρονικού ταχυδρομείου ή παριστάνοντας κάποιον άλλο
- Ανακατεύθυνση συνδέσμου Ιστού σε διεύθυνση διαφορετική από την επιδιωκόμενη, όπου η τοποθεσία μοιάζει με την επιδιωκόμενη

Spoofing / Masquerading

Επιθέσεις άρνησης εξυπηρέτησης (DoS)

- Κατακλύζουν ένα διακομιστή με χιλιάδες ψευδή αιτήματα ώστε να καταρρεύσει το δίκτυο
  - Δίκτυα ρομπότ (Botnets)
    - Δίκτυα «ζόμπι» υπολογιστών τρίτων μολυσμένων με κακόβουλο λογισμικό

Ηλεκτρονικό ψάρεμα (Phishing)

- Δημιουργία πλαστών τοποθεσιών Ιστού ή αποστολή ηλεκτρονικών μηνυμάτων που μοιάζουν να προέρχονται από νόμιμες επιχειρήσεις και ζητούν από τους χρήστες εμπιστευτικά προσωπικά δεδομένα

Phishing -Κοινωνική μηχανική (social engineering)

From: Owen Geven ([redacted])
To: Christopher Burgess ([redacted])
Subject: Work Online From Home!

My name is Owen Geven, a designer and also the Manager of Owen Geven Fabric and Consultant and I live and work here in United Kingdom, Would you like to work online from home and get paid without affecting your present job? Actually I need a representative who can be working for the company as online book-keeper. We make lots of supplies to some of our clients in the EUROPE/USA/CANADA, for which I do come to USA/CANADA to receive payment and have it cashed after I supply them raw materials. It's always too expensive and stressful for me to come down and receive such payment twice in a month so I therefore decided to contact you. I am willing to pay you 10% for every payment receives by you from our clients who make payment through you. Please note you don't have to be a book keeper to apply for the job. Kindly get back to me as soon as possible if you are interested in this job offer with you're:

1. FULL NAMES..... 2. ADDRESS (not P.O.box).....
..... 3. STATE..... 4. ZIPCODE.....
5. COUNTRY..... 6. PHONE NUMBER(S).....7. GENDER.....
8. AGE..... 9. OCCUPATION.....

PLEASE SEND YOUR REPLY ASAP TO: ([redacted])

Απάτη των κλικ

- Συμβαίνει όταν κάποιο άτομο ή πρόγραμμα υπολογιστή επιλέγει μια διαφήμιση με δόλιο σκοπό χωρίς να έχει πρόθεση να μάθει περισσότερα για τον διαφημιζόμενο ή να αγοράσει κάτι

Και άλλα προγράμματα και τεχνικές που εξελίσσονται διαρκώς!!!

Στρατηγικές Αμύνης

Μηχανισμοί Ασφάλειας - 1η Θεώρηση

Πρόληψη

Φυσική ασφάλεια, access control, replication, Firewalls, Κρυπτογράφηση, Ψηφ. Υπογραφή, Προγράμματα antivirus, Ασφαλής Προγραμματισμός, Πολιτική κωδικών ασφάλειας,…

Ανίχνευση

Συστήματα Ανίχνευσης Εισβολών (IDS), Αρχεία καταγραφής, penetration testing,…

Απόκριση

Back-up, Digital forensics, malware removal, hot sites,…

Μηχανισμοί Ασφάλειας - 2η Θεώρηση

*

NIST 800-100 I.S. Handbook: A Guide for Managers

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 11-1: Security Control Class, Family, and Identifier

Κατηγορία Ελέγχου`	Πρόληψη	Ανίχνευση	Αντιμετώπιση
Φυσικής πρόσβασης (παραδείγματα)			
Φράχτες	X		X
Προσωπικό Ασφαλείας	X	X	X
Έξυπνες Κάρτες (smartcards), Βιομετρία	X		
Διαχειριστικός (παραδείγματα)			
Πολιτικές Ασφάλειας	X	X	X
Έλεγχος και Εποπτεία	X	X	
Εκπαίδευση υπαλλήλων	X	X	X
Λογικής Πρόσβασης (παραδείγματα)			
Λίστες Ελέγχου Πρόσβασης (ACLs), MAC, RBAC,…	X		
Passwords, CAPTCHAs	X		
Λογισμικό Antivirus, Anti-spam, Anti-Spyware,..	X	X	X
Κρυπτογράφηση Δεδομένων και Επικοινωνιών	X	X	
Firewalls (Packet Filters, Application Gateways)	X	X	
Συστήματα Ανίχνευσης & Αποτροπής Εισβολών (IDS/IPS)	X	X	X

Προστασία του ΠΣ

- Φυσικός Έλεγχος: Προστασία από φυσικές καταστροφές, διακοπή ρεύματος, κλιματισμός, συναγερμός.

- Στρατηγική: Κατάλληλη σχεδίαση του χώρου.

Προστασία του ΠΣ

- Πρόσβαση: Ποιος έχει πρόσβαση στο ΠΣ;
  - στο Φυσικό Χώρο
  - Στα προγράμματα
  - Στα δεδομένα.

  - Στρατηγική: Βιομετρική (έλεγχος αποτυπωμάτων, ίριδος ματιού, έλεγχος φωνής, κλπ.)

Προστασία του ΠΣ

- Προστασία Δεδομένων;

- Στρατηγική: back-up, τα συστήματα Βάσεων Δεδομένων έχουν μηχανισμούς που ελέγχουν την ακεραιότητα των δεδομένων.

Προστασία του ΠΣ

- Προστασία Δικτύου - Διαδικτύου;

- Στρατηγική:
  - Encryption.
  - Firewalls (είναι Λογισμικό ή συνδυασμός Λογισμικού Υλικού που ελέγχει την πολιτική πρόσβασης από δίκτυο σε δίκτυο, π.χ. από το Διαδίκτυο στο δικό μας δίκτυο μέσω του οποίου έχουμε πρόσβαση στο Διαδίκτυο).
  - Προστασία από Ιούς.

Προστασίας Εφαρμογών του ΠΣ

- Προστασία Εφαρμογών ΠΣ.

- Στρατηγική:
  - Έλεγχος Δεδομένων Εισόδου.
  - Έλεγχος Λογισμικού Εφαρμογών (Διάφορες Τεχνικές – Black Box, White Box).
  - Έλεγχος Αποτελεσμάτων.

Ελεγκτική εξέταση πληροφοριακών συστημάτων διοίκησης (MIS audit)

- Εξετάζει το συνολικό περιβάλλον ασφάλειας της επιχείρησης καθώς και όλους τους ελέγχους των επιμέρους πληροφοριακών συστημάτων.
- Εξετάζει τεχνολογίες, διαδικασίες, τεκμηρίωση, εκπαίδευση και προσωπικό.
- Μπορεί ακόμη να προσομοιώσει μια καταστροφή για να ελέγξει την απόκριση της τεχνολογίας, του προσωπικού των συστημάτων και των άλλων υπαλλήλων.
- Απαριθμεί και ιεραρχεί όλες τις αδυναμίες ελέγχου και εκτιμά τις πιθανότητες να συμβούν ζημιές.
- Εκτιμά τον οικονομικό και οργανωσιακό αντίκτυπο κάθε απειλής.

Προστασίας του ΠΣ συνολικά

- Risk Management

- Για τον προσδιορισμό πιθανών αιτιών δυσλειτουργιών, εκτίμησης του κόστους πρόνοιας – επισκευής – επιχειρησιακού κόστους από τη δυσλειτουργία.

- Εκτίμηση οφέλους από την ανάπτυξη ασφαλιστικών δικλείδων.