***Corporate Computer Security, 5e* (Boyle/Panko)**
Chapter 1 The Threat Environment

1) The three common core goals of security are _____.
A) confidentiality, information, and authorization
B) confidentiality, integrity, and authentication
C) confidentiality, information, and availability
D) confidentiality, integrity, and availability
Answer: D
Page Ref: 3
Learning Objective: 1.1 Define the term threat environment
Difficulty: Moderate

2) If an attacker breaks into a corporate database and deletes critical files, this is an attack against the _____ security goal.
A) confidentiality
B) integrity
C) availability
D) CIA
Answer: B
Page Ref: 3
Learning Objective: 1.1 Define the term threat environment
Difficulty: Moderate

3) Which of the following is NOT a type of countermeasure?
A) Corrective
B) Preventative
C) Detective
D) Sustainable
Answer: D
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Moderate

4) When a threat succeeds in causing harm to a business, this is known as a(n) _____.
A) breach
B) PII
C) CIA
D) unintended access
Answer: A
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

5) Methods that security professionals use to try to stop threats include all of the following EXCEPT _____.
A) safeguards
B) countermeasure
C) protections
D) breaches
Answer: D
Page Ref: 3
Learning Objective: 1.1 Define the term threat environment
Difficulty: Moderate

6) Which of the following is NOT a type of countermeasure?
A) Detective
B) Corrective
C) Cyberwar
D) Preventative
Answer: C
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

7) The cost of computer crime is well known.
Answer: FALSE
Page Ref: 2
Learning Objective: 1.1 Define the term threat environment
Difficulty: Moderate

8) Availability means that attackers cannot change or destroy information.
Answer: FALSE
Page Ref: 3
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

9) Costs for all threats is increasing annually.
Answer: TRUE
Page Ref: 3
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

10) Corrective countermeasures identify when a threat is attacking.
Answer: FALSE
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

11) Preventative countermeasures keep attacks from succeeding.
Answer: TRUE
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

12) Detective countermeasures is considered one of the security goals of computer staff.
Answer: FALSE
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

13) Most countermeasure controls are preventative controls.
Answer: TRUE
Page Ref: 4
Learning Objective: 1.1 Define the term threat environment
Difficulty: Easy

14) A _____ happens when an unauthorized person is able to view, alter, or steal secured data.
A) countermeasure
B) data breach
C) safeguard
D) compromise
Answer: B
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

15) More than _____ records were stolen in 2018.
A) 2.2 billion
B) 1 million
C) 5 billion
D) 100,000
Answer: C
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

16) Which of the following is true about data breaches in 2018?
A) It's likely that half of all Americans lost their records at least one time in 2018.
B) It's likely that nearly everyone lost their records at least one time in 2018.
C) More than 12 billion people lost their records in 2018.
D) Slightly less than half of the world's population lost their records at least once in 2018.
Answer: B
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

17) Indirect costs due to data breaches are estimated to be:
A) $3.9 million per incident
B) $150 million per year
C) $10,000 per incident
D) $190,000 per year
Answer: A
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

18) The chances of an organization having a data breach over the next two years is approximately _____.
A) 10 percent
B) 20 percent
C) 42 percent
D) 28 percent
Answer: D
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

19) Which of the following is NOT an indirect cost of a major data breach?
A) Loss of reputation
B) Notification costs
C) Abnormal customer turnover
D) Increased customer acquisition activities
Answer: B
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

20) Which of the following is NOT a direct cost of a major data breach?
A) Loss of reputation
B) Notification costs
C) Legal fees
D) Detection
Answer: A
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

21) Which of the following companies experienced the largest data breach in history in 2016?
A) Amazon
B) Yahoo! Inc.
C) First American Corp.
D) Facebook
Answer: B
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

22) When a data breach occurs, hackers are primarily looking for _____.
A) personal and business addresses
B) access to systems
C) personally identifiable information
D) cash and credit card numbers
Answer: C
Page Ref: 6
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

23) Stolen information is commonly used for _____.
A) credit card fraud
B) identity theft
C) false claims
D) data mismanagement
Answer: A
Page Ref: 6
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

24) Which of the following is typically considered the first step in protecting your company from data breaches?
A) Locking up your data to prevent data breaches
B) Understanding how data breaches happen
C) Purchasing software to prevent data breaches
D) Hiring a qualified data security team
Answer: B
Page Ref: 7
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

25) Data from Target customers was stolen _____.
A) online
B) from point-of-sale (POS) systems
C) primary by internal hackers, mostly employees
D) through employee extortion
Answer: B
Page Ref: 7
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

26) Attackers in the Target data breach used malware and then used _____ or _____ to infect a Target third party vendor.
A) spear phishing; sabotage
B) hacking; sabotage
C) spear phishing; a targeted phishing attack
D) viruses; worms
Answer: C
Page Ref: 7
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

27) What is Trojan.POSRAM in regard to Target's data breach?
A) Employee sabotage
B) Malware
C) A virus
D) A worm
Answer: B
Page Ref: 8
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

28) The Target data breach helped impact a shift from swipe cards to _____.
A) EMV-compliant smart cards
B) POS systems
C) keystroke logger
D) rootkits
Answer: A
Page Ref: 8
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

29) One of the long-lasting effects of the data breach to Target was _____.
A) loss of money
B) loss of customer confidence
C) loss of merchandise
D) employee dissatisfaction
Answer: B
Page Ref: 8
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

30) Data breaches are rarely costly to a company.
Answer: FALSE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Moderate

31) Data breaches are always the result of hackers in distant locations.
Answer: FALSE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

32) Direct costs of handling a data breach include paying for notification and detection.
Answer: TRUE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

33) Indirect cost related to data breaches average an addition $10 million per incident in the U.S.
Answer: FALSE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

34) There is about a one in four chance that your organization will experience a data breach.
Answer: TRUE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

35) More than 67 percent of data breaches come from hackers trying to make money.
Answer: TRUE
Page Ref: 5
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

36) Rogue internal employees typically have a more difficult time stealing data than do external hackers.
Answer: FALSE
Page Ref: 6
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

37) The Target data breach affected 30 percent of the population of the U.S.
Answer: TRUE
Page Ref: 7
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

38) Trojan.POSRAM is a variant of the ILOVEYOU virus.
Answer: FALSE
Page Ref: 8
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

39) Hackers sold stolen credit card information gained from the Target breach.
Answer: TRUE
Page Ref: 9
Learning Objective: 1.2 Describe the impact of data breaches
Difficulty: Easy

40) Which of the following is FALSE about employees being considered dangerous in regard to security?
A) Employees usually have extensive knowledge of systems.
B) Employees often have the credentials needed to access sensitive parts of systems.
C) Companies generally have little trust in their employees.
D) Employees know corporate control mechanisms and so often know how to avoid detection.
Answer: C
Page Ref: 11
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Moderate

41) _____ are considered the most dangerous of all employees.
A) Financial professionals
B) IT security employees
C) CEOs
D) Data entry clerks
Answer: B
Page Ref: 11
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Moderate

42) _____ is the destruction of hardware, software, or data.
A) Extortion
B) Denial of service
C) Hacking
D) Sabotage
Answer: D
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

43) In _____, a perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest.
A) fraud
B) hacking
C) abuse
D) extortion
Answer: D
Page Ref: 14
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

44) _____ consists of activities that violate a company's IT use and/or ethics policies.
A) Abuse
B) Fraud
C) Extortion
D) Hacking
Answer: A
Page Ref: 14
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

45) Which of the following is considered a trade secret?
A) Product formulations
B) Patents
C) Trade names
D) Trademarks
Answer: A
Page Ref: 14
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

46) Employees often have extensive knowledge of systems and can pose a greater risk than external attackers.
Answer: TRUE
Page Ref: 11
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

47) Penalties for hacking are significantly different if you are attempting to steal a million dollars or attempting to steal nothing of value.
Answer: FALSE
Page Ref: 11
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

48) Misappropriation of assets is an example of employee financial theft.
Answer: TRUE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

49) Downloading pornography can invoke a sexual harassment lawsuit.
Answer: TRUE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

50) If you are explicitly or implicitly allowed to use the resources that you're accessing on a company computer, you have authorization to do so.
Answer: TRUE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

51) Copyrights and patents are known as trade secrets.
Answer: FALSE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Moderate

52) You have access to your home page on a server. By accident, you discover that if you hit a certain key, you can get into someone else's files. You spend just a few minutes looking around. This is hacking.
Answer: TRUE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Moderate

53) The terms "intellectual property" and "trade secret" are synonymous.
Answer: FALSE
Page Ref: 13
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

54) Contract workers can also be considered a threat to a business.
Answer: TRUE
Page Ref: 15
Learning Objective: 1.3 Describe threats from employees and ex-employees
Difficulty: Easy

55) _____ is a generic term for "evil software."
A) Spyware
B) Payloads
C) Malware
D) Ransomware
Answer: C
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

56) _____ are programs that attach themselves to legitimate programs.
A) Viruses
B) Worms
C) Payloads
D) Direct-propagation worms
Answer: A
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

57) _____ are spread through e-mail with infected attachments.
A) Viruses
B) Worms
C) Direct-propagation worms
D) Distributed denial-of-service (DDoS) attacks
Answer: C
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

58) Some _____ can jump directly between computers without human intervention.
A) DDoS attacks
B) viruses
C) worms
D) direct-propagation worms
Answer: B
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

59) _____ take advantage of vulnerabilities in software.
A) Direct-propagation worms
B) Trojan horses
C) Blended threats
D) Bots
Answer: D
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

60) What is a payload?
A) Malicious software that blocks access to a system or data until money is paid to the attacker
B) A generic name for any "evil software"
C) A piece of code executed by a virus or a worm
D) A program that gives an attacker remote control of your computer
Answer: C
Page Ref: 18
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Difficult

61) A program that gives an attacker remote access control of your computer is known as _____.
A) a RAT
B) a Trojan horse
C) spyware
D) a cookie
Answer: A
Page Ref: 19
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

62) A _____ is a small program that, after installed, downloads a larger attack program.
A) rootkit
B) keystroke logger
C) downloader
D) Trojan horse
Answer: C
Page Ref: 19
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

63) Which of the following is a type of spyware?
A) Keystroke loggers
B) Rootkits
C) Spam
D) Downloaders
Answer: A
Page Ref: 20
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

64) Which of the following is FALSE about rootkits?
A) Rootkits are seldom caught by ordinary antivirus programs.
B) Rootkits take over the root account of a computer.
C) Rootkits use a root account's privileges to hide themselves.
D) Rootkits are typically less of a threat than are Trojan horses.
Answer: D
Page Ref: 20
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Difficult

65) Mobile code usually is delivered through _____.
A) e-mail
B) direct-propagation worms
C) webpages
D) spam
Answer: C
Page Ref: 20
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

66) _____ take advantage of flawed human judgment by convincing a victim to take actions that are counter to security policies.
A) Phishing attacks
B) Hoaxes
C) Social engineering attacks
D) Spear phishing attacks
Answer: C
Page Ref: 21
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

67) You receive an e-mail that seems to come from your bank. Clicking on a link in the message takes you to a website that seems to be your bank's website. However, the website is fake. This is called _____.
A) a hoax
B) social engineering
C) spear fishing
D) phishing
Answer: D
Page Ref: 21
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

68) You receive an e-mail that appears to come from a frequent customer. It contains specific information about your relationship with the customer. Clicking on a link in the message takes you to a website that seems to be your customer's website. However, the website is fake. This is an example of _____.
A) social engineering
B) spear fishing
C) phishing
D) a hoax
Answer: B
Page Ref: 21
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

69) Worms and viruses act much in the same way in how they propagate.
Answer: TRUE
Page Ref: 16
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

70) Nonmobile malware can be carried to a system as part of a payload.
Answer: TRUE
Page Ref: 18
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

71) A malicious payload is a program that hides itself by deleting a system file and taking on the system file's name.
Answer: FALSE
Page Ref: 19
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Moderate

72) Cookies are small text strings stored on your own personal computer.
Answer: TRUE
Page Ref: 20
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

73) Mobile code usually is contained in webpages.
Answer: TRUE
Page Ref: 20
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

74) The definition of spam is "unsolicited commercial e-mail."
Answer: TRUE
Page Ref: 21
Learning Objective: 1.4 Describe threats from malware writers
Difficulty: Easy

75) Most traditional external attackers were primarily motivated by _____.
A) the thrill of breaking in
B) making money through crime
C) stealing personal identity data
D) capturing thousands and thousands of credit card numbers
Answer: A
Page Ref: 22
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

76) ICMP Echo messages are often used in _____.
A) port scanning
B) IP address scanning
C) spoofing
D) DDoS attacks
Answer: B
Page Ref: 24
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Moderate

77) Sending packets with false IP source addresses is known as _____.
A) spear phishing
B) sabotage
C) IP address spoofing
D) hacking
Answer: C
Page Ref: 24
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Moderate

78) When a hacker sends a first round of probe packets to find hosts that are active, the attacker is sending _____ probes.
A) IP address scanning
B) a chain of attack
C) piggybacking
D) IP address spoofing
Answer: A
Page Ref: 24
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Moderate

79) Following someone through a secure door for access without using an authorized ID card or pass code is called _____.
A) piggybacking
B) a chain of attack
C) social engineering
D) shoulder surfing
Answer: A
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

80) Watching someone type their password in order to learn the password is called _____.
A) piggybacking
B) a chain of attack
C) social engineering
D) shoulder surfing
Answer: D
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

81) A(n) _____ attack attempts to make a server or network unavailable to serve legitimate users by flooding it with attack packets.
A) directly-propagating worm
B) virus
C) bot
D) DoS
Answer: D
Page Ref: 27
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

82) In a DoS attack, the botmaster is also known as a _____.
A) handler
B) hacker
C) hoax
D) rootkit
Answer: A
Page Ref: 28
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

83) Skilled hackers have dubbed a new type of hacker that is less sophisticated as _____.
A) Bug bounties
B) DoS attackers
C) script kiddies
D) black marketers
Answer: C
Page Ref: 29
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Moderate

84) Traditional hackers often focused on embarrassing a victim.
Answer: TRUE
Page Ref: 23
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

85) The act of implementing an attacker's exploit is called "spoofing the host."
Answer: FALSE
Page Ref: 25
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

86) In response to a chain of attack, victims can often trace the attack back to the final attack computer.
Answer: TRUE
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

87) In pretexting, an attacker sends an email claiming to be an employee for a certain company in order to ask for private information about that person.
Answer: FALSE
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

88) A distributed denial-of-service attach is the most common type of DoS attack.
Answer: TRUE
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Moderate

89) Social engineering is rarely used in hacking.
Answer: FALSE
Page Ref: 26
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

90) Script kiddies are typically hacker experts.
Answer: FALSE
Page Ref: 28
Learning Objective: 1.5 Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks
Difficulty: Easy

91) _____ are the most common external attacker who attack to make money illegally.
A) Hackers
B) Career criminal
C) Script kiddies
D) IT or security employer
Answer: B
Page Ref: 29
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

92) Many e-commerce companies will not ship to certain countries because of a high rate of consumer fraud. To get around this, criminal gangs engage _____ in the United States.
A) transshippers
B) APTs
C) black-market websites
D) IP address spoofing
Answer: A
Page Ref: 31
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

93) _____ programs reward researchers for finding vulnerabilities.
A) Transshipper
B) APT
C) Black-market website
D) Bug bounty
Answer: D
Page Ref: 31
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Moderate

94) _____ is a sophisticated computer hack usually perpetrated by a large, well-funded organization.
A) An APT
B) A black-market websites
C) A bug bounty
D) Carding
Answer: A
Page Ref: 31
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Moderate

95) Credit card theft is also known as _____.
A) extortion
B) click fraud
C) bug bounty
D) carding
Answer: D
Page Ref: 33
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Moderate

96) Which of the following is considered more serious than credit card number theft?
A) Bank account theft
B) Carding
C) Spoofing
D) Click fraud
Answer: A
Page Ref: 33
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

97) Which of the following is likely the most common criminal attack on individuals?
A) Bank account theft
B) Credit card number theft
C) Spoofing
D) Spam
Answer: B
Page Ref: 33
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Moderate

98) Most black markets deal in credit card and identity information.
Answer: TRUE
Page Ref: 31
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

99) Black-market websites are websites that offer stolen consumer information.
Answer: TRUE
Page Ref: 31
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

100) In click fraud, a criminal website owner creates a program so cookies are automatically downloaded to the computer's hard drive.
Answer: FALSE
Page Ref: 32
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

101) Black-market website programs reward researchers for finding vulnerabilities within their computer systems.
Answer: FALSE
Page Ref: 32
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

102) Identify theft can (and does) happen to individuals, but it is not a worry or risk that corporations have.
Answer: FALSE
Page Ref: 33
Learning Objective: 1.6 Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation
Difficulty: Easy

103) A company's website and Facebook pages may divulge information that competitors may seek out. This is known as _____.
A) public intelligence gathering
B) spoofing
C) bug bounty
D) carding
Answer: A
Page Ref: 35
Learning Objective: 1.7 Describe the types of attacks that could come from corporate competitors
Difficulty: Easy

104) Which of the following countries was NOT cited by the Foreign Economic Espionage in Cyberspace as being the most capable cyber actors actively engaged in economic espionage?
A) China
B) Russia
C) Iran
D) United States
Answer: D
Page Ref: 36
Learning Objective: 1.7 Describe the types of attacks that could come from corporate competitors
Difficulty: Easy

105) Illegally stealing a company's trade secrets is known as trade secret espionage.
Answer: TRUE
Page Ref: 35
Learning Objective: 1.7 Describe the types of attacks that could come from corporate competitors
Difficulty: Easy

106) Commercial espionage is limited to corporate competitors.
Answer: FALSE
Page Ref: 35
Learning Objective: 1.7 Describe the types of attacks that could come from corporate competitors
Difficulty: Easy

107) Cyberwar consists of computer-based attacks made by _____.
A) multinational corporations
B) state, regional, and local governments
C) national governments
D) private citizens
Answer: C
Page Ref: 36
Learning Objective: 1.8 Distinguish between cyberware and cyberterror
Difficulty: Moderate

108) In cyberterror, attackers are typically _____.
A) terrorists or groups of terrorists
B) national governments
C) large multinational corporations
D) Russian and/or Chinese citizens
Answer: D
Page Ref: 37
Learning Objective: 1.8 Distinguish between cyberware and cyberterror
Difficulty: Moderate

109) Russia, China, and Iran are quite active in cyberwar espionage.
Answer: TRUE
Page Ref: 36
Learning Objective: 1.8 Distinguish between cyberware and cyberterror
Difficulty: Easy

110) It is most common for cyberterrorists to recruit through face-to-face means.
Answer: FALSE
Page Ref: 37
Learning Objective: 1.8 Distinguish between cyberware and cyberterror
Difficulty: Easy