Computers Are Your Future

Chapter 9

Privacy, Crime, AND Security

# Answers to End-of-Chapter Questions

## Matching

\_\_**m**\_\_\_ 1. cookie “Technology and Anonymity”

\_\_**e**\_\_\_ 2. phishing “Types of Computer Crime”

\_\_**a**\_\_\_ 3. spim “Types of Computer Crime”

\_\_**i**\_\_\_ 4. Trojan horse “Types of Computer Crime”

\_\_**g**\_\_\_ 5. worm “Types of Computer Crime”

\_\_**o**\_\_\_ 6. spyware “Types of Computer Crime”

\_\_**k**\_\_\_ 7. podslurping “Security Risks”

\_\_**c**\_\_\_ 8. memory shaving “Security Risks”

\_\_**n**\_\_\_ 9. digital signature “Public Key Encryption”

\_\_**b**\_\_\_ 10. adware “Types of Computer Crime”

\_\_**f**\_\_\_ 11. botnet “Types of Computer Crime”

\_\_**d\_**\_\_ 12. trap door “Security Risks”

\_\_**j\_**\_\_ 13. wardriving “Security Risks”

\_\_**h**\_\_\_ 14. backdoor “Encryption and Public Security Issues”

\_**\_l\_**\_\_ 15. salami shaving “Types of Computer Crime”

## Multiple Choice

1. What is the act of harassing or threatening an individual less capable of defending himself or herself repeatedly through the use of electronic communications?

a. phishing

b. cracking

**c. cyberbullying** “Types of Computer Crime”

d. hacking

2. What is the substitute for barcodes, often used for inventory tracking, which can also pose privacy risks if not deactivated?

**a. RFID** “Technology and Anonymity”

b. SET

c. WEP

d. WPA

3. What is the name for text that has been encrypted and converted to a coded message format?

a. DoS

**b. ciphertext** “Encryption Basics”

c. GUID

d. spim

4. What is the term for flooding a service with meaningless data in an attempt to make that service unavailable to other users?

a. salami shaving

b. spam

c. spim

d. a denial of service (DoS) attack “Types of Computer Crime”

5. In an auction, which of the following refers to an accomplice of the seller who drives up prices by bidding for an item he or she has no intention of buying?

**a. shill** “Meet the Attackers”

b. phish

c. spim

d. variant

6. Which of the following is an example of malware?

a. a zombie

b. an evil twin

**c. a macro virus** “Types of Computer Crime”

d. an active badge

7. What is malware that sits harmlessly on your system until a certain event or set of circumstances makes the program active?

a. a macro virus

b. a worm

c. shaving Trojan horse

**d. a time bomb** “Types of Computer Crime”

8. What is the name for an identification number that is generated by a hardware component or a program that can be read by Web servers or embedded in various documents, making anonymity difficult?

a. global unique identifier (GUID) “Technology and Anonymity”

b. file infector

c. key interception

d. zombie

9. What method of user validation uses a variety of techniques such as voice recognition, retina scans, and fingerprints?

a. digital signature

b. digital certificate

c. biometric authentication “Protecting Your Privacy”

d. global unique identifier

10. Which of the following is one of the earliest wireless security standards and may be the only option for older devices despite known weaknesses?

a. 802.11n

b. WPA

c. GUID

**d. WEP** “Security Risks”

## Fill-In

1. \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ uses a single key to encrypt and decrypt.

Symmetric key encryption “Encryption Basics”

2. Applications such as NetStumbler and Kismet are often used in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to locate wireless networks.

**wardriving** “Security Risks”

3. A(n) \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ is a transparent graphic image, usually no larger than 1 pixel × 1 pixel, that is placed on a Web site or in an e-mail and used to monitor the behavior of the user visiting the Web site or sending the e-mail.

**Web beacon** “Protecting Your Privacy”

4. A(n) \_\_\_\_\_\_\_\_\_\_\_\_ is an individual who studies the process of transforming information into an encoded state.

**cryptographer** “The Encryption Debate”

5. \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ refers to a coding or scrambling process that renders a message unreadable by anyone except the intended recipient.

Public key encryption “Public Key Encryption”

6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_is the ability to convey a message without disclosing your name or identity.

**Anonymity** “Technology and Anonymity”

7. \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ makes use of fake e-mails and social engineering to trick specific people, such as senior executives or members of a particular organization, into providing personal information to enable identity theft.

**Spear phishing** “Types of Computer Crime”

8. \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ is a computing scenario that foresees individuals interacting with multiple devices in every aspect of our lives connected through an omnipresent network.

**Ubiquitous computing** “Technology and Anonymity”

9.A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_is a type of software program that records all the keystrokes a user enters—such as passwords, account numbers, or conversations—and relays them to others.

**keylogger** “Types of Computer Crime”

10. A(n) \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ is a form of malware that installs itself on the beginning tracks of a hard drive, where stored code is automatically executed every time you start the computer. Thus, the infection is spread by simply starting your system.

**boot sector virus** “Types of Computer Crime”

11. \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ makes use of an encryption and decryption key.

Symmetric key encryption “Encryption Basics”

12. Commandeered computers known as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are often used by botnets to

distribute spam and malware.

**zombies** “Types of Computer Crime”

13. A(n) \_\_\_\_\_\_\_\_\_\_\_ is a group of computer users who are obsessed with gaining entry into highly secure computer systems.

**cybergang** “Meet the Attackers”

14. A(n) \_\_\_\_\_\_\_\_\_\_\_ is a program that permits an organization’s computers to use the Internet but places severe limits on the ability of outsiders to access internal data.

**firewall** “Protecting Your Computer System”

15. \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_is an online shopping and security standard for merchants and customers.

**Secure Electronic Transaction** “Public Key Encryption”

## Short Answer

1. Define and explain the difference between the two different types of phishing.

***Phishing* refers to the act of a “phisher” sending e-mails or setting up a Web site that appears to be from a legitimate company in an attempt to obtain personal information such as your social security number, user name, password, or account numbers. Because the communication looks legitimate, you may comply, thus providing the phisher with access to your accounts.**

***Spear phishing*, similar to phishing, also uses fake e-mails and social engineering to trick recipients into providing personal information to enable identity theft; however, spear phishing attempts are targeted to specific people rather than randomly.**

1. List the five actions that an organization can take to deter corporate espionage.
* **Identify and label sensitive information.**
* **Protect against data deletion and loss by write- and password protecting documents and by creating regular backups.**
* **Make employees aware of security policies and the consequences of violating them.**
* **Reassess security policies annually, or more frequently if needed.**
* **Perform regular auditing and random and regular monitoring.**
* **Install necessary hardware and software to protect systems and data from violations from both inside and outside sources.**
* **Force password changes at least every 5 days if data within the organization is highly sensitive.**
1. List the three types of viruses and explain how they differ.

***A file infector virus* attaches itself to a program file. When the program is executed, the virus spreads to other programs on the user’s hard disk.**

***A boot sector virus* also propagates by an infected program, but it installs itself on the beginning tracks of a hard drive, where code is stored that automatically executes every time you start the computer.**

***A macro virus* takes advantage of the automatic command execution capabilities called macros, which are found in some productivity software; a macro is a saved sequence of commands or keyboard strokes that are recalled when needed with a single command or keyboard stroke.**

1. What are some of the signs that might indicate that spyware is on a system?

**Signs of spyware on a computer system include pop-up ads, targeted banner ads, sluggish performance, frequent crashes, unauthorized changes to your home or search pages, and the appearance of new browser toolbars.**

1. List three actions that a user can take to avoid inadvertently obtaining spyware or malware.

**The following actions can help a computer user avoid spyware or malware:**

* **Install antispyware software and update it frequently.**
* **Create a firewall.**
* **Avoid questionable Web sites.**
* **Never click on pop-up ads.**
* **Download software only from reputable sources.**