CHAPTER 10:

COMPUTER SECURITY AND RISKS

Multiple Choice:

1. In a survey of more than 500 companies and government agencies, _____ percent detected computer security breaches.

A. 20

B. 75

C. 85

D. 99

Answer: C **Reference:** The Digital Dossier **Difficulty:** Moderate

2. The survey showed that these businesses lost more than _____ due to security breaches.

A. $100,000 each

B. $377 million

C. five employees each

D. $1 million

Answer: B **Reference:** The Digital Dossier **Difficulty:** Moderate

3. The typical computer criminal is a(n):

A. young hacker.

B. trusted employee with no criminal record.

C. trusted employee with a long, but unknown criminal record.

D. overseas young cracker.

Answer: B **Reference:** The Digital Dossier **Difficulty:** Moderate

4. The majority of computer crimes are committed by:

A. hackers.

B. insiders.

C. overseas criminals.

D. young teenage computer geniuses.

Answer: B **Reference:** The Digital Dossier **Difficulty:** Moderate

5. The common name for the crime of stealing passwords is:

A. spooling.

B. identity theft.

C. spoofing.

D. hacking.

Answer: C **Reference:** Theft by Computer **Difficulty:** Moderate

6. The FBI's Operation Cyber Loss was designed to crack down on:

A. computer theft.

B. identity theft.

C. Internet fraud.

D. theft in Banking.

Answer: C **Reference:** Theft by Computer **Difficulty:** Moderate

7. Collecting personal information and effectively posing as another individual is known as the crime of:

A. spooling.

B. identity theft.

C. spoofing.

D. hacking.

Answer: B **Reference:** Identity Theft **Difficulty:** Easy

8. _____ is the term for the use of deception to get someone's sensitive information.

A. Identity theft

B. Social engineering

C. Spoofing

D. Hacking

Answer: B **Reference:** Identity Theft **Difficulty:** Easy

9. Malicious software is known as:

A. badware.

B. malware.

C. maliciousware.

D. illegalware.

Answer: B **Reference:** Software Sabotage: Viruses and Other Malware **Difficulty:** Easy

10. A program that performs a useful task while simultaneously allowing destructive acts is a:

A. worm.

B. Trojan horse.

C. virus.

D. macro virus.

Answer: B **Reference:** Trojan Horses **Difficulty:** Moderate

11. An intentionally disruptive program that spreads from either from program-to-program or from disk-to-disk is known as a:

A. Trojan horse.

B. virus.

C. time bomb.

D. time-related bomb sequence.

Answer: B **Reference:** Viruses **Difficulty:** Easy

12. In 1999, the Melissa virus was a widely publicized:

A. email virus.

B. macro virus.

C. Trojan horse.

D. Time bomb.

Answer: A **Reference:** Viruses **Difficulty:** Challenging

13. This virus that attaches itself to macros is called:

A. email virus.

B. macro virus.

C. Trojan horse.

D. time bomb.

Answer: B **Reference:** Viruses **Difficulty:** Easy

14. What type of virus uses computer hosts to reproduce itself?

A. Time bomb

B. Worm

C. Melissa virus

D. Macro virus

Answer: B **Reference:** Worms **Difficulty:** Moderate

15. The Code Red worm attacked:

A. UNIX operating systems

B. Microsoft Word

C. Microsoft server software

D. personal computers

Answer: C **Reference:** Worms **Difficulty:** Moderate

16. The thing that eventually terminates a worm is a lack of:

A. memory or disk space.

B. time.

C. CD drive space.

D. CD-RW.

Answer: A **Reference:** Worms **Difficulty:** Moderate

17. When a logic bomb is activated by a time-related event, it is known as a:

A. time-related bomb sequence.

B. virus.

C. time bomb.

D. Trojan horse.

Answer: C **Reference:** Trojan Horses **Difficulty:** Easy

18. A logic bomb that was created to erupt on Michelangelo's birthday is an example of a:

A. time-related bomb sequence.

B. virus.

C. time bomb.

D. Trojan horse.

Answer: C **Reference:** Trojan Horses **Difficulty:** Moderate

19. What is the name of an application program that gathers user information and sends it to someone through the Internet?

A. A virus

B. Spybot

C. Logic bomb

D. Security patch

Answer: B **Reference:** Spyware **Difficulty:** Moderate

20. When you visit certain Web sites spyware may be automatically downloaded. This is called a:

A. virus.

B. spybot.

C. logic bomb.

D. drive-by download.

Answer: D **Reference:** Spyware. **Difficulty:** Moderate

21. Standardization of Microsoft programs and the Windows operating system has made the spread of viruses:

A. more complicated.

B. more difficult.

C. easier.

D. slower.

Answer: C **Reference:** Virus Wars **Difficulty:** Easy

22. HTML viruses infect:

A. your computer.

B. a Web page in the HTML code.

C. both a Web page and the computer that is viewing it.

D. None of these answers is correct.

Answer: B **Reference:** Virus Wars **Difficulty:** Moderate

23. Software programs that close potential security breaches in an operating system are known as:

A. security breach fixes.

B. refresh patches.

C. security repairs.

D. security patches.

Answer: D **Reference:** Virus Wars **Difficulty:** Moderate

24. When customers of a Web site are unable to access it due to a bombardment of fake traffic, it is known as:

A. a virus.

B. a Trojan horse.

C. cracking.

D. a denial of service attack.

Answer: D **Reference:** Hacking and Electronic Trespassing **Difficulty:** Easy

25. Unauthorized access to computers is called:

A. a virus.

B. a worm.

C. cracking.

D. hacking.

Answer: D **Reference:** Hacking and Electronic Trespassing **Difficulty:** Easy

26. Criminal hacking is called:

A. a virus.

B. a Trojan horse.

C. cracking.

D. a worm.

Answer: C **Reference:** Hacking and Electronic Trespassing **Difficulty:** Easy

27. Hackers who hijack legitimate Web sites and redirect users to other sites are called:

A. hackers.

B. Trojan horses.

C. webjackers.

D. denial of service attackers.

Answer: C **Reference:** Hacking and Electronic Trespassing **Difficulty:** Easy

28. _____ is the measurement of things such as fingerprints and retinal scans used for security access.

A. Biometrics

B. Biomeasurement

C. Computer security

D. Smart weapon machinery

Answer: A **Reference:** Physical Access Restrictions **Difficulty:** Moderate

29. What is the most common tool used to restrict access to a computer system?

A. User logins

B. Passwords

C. Computer keys

D. Access-control software

Answer: B **Reference:** Passwords **Difficulty:** Moderate

30. The most common passwords in the U.S. or Britain include all EXCEPT:

A. love.

B. Fred.

C. God.

D. 123.

Answer: D **Reference:** Passwords **Difficulty:** Challenging

31. Hardware or software designed to guard against unauthorized access to a computer network is known as a(n):

A. hacker-proof program.

B. firewall.

C. hacker-resistant server.

D. encryption safe wall.

Answer: B **Reference:** Firewalls, Encryption, and Audits **Difficulty:** Easy

32. The scrambling of code is known as:

A. encryption.

B. firewalling.

C. scrambling.

D. password-proofing.

Answer: A **Reference:** Firewalls, Encryption, and Audits **Difficulty:** Moderate

33. If you want to secure a message, use a(n):

A. cryptology source.

B. encryption key.

C. encryption software package.

D. cryptosystem.

Answer: D **Reference:** How It Works: Cryptography **Difficulty:** Moderate

34. To prevent the loss of data during power failures, use a(n):

A. encryption program.

B. surge protector.

C. firewall.

D. UPS.

Answer: D **Reference:** Backups and Other Precautions **Difficulty:** Moderate

35. A(n) _____ can shield electronic equipment from power spikes.

A. encryption program

B. surge protector

C. firewall

D. UPS

Answer: B **Reference:** Backups and Other Precautions **Difficulty:** Moderate

36. All of these are suggestions for safe computing EXCEPT:

A. Don't borrow disks from other people.

B. Open all e-mail messages but open them slowly.

C. Download shareware and freeware with caution.

D. Disinfect your system.

Answer: B **Reference:** Working Wisdom: Safe Computing **Difficulty:** Easy

37. Freeware _____ encrypts data.

A. encryption

B. firewall software

C. PGP

D. private and public keys

Answer: C **Reference:** Working Wisdom: Safe Computing **Difficulty:** Moderate

38. _____ is defined as any crime completed through the use of computer technology.

A. Computer forensics

B. Computer crime

C. Hacking

D. Cracking

Answer: B **Reference:** The Digital Dossier **Difficulty:** Moderate

39. Most computer systems rely solely on _____ for authentication.

A. logins

B. passwords

C. encryption

D. lock and key

Answer: B **Reference:** The Role of System Administrators **Difficulty:** Moderate

40. Creating strong computer security to prevent computer crime usually simultaneously helps protect:

A. privacy rights.

B. personal ethics.

C. the number of cookies downloaded to your personal computer.

D. personal space.

Answer: A **Reference:** When Security Threatens Privacy **Difficulty:** Moderate

41. Over _____ was spent by businesses and government to repair problems in regard to Y2K.

A. 20 million dollars

B. 100 million dollars

C. 1 billion dollars

D. 100 billion dollars

Answer: D **Reference:** Bugs and Breakdowns **Difficulty:** Moderate

42. What is a complex system that takes on nearly complete responsibility for a task eliminating the need for people, verification, or decision making?

A. Autonomous system

B. Missile defense auto-system

C. Smart weapon

D. Independent system

Answer: A **Reference:** Autonomous System **Difficulty:** Moderate

43. Security procedures can:

A. eliminate all computer security risks.

B. reduce but not eliminate risks.

C. are prohibitively expensive.

D. are inaccessible for the average home user.

Answer: B **Reference:** Is Security Possible? **Difficulty:** Easy

Fill in the Blank:

44. The field of computer _____ uses special software to scan hard drives of criminal suspects.

Answer: forensics **Reference:** Online Outlaws: Computer Crime **Difficulty:** Challenging

45. Computer _____ often goes unreported because businesses fear negative publicity.

Answer: crime **Reference:** The Digital Dossier **Difficulty:** Moderate

46. _____ connections are the most frequent point of attack for Internet commerce sites.

Answer: Internet **Reference:** The Digital Dossier **Difficulty:** Easy

47. _____ is the most common form of computer crime.

Answer: Theft **Reference:** Theft by Computer **Difficulty:** Moderate

48. Operation Cyber Loss was designed by the FBI was to crack down on_____.

Answer: Internet fraud **Reference:** Theft by Computer **Difficulty:** Moderate

49. The use of deception to get someone's sensitive information is called _____.

Answer: Social engineering **Reference:** Theft by Computer **Difficulty:** Moderate

50. A survey by eMarketer.com found that _____ are the most frequently cited online fraud cases.

Answer: online auctions **Reference:** Identity Theft **Difficulty:** Challenging

51. Theft of computers is most common for PDAs and _____ computers.

Answer: notebook **Reference:** Theft by Computer **Difficulty:** Moderate

52. When you use a disk in several different computers within the same day, you are taking the chance of contracting a(n) _____.

Answer: virus **Reference:** Viruses **Difficulty:** Easy

53. A(n) _____ attaches itself to documents that contain embedded programs that automate tasks.

Answer: macro virus **Reference:** Viruses **Difficulty:** Moderate

54. Both viruses and _____ use computer hosts to replicate.

Answer: worms **Reference:** Worms **Difficulty:** Challenging

55. The Code Red worm attacked_____.

Answer: Microsoft servers **Reference:** Worms **Difficulty:** Challenging

56. _____ programs search for and eliminate viruses.

Answer: Antivirus **Reference:** Virus Wars **Difficulty:** Easy

57. A security patch is a software program that closes possible security breaches in the operating system. The cost to the consumer is _____.

Answer: nothing or free **Reference:** Virus Wars **Difficulty:** Easy

58. _____ refers to electronic trespassing or criminal hacking.

Answer: Cracking **Reference:** Hacking and Electronic Trespassing **Difficulty:** Moderate

59. DoS stands for _____.

Answer: denial of service **Reference:** Hacking and Electronic Trespassing **Difficulty:** Moderate

60. DDoS stands for _____.

Answer: distributed denial of service **Reference:** Hacking and Electronic Trespassing **Difficulty:** Moderate

61. _____ hijack Web pages and redirect users to other sites.

Answer: Webjackers **Reference:** Hacking and Electronic Trespassing **Difficulty:** Challenging

62. _____ software monitors and records computer transactions.

Answer: Audit-control **Reference:** Firewalls, Encryption, and Audits **Difficulty:** Challenging

63. Each individual who uses a public key cryptosystem has _____ keys.

Answer: two **Reference:** How It Works: Cryptography **Difficulty:** Easy

64. Most widely used recovery technique is _____.

Answer: Backups **Reference:** Backups and other precautions **Difficulty:** Easy

65. RAID stands for _____.

Answer: Redundant array of independent disk **Reference:** Backups and other precautions
Difficulty: moderate

66. A(n) _____ guarantees that users have permission to perform particular actions.

Answer: authorization mechanism **Reference:** The Role of System Administrators
Difficulty: Challenging

67. PGP stands for _____.

Answer: Pretty Good Privacy **Reference:** Working Wisdom: Safe Computing **Difficulty:** Moderate

68. In 2000 the U.S. government found Microsoft guilty of _____.

Answer: Monopolistic activities **Reference:** Working Wisdom: Safe Computing **Difficulty:** Moderate

69. A microprocessor-controlled badge is called a(n) _____.

Answer: active badge **Reference:** Working Wisdom: Safe Computing **Difficulty:** Moderate

70. Most operating systems, including Windows XP, assign each user a unique _____.

Answer: user identifier or user ID **Reference:** Human Security Controls **Difficulty:** Moderate

71. Special purpose hardware that will allow every message to be encrypted is called a(n) _____.

Answer: security processor **Reference:** The Future of Internet Security **Difficulty:** Moderate

72. The term once used for malicious computer wizardry is _____.

Answer: hackers or hacking **Reference:** Hacking and Electronic Trespassing **Difficulty:** Moderate

Matching:

73. Match the acts and centers with their purposes:

I. Computer Fraud and Abuse Act	A. created by Attorney General Janet Reno in 1998
II. USA Patriot Act	B. defines what kinds of communications are legal online
III. Digital Millennium Copyright Act	C. created in 2001 as a response to the terrorist attacks of September 11, 2001
IV. Telecommunications Act of 1996	D. provides instant information on crimes and criminals
V. Communications Decency Act	E. declared unconstitutional by the Supreme Court
VI. National Infrastructure Protection Center	F. created as a result of the first headline-making worm
VII. National Crime Information Center	G. used to arrest a student for writing to crack an Adobe product

Answers: F, C, G, B, E, A, D **Reference:** Multiple locations **Difficulty:** Challenging

74. Match the following rules of thumb about safe computing with the proper descriptions:

I. share with care	A. be aware of e-mail from what appear to be legitimate companies
II. handle email carefully	B. don't choose a dictionary word
III. disinfect regularly	C. keep your disks in your own computer
IV. take your password seriously	D. copy, copy, copy
V. if it's important, back it up	E. encrypt
VI. sensitive info over the Internet?	F. use antivirus software

Answers: C, A, F, B, D, E **Reference:** Working Wisdom: Safe Computing **Difficulty:** Moderate

