**UNIT 6**

**Cyber Crime and Cyber Laws**

1. Which of the following is not a type of cyber crime?  
a) Data theft  
b) Forgery  
c) Damage to data and systems  
d) Installing antivirus for protection

Answer: d  
Explanation: Cyber crimes are one of the most threatening terms that is an evolving phase. It is said that major percentage of the World War III will be based on cyber-attacks by cyber armies of different countries.

2. Cyber-laws are incorporated for punishing all criminals only.  
a) True  
b) False

Answer: b  
Explanation: Cyber-laws were incorporated in our law book not only to punish cyber criminals but to reduce cyber crimes and tie the hands of citizens from doing illicit digital acts that harm or damage other’s digital property or identity.

3. Cyber-crime can be categorized into \_\_\_\_\_\_\_\_ types.  
a) 4  
b) 3  
c) 2  
d) 6

Answer: c  
Explanation: Cyber crime can be categorized into 2 types. These are peer-to-peer attack and computer as weapon. In peer-to-peer attack, attackers target the victim users; and in computer as weapon attack technique, computers are used by attackers for a mass attack such as illegal and banned photo leak, IPR violation, pornography, cyber terrorism etc.

4. Which of the following is not a type of peer-to-peer cyber-crime?  
a) Phishing  
b) Injecting Trojans to a target victim  
c) MiTM  
d) Credit card details leak in deep web

Answer: d  
Explanation: Phishing, injecting Trojans and worms to individuals comes under peer-to-peer cyber crime. Whereas, leakage of credit card data of a large number of people in deep web comes under computer as weapon cyber-crime.

5. Which of the following is not an example of a computer as weapon cyber-crime?  
a) Credit card fraudulent  
b) Spying someone using keylogger  
c) IPR Violation  
d) Pornography

Answer: b  
Explanation: DDoS (Distributed Denial of Service), IPR violation, pornography are mass attacks done using a computer. Spying someone using keylogger is an example of peer-to-peer attack.

6. Which of the following is not done by cyber criminals?  
a) Unauthorized account access  
b) Mass attack using Trojans as botnets  
c) Email spoofing and spamming  
d) Report vulnerability in any system

Answer: d  
Explanation: Cyber-criminals are involved in activities like accessing online accounts in unauthorized manner; use Trojans to attack large systems, sending spoofed emails. But cyber-criminals do not report any bug is found in a system, rather they exploit the bug for their profit.

7. What is the name of the IT law that India is having in the Indian legislature?  
a) India’s Technology (IT) Act, 2000  
b) India’s Digital Information Technology (DIT) Act, 2000  
c) India’s Information Technology (IT) Act, 2000  
d) The Technology Act, 2008

Answer: c  
Explanation: The Indian legislature thought of adding a chapter that is dedicated to cyber law. This finally brought India’s Information Technology (IT) Act, 2000 which deals with the different cyber-crimes and their associated laws.

8. In which year India’s IT Act came into existence?  
a) 2000  
b) 2001  
c) 2002  
d) 2003

Answer: a  
Explanation: On 17th Oct 2000, the Indian legislature thought of adding a chapter that is dedicated to cyber law, for which India’s Information Technology (IT) Act, 2000 came into existence.

9. What is the full form of ITA-2000?  
a) Information Tech Act -2000  
b) Indian Technology Act -2000  
c) International Technology Act -2000  
d) Information Technology Act -2000

Answer: d  
Explanation: Information Technology Act -2000 (ITA-2000), came into existence on 17th Oct 2000, that is dedicated to cyber-crime and e-commerce law in India.

10. The Information Technology Act -2000 bill was passed by K. R. Narayanan.  
a) True  
b) False

Answer: b  
Explanation: The bill was passed & signed by Dr. K. R. Narayanan on 9th May, in the year 2000. The bill got finalised by head officials along with the Minister of Information Technology, Dr. Pramod Mahajan.

11. Under which section of IT Act, stealing any digital asset or information is written a cyber-crime.  
a) 65  
b) 65-D  
c) 67  
d) 70

Answer: a  
Explanation: When a cyber-criminal steals any computer documents, assets or any software’s source code from any organization, individual, or from any other means then the cyber crime falls under section 65 of IT Act, 2000.

12. What is the punishment in India for stealing computer documents, assets or any software’s source code from any organization, individual, or from any other means?  
a) 6 months of imprisonment and a fine of Rs. 50,000  
b) 1 year of imprisonment and a fine of Rs. 100,000  
c) 2 years of imprisonment and a fine of Rs. 250,000  
d) 3 years of imprisonment and a fine of Rs. 500,000

Answer: d  
Explanation: The punishment in India for stealing computer documents, assets or any software’s source code from any organization, individual, or from any other means is 3 years of imprisonment and a fine of Rs. 500,000.

13. What is the updated version of the IT Act, 2000?  
a) IT Act, 2007  
b) Advanced IT Act, 2007  
c) IT Act, 2008  
d) Advanced IT Act, 2008

Answer: c  
Explanation: In the year 2008, the IT Act, 2000 was updated and came up with a much broader and precise law on different computer-related crimes and cyber offenses.

14. In which year the Indian IT Act, 2000 got updated?  
a) 2006  
b) 2008  
c) 2010  
d) 2012

Answer: b  
Explanation: In the year 2008, the IT Act, 2000 was updated and came up with a much broader and precise law on different computer-related crimes and cyber offenses.

15. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?  
a) Cracking or illegally hack into any system  
b) Putting antivirus into the victim  
c) Stealing data  
d) Stealing hardware components

Answer: a  
Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law says that cracking or illegally hacking into any victim’s computer is a crime. It covers a wide range of cyber-crimes under this section of the IT Act.

16 Which of the following is not an example of a computer as weapon cyber-crime?

A Credit card fraudulent

B Spying someone using keylogger

C IPR Violation

D None of the above

Answer: Spying someone using keylogger

17 Which of the following is not done by cyber criminals?

A Unauthorized account access

B Mass attack using Trojans as botnets

C Email spoofing and spamming

D Report vulnerability in any system

Answer: Report vulnerability in any system

18 Which of the following is not a factor in securing the environment against an attack on security?

A The education of the attacker

B The system configuration

C The network architecture

D The business strategy of the company

Answer: To identify live systems

19 What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?

A Cracking or illegally hack into any system

B Putting antivirus into the victim

C Stealing data

D Stealing hardware components

Answer: Cracking or illegally hack into any system

1. Accessing computer without prior authorization is a cyber-crimes that come under \_\_\_\_\_\_\_  
a) Section 65  
b) Section 66  
c) Section 68  
d) Section 70

Answer: b  
Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law says that without prior authorization or permission, if any individual access any computer system, it is a cyber-crime.

2. Cracking digital identity of any individual or doing identity theft, comes under \_\_\_\_\_\_\_\_\_\_ of IT Act.  
a) Section 65  
b) Section 66  
c) Section 68  
d) Section 70

Answer: b  
Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law (as IT Act, 2008) says that if any individual steals the identity or misuse any victim’s identity for his/her own profit, it is a cyber-crime.

3. Accessing Wi-Fi dishonestly is a cyber-crime.  
a) True  
b) False

Answer: a  
Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law (as IT Act, 2008) says that if any individual access anyone’s Wi-Fi network without the permission of the owner or for doing a malicious activity, it is a cyber-crime.

4. Download copy, extract data from an open system done fraudulently is treated as \_\_\_\_\_\_\_\_\_  
a) cyber-warfare  
b) cyber-security act  
c) data-backup  
d) cyber-crime

Answer: d  
Explanation: Download copy, extract data from an open system done fraudulently is treated as according to section 66 of the Indian IT Act.

5. Any cyber-crime that comes under section 66 of IT Act, the accused person gets fined of around Rs \_\_\_\_\_\_\_\_  
a) 2 lacs  
b) 3 lacs  
c) 4 lacs  
d) 5 lacs

Answer: d  
Explanation: Any cyber-crime that comes under section 66 of the Indian IT Act, the person accused of such cyber-crime gets fined of around five lacs rupees.

6. How many years of imprisonment can an accused person face, if he/she comes under any cyber-crime listed in section 66 of the Indian IT Act, 2000?  
a) 1 year  
b) 2 years  
c) 3 years  
d) 4 years

Answer: c  
Explanation: Any cyber-crime that comes under section 66 of the Indian IT Act, the person accused of such cyber-crime gets fined of around five lacs rupees and 3 years of imprisonment.

7. Any digital content which any individual creates and is not acceptable to the society, it’s a cyber-crime that comes under \_\_\_\_\_\_\_\_\_ of IT Act.  
a) Section 66  
b) Section 67  
c) Section 68  
d) Section 69

Answer: b  
Explanation: Any digital content which is either lascivious is not acceptable by the society or viewers or that digital item corrupts the minds of the audience, then the creator of such contents falls under the cyber-crime of section 67 of the Indian IT Act.

8. IT Act 2008 make cyber-crime details more precise where it mentioned if anyone publishes sexually explicit digital content then under \_\_\_\_\_\_\_\_\_\_\_ of IT Act, 2008 he/she has to pay a legitimate amount of fine.  
a) section 67-A  
b) section 67-B  
c) section 67-C  
d) section 67-D

Answer: a  
Explanation: IT Act 2008 makes cyber-crime details more precise where it mentioned if anyone publishes sexually explicit digital content then under section 67 – A he/she has to pay a legitimate amount of fine.

9. If anyone publishes sexually explicit type digital content, it will cost that person imprisonment of \_\_\_\_\_\_\_\_\_ years.  
a) 2  
b) 3  
c) 4  
d) 5

Answer: d  
Explanation: IT Act 2008 make cyber-crime details more precise where it mentioned if anyone publishes sexually explicit digital content then under section 67 – A he/she has to pay a legitimate amount of fine and imprisonment of five years.

10. Using spy cameras in malls and shops to capture private parts of any person comes under \_\_\_\_\_\_\_ of IT Act, 2008.  
a) Section 66  
b) Section 67  
c) Section 68  
d) Section 69

Answer: b  
Explanation: Using of spy cameras in malls and shops to capture private parts of any person, without the concern of that victim, then it comes under section 67 of IT Act, 2008 as a punishable offense.

11. Using spy cameras in malls and shops to capture private parts of any person comes under section 67 of IT Act, 2008 and is punished with a fine of Rs. 5 Lacs.  
a) True  
b) False

Answer: a  
Explanation: Using of spy cameras in malls and shops to capture private parts of any person, without the concern of that victim, then it comes under section 67 of IT Act, 2008 where the person doing such crime is punished with a fine of Rs. 5 Lacs.

12. Using of spy cameras in malls and shops to capture private parts of any person comes under section 67 of IT Act, 2008 and is punished with imprisonment of \_\_\_\_\_\_\_\_\_\_\_  
a) 2 years  
b) 3 years  
c) 4 years  
d) 5 years

Answer: b  
Explanation: Using of spy cameras in malls and shops to capture private parts of any person, without the concern of that victim, then it comes under section 67 of IT Act, 2008 where the person doing such crime is punished with imprisonment of 3 years.

13. Misuse of digital signatures for fraudulent purposes comes under \_\_\_\_\_\_\_\_\_\_ of IT Act.  
a) section 65  
b) section 66  
c) section 71  
d) section 72

Answer: d  
Explanation: Cyber-criminals and black hat hackers do one common form of cyber-crime that is a misuse of digital signatures. The law for this fraudulent act comes under section 72 of the Indian IT Act.

14. Sending offensive message to someone comes under \_\_\_\_\_\_\_\_\_\_\_\_\_ of the Indian IT Act \_\_\_\_\_\_  
a) section 66-A, 2000  
b) section 66-B, 2008  
c) section 67, 2000  
d) section 66-A, 2008

Answer: d  
Explanation: Sending an offensive message, emails o any digital content through an electronic medium to your recipient is a punishable offense that comes under section 66 – A of the Indian IT Act, 2008.

15. Stealing of digital files comes under \_\_\_\_\_\_\_\_\_\_ of the Indian IT Act.  
a) section 66-A  
b) section 66-B  
c) section 66-C  
d) section 66-D

Answer: c  
Explanation: Stealing of digital files, e-documents from any system or cloud or electronic device is a punishable offense that comes under section 66 – C of the Indian IT Act.

16. Section 79 of the Indian IT Act declares that any 3rd party information or personal data leakage in corporate firms or organizations will be a punishable offense.  
a) True  
b) False

Answer: a  
Explanation: Section 79 of the Indian IT Act covers some of the corporate and business laws circulating technologies and cyberspace; declares that any 3rd party information or personal data leakage in corporate firms or organizations will be a punishable offense.