Chapter 6: Network and Internet Security and Privacy
Quiz Yourself Answers

1. Many organizations and education institutions publish codes of conduct to explain acceptable computer use to their employees, students, or other users.

2. The typical motivation for hacking is to steal data, sabotage a computer system, or perform some other type of illegal act.

3. Hackers might be moving away from targeting data stored on a company servers and focusing on stealing data in real time during credit card and debit card transactions because due to the Payment Card Industry Data Security Standard (PCI DSS) rules that require companies to limit the credit card data stored on company servers and to encrypt the data that is allowed to be stored.

4. A botnet is a group of bots that are controlled by one hacker or other computer criminal.

5. Malware is the generic term that refers to any type of malicious software that are written to perform destructive acts.

6. A DoS attack disables a server by flooding a network server or Web server with so many request for action that is shuts down or cannot handle legitimate requests any longer, causing legitimate users to be denied service.

7. Phishing is the use of a spoofed email message—an email that appears to come from a legitimate organization but is actually sent from a phisher—to trick the recipient into revealing sensitive personal information that is then used in identity theft and other fraudulent activities.

8. Online auction fraud (also called Internet auction fraud) occurs when an online auction buyer pays for merchandise that is never delivered, or that is delivered but is not as represented.

9. The purpose of a digital signature is to authenticate the identity of an individual or organization.

10. Many states and schools are reviewing their harassment statues and bullying policies because cyberbullying is so common today, affecting as many as one-half of all U.S. teenagers.

11. A hard drive that use uses full-disk encryption is often called a self-encrypting hard drive.

12. Antivirus software protects a computer against computer viruses and other types of malware.

13. A firewall helps to protect a computer by essentially creating a barrier between a computer or network and the Internet t protect against unauthorized use.

14. A marketing database contains marketing and demographic data about people that is then used for marketing purposes.

15. A throw-away email address is a second address obtained from your ISP or a free email address such as one from Windows Live Hotmail or Google's Gmail.

16. Opting out refers to following a predesignated procedure to remove yourself from marketing lists, or otherwise preventing our personal information from being obtained by or shared with others. Opting in refers to requesting participation in to a particular marketing activity before companies can collect or share any personal data.

17. Computer monitoring software records keystrokes, logs the programs or Web site accessed, or otherwise monitors someone's computer activity.

18. It is legal for a company to review the email of its employees.