

(Multiple Choice type Questions)

Cyber law and Security Policy

1) The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organisation is termed:

- (a) Cyberspace
- (b) Cyber stalking**
- (c) Pornography
- (d) None of these

2) Which of the following is a cybercrime?

- (a) Hacking
- (b) Worm attack
- (c) Virus attack
- (d) All of these**

3) Refers to email that appears to have been originated from one source when it was actually sent from another source.

- (a) Email bombing
- (b) Email spoofing**
- (c) Email spamming
- (d) None of these

4) In cyber law terminology 'DoS' means:

- (a) Denial of Service**
- (b) Disc operating System
- (c) Distant operator Service
- (d) None of these

5) refers to sending email to thousands and thousands of users-similar to a chain letter.

- (a) Email spamming**
- (b) Email bombing
- (c) Trojan attack
- (d) None of these

6) By hacking web server taking control on another person's website called as web

- (a) Spoofing
- (b) Hijacking**
- (c) Spamming
- (d) None of these

7) **Programs that multiply like viruses but spread from computer to computer are called as:**

- (a) Worms**
- (b) Virus
- (c) Boot
- (d) None of these

8) **Section 66F of IT Act deals with**

- a) Cyber stalking
- b) Email bombing
- c) Child pornography
- d) Cyber terrorism**

9) **Act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity is called**

- a) email bombing
- b) Spamming
- c) Cyber stalking
- d) Phishing**

10) **Use of electronic messaging systems to send unsolicited bulk messages are called**

- a) email bombing
- b) Spamming**
- c) Cyber stalking
- d) Phishing

11) **The practice of making a transmission appears to come from an authorized user.**

- a) Hacking
- b) Spoofing**
- c) Spamming
- d) spamdexing

12) **Which section of IT Act covers most of the common crimes arising out of “Unauthorised Access”**

- a) Section 66**
- b) Section 67
- c) Section 73
- d) Section 74

13) **In cyber law terminology ‘DDoS’ means:**

- (a) Distributed Denial of Service**
- (b) Disc operating System
- (c) Distant operator Service

(d)None of these

14) The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organisation is termed:

- (a)Cyberspace
- (b)Cyber stalking**
- (c)Pornography
- (d)None of these

15) Programs that multiply like viruses but spread from computer to computer are called as:

- (a)Worms**
- (b)Virus
- (c)Boot
- (d)None of these

16) Section 66C of IT Act deals with

- a) Cyber stalking
- b) Email bombing
- c) Child pornography
- d) Punishment for Identity Theft**

17) Section-66E of IT Act deals with

- a) Punishment for violation of Privacy.**
- b) Spamming
- c) Cyber stalking
- d) Phishing

18) India's first cyber police station

- a) Delhi
- b) Bangalore**
- c) Chennai
- d) Mumbai

19) Information Technology Amendment Act form in year

- a) 2000
- b) 2001
- c) 2008**
- d) 2009

20) Punishment for sending offensive messages through communication service are belong

- a) 66A**
- b) 65
- c) 66B
- d) 66F

21) Vishing is mean for

- a) SMS phishing
- b) Voice phishing**
- c) Phishing
- d) All the above.

22) This is a program in which malicious or harmful code is contained inside apparently harmless programming or data.

- a) War dialer
- b) Spam trap
- c) Trojan horse**
- d) Email

23) Which of the following is the most important to install and keep up to date on your personal computer?

- a) Anti-virus and anti-spyware software
- b) A Firewall
- c) Operating system updates
- d) All of the above must be installed and kept up to date**

24) What is "phishing?"

- a) "Spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords**
- b) A type of computer virus
- c) An example of a strong password
- d) None of the above

25) What type of attack relies on the trusting nature of employees and the art of deception?

- a) Social Engineering**
- b) Fraud
- c) Phishing
- d) Dumpster Diving

26) This is a document that states in writing how a company plans to protect the company's physical and IT assets.

- a) Data Encryption Standard
- b) Security policy**
- c) Public key certificate
- d) Access control list

27) Which of the following are examples of Mobile virus:

- a) Skull Trojan
- b) Cabir Worm
- c) Mosquito Trojan
- d) All of the above.**

28) Amendments to the Indian IT act which are new offences are added:

- a) 67A (Sexually explicit content)
- b) 67B (Child pornography)
- c) 66F (Cyber terrorism).
- d) All of the above.**

29) Which are the following is not part of cyber space:

- a) Computer
- b) Computer network
- c) Website
- d) Calculator**

30) Tampering of computer source code cover in:

- a) Section 66A
- b) Section 66B
- c) Section 65**
- d) Section 67

Some common Cyber crime offences and punishment:

Sections / Sub Section	Imprisonment	Fine
Section – 65 (Tampering of Source Code)	Up to 3 years and /or fine both	Up to 2 Lac
Section– 66A: Punishment for Sending offensive messages	Up to 3 years and with fine both	No ceiling
Section- 66B: Punishment for dishonestly receiving stolen computer resource or devices.	Up to 3 years and / or fine or both	1 Lac
Section– 66C: Punishment for Identity Theft	Up to 3 years and fine	Up to 1 Lac

Section-66E: Punishment for violation of Privacy.	Up to 3 years and / or fine	Up to 2 Lac
Section-66F: Punishment for cyber terrorism	Imprisonment for life. No fine	
Section – 67A (Punishment for publishing or transmitting material containing sexually explicit act in electronic form.	1 st conviction :Up to 5 years and with fine both. 2 nd conviction:Up to 7 years and also with fine both.	Up to 10 Lac Up to 10 Lac
Section – 67B (Punishment for publishing or transmitting of material depicting children in sexually explicit act.	1 st conviction: Up to 5 years and with fine both. 2 nd convictionUp to 7 years and also with fine both.	Up to 10 Lac Up to 10 Lac