Test Bank

Chapter 1

Multiple Choice

1. _____ refers to unauthorized access to computer systems and digital devices utilizing the Internet, computers, and related technology.

A. Cybertrespass
B. Cybervandalism
C. Cybertheft
D. Cyberdeviance
E. Public order cybercrime

Answer: A (p. 4)

2. _____ refers to the virtual defacement of someone else's property.

A. Cybertrespass
B. Cybervandalism
C. Cybertheft
D. Cyberdeviance
E. Public order cybercrime

Answer: B (p. 5)

3. _____ involves the preying on children, adults, and the elderly through communications, information, and computer technologies.

A. Cyberdeviance
B. Public order cybercrime
C. Cybervice
D. Cyberpredation
E. None of the above

Answer: D (p. 8)

4. _____ is an act wherein an individual places a hoax call to emergency services that a crime or other critical incident that requires an emergency police response is underway.

A. Hacking
B. Website defacement
C. Swatting
D. Wardriving
E. None of the above

Answer: C (p. 8)

5. _____ refers to the use of the Internet, computers, and related technology to engage in conduct that violates social norms and expectations.

A. Cyberdeviance
B. Cybertrespass
C. Cybervandalism
D. Cyberpredation
E. None of the above

Answer: A (p. 9)

6. _____ involves the planning and executing of illegal business ventures online by either hierarchical groups or decentralized networks that often conduct their operations from more than one country.

A. Cyberdeviance
B. Cybervice
C. Cybervandalism
D. Organized cybercrime
E. None of the above

Answer: D (p. 10)

7. _____ is a cybercrime committed by individuals, groups, or nations in furtherance of some political goal or agenda.

A. Public order cybercrime
B. Political cybercrime
C. Cybervice
D. Organized cybercrime
E. None of the above

Answer: B (p. 11)

8. _____ is a crime committed via the Internet, computers, and related technology that offends the public's shared norms, morals, values, and customs.

A. Public order cybercrime
B. Political cybercrime
C. Cybervice
D. Organized cybercrime
E. None of the above

Answer: A (p. 9)

9. Cybercrime _____.

A. occurs on a far greater scale than traditional crime
B. transcends borders

C. has the ability to reach and affect individuals around the globe
D. all of the above
E. none of the above

Answer: D (p. 4)

10. Cyberspace has transformed and enhanced _____.

A. the way information is viewed, exchanged, and retrieved
B. the way in which individuals develop and maintain relationships
C. trade
D. the way money is moved
E. all of the above

Answer: E (p. 4)

Fill-in-the-blank

1. A _____ is an act that violates existing laws.

Answer: crime (p. 4)

2. A _____ is a person who violates the law.

Answer: criminal (p. 4)

3. A _____ is an illicit act that targets digital devices or is committed via the Internet, computers, and related technology.

Answer: cybercrime (p. 4)

4. A _____ is a person who utilizes the Internet, computers, and related technology to violate the law.

Answer: cybercriminal (p. 4)

5. _____ is the system of rules that regulate the public's actions and provide penalties for noncompliance.

Answer: Law (p. 4)

6. Those engaging in _____ drive around areas looking for vulnerable Wi-Fi networks to hack into.

Answer: wardriving (pp. 6–7)

7. _____ is the environment within which communications and other online activities through Internet-enabled digital devices take place.

Answer: Cyberspace (p. 4)

8. Cybercrime can fall under _____ proposed typologies.

Answer: six (p. 4)

9. _____ is the scientific study of the causes of crime, the scope of crime, the responses to crime by the public, media, social and political institutions, and criminal justice systems, and the ways to control, mitigate, and prevent crime.

Answer: Criminology (p. 12)

10. _____ is the study of cybercrime through the lens of criminology.

Answer: Cybercriminology (pp. 12–13)

True or False

1. Cybertheft refers to the stealing of personal information, medical information, financial information, and/or money via the Internet, computers, and related technology for personal or other use.

Answer: True (p. 6)

2. A cybervice is a crime committed via communications, information, and computer technologies against an individual with whom the perpetrator is communicating or has some form of relationship (real or imagined).

Answer: False (p. 7; this is an interpersonal cybercrime)

3. An example of an interpersonal cybercriminal is an online child sexual predator.

Answer: True (p. 8)

4. A cybervice is online behavior that is deemed immoral because it violates accepted codes of conduct.

Answer: True (p. 9)

5. An example of cyberdeviance is online paraphilia.

Answer: True (p. 9)

6. Biastophilia involves abnormal sexual desires obtained from violent assaults.

Answer: True (p. 9)

7. Impersonation fraud involves the manipulation of financial markets or the defrauding of investors through deception; it has also been perpetrated online.

Answer: False (p. 7; this is securities fraud)

8. Skimmers are electronic devices that are used to steal the personal information stored on users' credit or debit cards and to record the users' PIN numbers.

Answer: True (p. 10)

9. Impersonation fraud takes advantage of people's interest in important news stories and celebrities to get individuals to click on links that surreptitiously download malware onto a user's machine.

Answer: False (p. 7; this is a click bait scam)

10. Lulz is a term used to describe actions that occur at someone's expense to hurt the individual or create mayhem for enjoyment purposes.

Answer: True (p. 5)

Chapter 2

Multiple Choice

1. _____ is a Part 1 offense in the Uniform Crime Reporting program.

A. Forgery and counterfeiting
B. Fraud
C. Motor vehicle theft
D. Embezzlement
E. Drunkenness

Answer: C (p. 21)

2. _____ is a Part 1 offense in the Uniform Crime Reporting program.

A. Murder
B. Fraud
C. Embezzlement
D. Vagrancy
E. Gambling

Answer: A (p. 21)

3. _____ is a Part 2 offense in the Uniform Crime Reporting program.

A. Arson
B. Forcible rape
C. Robbery
D. Disorderly conduct
E. Burglary

Answer: D (p. 21)

4. _____ is a Part 2 offense in the Uniform Crime Reporting program.

A. Drug abuse violation
B. Arson
C. Aggravated assault

D. Larceny-theft
E. Motor vehicle theft

Answer: A (p. 21)

5. An example/examples of Part 1 offenses in the Uniform Crime Reporting program is/are _____.

A. arson
B. burglary
C. motor vehicle theft
D. larceny-theft
E. all of the above

Answer: E (p. 21)

6. The Federal Crime Data report includes data about _____.

A. human trafficking
B. hate crime
C. criminal computer intrusion
D. all of the above
E. none of the above

Answer: D (p. 22)

7. An example/examples of Group B offenses in the National Incident-Based Reporting System is/are _____.

A. embezzlement
B. extortion
C. bad checks
D. gambling
E. all of the above

Answer: C (p. 24)

8. An example/examples of Group A offenses in the National Incident-Based Reporting System is/are _____.

A. fraud
B. drunkenness
C. trespass of real property
D. disorderly conduct
E. all of the above

Answer: A (p. 24)

9. An example/examples of an official data source for U.S. crime statistics is/are _____.

A. the National Incident-Based Reporting System
B. the Uniform Crime Reporting program
C. the National Crime Victimization
D. all of the above
E. none of the above

Answer: D (pp. 21, 23, 27)

10. The _____ collects victimization data from several countries and victims' views on their own security.

A. Crime Survey for England and Wales
B. International Crime Victim Survey
C. National Crime Victimization Survey
D. National Computer Security Survey
E. National Incident-Based Reporting System

Answer: B (p. 33)

Fill-in-the-blank

1. _____ is viewed as one of the greatest economic and national security threats facing the United States.

Answer: Cybercrime (p. 20)

2. Since 1958, crime data in the United States have been made available in the FBI _____ publication.

Answer: Crime in the United States (p. 21)

3. The UCR Program in its traditional _____ includes data about Part 1 and Part 2 offenses.

Answer: Summary Reporting System (p. 21)

4. _____ can explain why individuals may choose not to report cybercrime.

Answer: Expected utility theory (p. 25)

5. The _____ provides guidance on how organizations can enhance their cybersecurity posture.

Answer: NIST Cybersecurity Framework (p. 30)

6. The _____ is an official crime measurement tool in Canada that collects information about victimization.

Answer: General Social Survey (p. 33)

7. A _____ asks respondents to report on their own participation in criminal activity.

Answer: self-report survey (p. 34)

8. The _____ requires that only the most serious crime of multiple offenses be recorded in the Uniform Crime Reporting program.

Answer: hierarchy rule (p. 22)

9. The _____ collected information from U.S. businesses about cybercrimes they were subjected to.

Answer: National Computer Security Survey (p. 29)

10. _____ is the probability of harm or damage or threat of harm or damage from a security threat because of vulnerabilities.

Answer: Risk (p. 34)

True or False

1. Part 1 offenses of the Uniform Crime Reporting program include only property crimes.

Answer: False (p. 21; violent crimes and property crimes are included)

2. Part 2 offenses of the Uniform Crime Reporting program include violent crimes and property offenses.

Answer: False (p. 21; violent crimes and property crimes are included in Part 1 offenses)

3. Of the offenses listed in Part 1 of the Uniform Crime Reporting program, property crimes are considered the most severe.

Answer: False (p. 21; violent crimes are considered the most severe)

4. Arson can be classified as a violent crime or a property crime.

Answer: True (p. 21)

5. If multiple offenses are committed in one criminal incident, only the most serious of the offenses is recorded in the Uniform Crime Reporting program.

Answer: True (p. 22)

6. Unlike the Crime in the United States publication, the National Incident-Based Reporting System does not apply estimation procedures for missing crime data by participating and nonparticipating jurisdictions.

Answer: True (p. 23)

7. Cybercrime is not listed as part of Group A or Group B offenses, but it is recorded in the National Incident-Based Reporting System.

Answer: True (p. 23)

8. The Crime Survey for England and Wales is distributed to households to obtain information about the dark figure of crime.

Answer: True (p. 28)

9. An international measurement tool exists that validly and reliably measures cybercrime against individuals and businesses.

Answer: False (p. 31; there is no such tool)

10. Cybersecurity companies' surveys provide valid and reliable cybercrime data.

Answer: False (p. 30)