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.
	1. 20
	2. 75
	3. 85
	4. 99

**Answer:** C **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. The survey showed that these businesses lost more than \_\_\_\_\_\_\_\_\_\_\_\_ due to security breaches.
	1. $100,000 each
	2. $377 million
	3. five employees each
	4. $1 million

**Answer:** B **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. The typical computer criminal is a(n):
	1. young hacker.
	2. trusted employee with no criminal record.
	3. trusted employee with a long, but unknown criminal record.
	4. overseas young cracker.

**Answer:** B **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. The majority of computer crimes are committed by:
	1. hackers.
	2. insiders.
	3. overseas criminals.
	4. young teenage computer geniuses.

**Answer:** B **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. The common name for the crime of stealing passwords is:
	1. spooling.
	2. identity theft.
	3. spoofing.
	4. hacking.

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

1. Collecting personal information and effectively posing as another individual is known as the crime of:
	1. spooling.
	2. identity theft.
	3. spoofing.
	4. hacking.

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

1. Malicious software is known as:
	1. badware.
	2. malware.
	3. maliciousware.
	4. illegalware.

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

1. A program that performs a useful task while simultaneously allowing destructive acts is a:
	1. worm.
	2. Trojan horse.
	3. virus.
	4. macro virus.

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

1. An intentionally disruptive program that spreads from program to program or from disk to disk is known as a:
	1. Trojan horse.
	2. virus.
	3. time bomb.
	4. time-related bomb sequence.

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

1. In 1999, the Melissa virus was a widely publicized:
	1. e-mail virus.
	2. macro virus.
	3. Trojan horse.
	4. Time bomb.

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

1. What type of virus uses computer hosts to reproduce itself?
	1. Time bomb
	2. Worm
	3. Melissa virus
	4. Macro virus

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

1. The thing that eventually terminates a worm virus is a lack of:
	1. memory or disk space.
	2. time.
	3. CD drive space.
	4. CD-RW.

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

1. When a logic bomb is activated by a time-related event, it is known as a:
	1. time-related bomb sequence.
	2. virus.
	3. time bomb.
	4. Trojan horse.

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

1. A logic bomb that was created to erupt on Michelangelo’s birthday is an example of a:
	1. time-related bomb sequence.
	2. virus.
	3. time bomb.
	4. Trojan horse.

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

1. What is the name of an application program that gathers user information and sends it to someone through the Internet?
	1. A virus
	2. Spybot
	3. Logic bomb
	4. Security patch

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

1. Standardization of Microsoft programs and the Windows operating system has made the spread of viruses:
	1. more complicated.
	2. more difficult.
	3. easier.
	4. slower.

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

1. HTML viruses infect:
	1. your computer.
	2. a Web page in the HTML code.
	3. both a Web page and the computer that is viewing it.
	4. None of these answers is correct.

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

1. Software programs that close potential security breaches in an operating system are known as:
	1. security breach fixes.
	2. refresh patches.
	3. security repairs.
	4. security patches.

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

1. When customers of a Web site are unable to access it due to a bombardment of fake traffic, it is known as:
	1. a virus.
	2. a Trojan horse.
	3. cracking.
	4. a denial of service attack.

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

1. \_\_\_\_\_\_\_\_\_\_\_ is the measurement of things such as fingerprints and retinal scans used for security access.
	1. Biometrics
	2. Biomeasurement
	3. Computer security
	4. Smart weapon machinery

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

1. What is the most common tool used to restrict access to a computer system?
	1. User logins
	2. Passwords
	3. Computer keys
	4. Access-control software

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

1. The most common passwords in the U.S. or Britain include all EXCEPT:
	1. love.
	2. Fred.
	3. God.
	4. 123.

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

1. Hardware or software designed to guard against unauthorized access to a computer network is known as a(n):
	1. hacker-proof program.
	2. firewall.
	3. hacker-resistant server.
	4. encryption safe wall.

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

1. The scrambling of code is known as:
	1. encryption.
	2. a firewall.
	3. scrambling.
	4. password-proofing.

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

1. If you want to secure a message, use a(n):
	1. cryptology source.
	2. encryption key.
	3. encryption software package.
	4. cryptosystem.

**Answer:** D **Reference:** How It Works: 10.2 Cryptography **Difficulty:** Moderate

1. To prevent the loss of data during power failures, use a(n):
	1. encryption program.
	2. surge protector.
	3. firewall.
	4. UPS.

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

1. A(n) \_\_\_\_\_\_\_\_\_\_\_\_ can shield electronic equipment from power spikes.
	1. encryption program
	2. surge protector
	3. firewall
	4. UPS

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

1. All of these are suggestions for safe computing EXCEPT:
	1. don’t borrow disks from other people.
	2. open all e-mail messages but open them slowly.
	3. download shareware and freeware with caution.
	4. disinfect your system.

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

1. Freeware \_\_\_\_\_\_\_\_\_\_\_ encrypts data.
	1. encryption
	2. firewall software
	3. PGP
	4. private and public keys

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

1. \_\_\_\_\_\_\_\_\_\_\_\_ is defined as any crime completed through the use of computer technology.
	1. Computer forensics
	2. Computer crime
	3. Hacking
	4. Cracking

 **Answer:** B **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. Most computer systems rely solely on \_\_\_\_\_\_\_\_\_\_\_ for authentication.
	1. logins
	2. passwords
	3. encryption
	4. lock and key

**Answer:** B **Reference:** Human Security Controls: Law, Management, and Ethics **Difficulty:** Moderate

1. Creating strong computer security to prevent computer crime usually simultaneously helps protect :
	1. privacy rights.
	2. personal ethics.
	3. the number of cookies downloaded to your personal computer.
	4. personal space.

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

1. Over \_\_\_\_\_\_\_\_\_\_\_ was spent by businesses and government to repair problems in regard to Y2K.
	1. 20 million dollars
	2. 100 million dollars
	3. 1 billion dollars
	4. 100 billion dollars

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

1. What is a complex system that takes on nearly complete responsibility for a task eliminating the need for people, verification, or decision making?
	1. Autonomous system
	2. Missile defense auto-system
	3. Smart weapon
	4. Independent system

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

1. Security procedures can:
	1. will eliminate all computer security risk.
	2. reduce but not eliminate risks.
	3. are prohibitively expensive.
	4. are inaccessible for the average home user.

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

## Fill in the Blank:

1. The field of computer \_\_\_\_\_\_\_\_\_\_\_\_ uses special software to scan hard drives of potential criminal suspects.

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

1. Computer \_\_\_\_\_\_\_\_\_\_\_\_ often goes unreported because businesses fear negative publicity.

**Answer:** crime **Reference:** The Computer Crime Dossier **Difficulty:** Moderate

1. \_\_\_\_\_\_\_\_\_\_\_\_ connections are the most frequent point of attack for Internet commerce.

**Answer:** Internet **Reference:** The Computer Crime Dossier **Difficulty:** Easy

1. \_\_\_\_\_\_\_\_\_\_\_\_ is the most common form of computer crime.

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

1. A survey by eMarketer.com found that \_\_\_\_\_\_\_\_\_\_\_\_ are the most often cited online fraud cases.

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

1. Theft of computers is most common for PDAs and \_\_\_\_\_\_\_\_\_\_\_\_ computers.

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

1. 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

1. A(n) \_\_\_\_\_\_\_\_\_\_\_\_ attaches itself to documents that contain embedded programs that automate tasks.

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

1. Both viruses and \_\_\_\_\_\_\_\_\_\_\_\_ use computer hosts to replicate.

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

1. \_\_\_\_\_\_\_\_\_\_\_\_ programs search for and eliminate viruses.

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

1. 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

1. \_\_\_\_\_\_\_\_\_\_\_\_ was once the word used for malicious computer wizardry.

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

1. \_\_\_\_\_\_\_\_\_\_\_\_ refers to electronic trespassing or criminal hacking.

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

1. DoS stands for \_\_\_\_\_\_\_\_\_\_\_.

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

1. DDoS stands for \_\_\_\_\_\_\_\_\_\_\_.

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

1. \_\_\_\_\_\_\_\_\_\_\_\_ hijack Web pages and redirect users to other sites.

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

1. \_\_\_\_\_\_\_\_\_\_\_ software monitors and records computer transactions.

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

1. Each individual who uses a public key cryptosystem has \_\_\_\_\_\_\_\_\_\_\_ keys.

**Answer:** two **Reference:** How It Works: 10.2 Cryptography **Difficulty:** Easy

1. PGP stands for \_\_\_\_\_\_\_\_\_\_\_.

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

1. Most operating systems, including Windows XP, assign each user a unique \_\_\_\_\_\_\_\_\_\_\_.

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

1. It should now be common knowledge that users should not open \_\_\_\_\_\_\_\_\_\_\_ from e-mail recipients that the user does not know.

**Answer:** attachments **Reference:** Crosscurrents: Idiocy Imperils the Web **Difficulty:** Moderate

## Matching:

1. 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

1. 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 e-mail 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