MULTIPLE CHOICE QUESTIONS UNIT 1: INTRODUCTION TO CYBER SECURITY

1) "IoT" stand for in the context of cybersecurity ……..

[a] Internet of Things [b] Input-Output Technology [c] Information Overload Toolkit [d] International Online Tracking

2. VPN (Virtual Private Network) primarily provide …….

[a] Firewall protection [b] Anonymity on the internet

[c] Enhanced download speed [d] Video streaming services

3. The primary purpose of a firewall in cybersecurity ……

[a] Protecting against physical break-ins [b]Monitoring web traffic

[c] Encrypting data transmissions [d] Filtering and controlling network traffic

4. The term for the practice of sending fraudulent emails to deceive individuals into revealing personal information …….

[a] Malware [b] Hacking

[c] Social engineering [d] Encryption

5. What is cyberspace? ……..

[a] A physical location

[b] A virtual environment created by interconnected computers

[c] An alternate reality [d] A fictional concept

6. The primary purpose of a VPN (Virtual Private Network) ……..

[a] To play online games [b] To secure and anonymize internet connections

[c] To access outer space [d] To send physical mail

7. The term for the deliberate spreading of false information online to deceive and manipulate people ……..

[a] Cyberwarfare [b] Cyberbullying

[c] Disinformation [d] Cyber espionage

8. The "URL" stand for in the context of web addresses ……

[a] Uniform Resource Locator [b] Universal Resource Language

[c] Unidentified Real-time Link [d] Universal Remote Location

9. The common cybersecurity threat in cyberspace ……..

[a] Solar flares [b] Hurricanes

[c] Malware [d] Earthquakes

10. The "ISP" stand for in the context of internet services ……..

[a] Internet Security Protocol [b] Internet Speed Provider

[c] Internet Service Provider [d] Internet Search Platform

11. The protocol is commonly used for sending emails in cyberspace ……

[a] HTTP (Hypertext Transfer Protocol) [b] SMTP (Simple Mail Transfer Protocol)

[c] VPN (Virtual Private Network) [d] FTP (File Transfer Protocol)

12. The primary goal of cybersecurity in cyberspace …….

[a] To facilitate online shopping

[b] To eliminate all online risks

[c] To protect digital information and systems from threats

[d] To increase social media engagement

13. HTML stand for in web technology …….

[a] Hyperlink Text Markup Language [b] Hypertext Transfer Protocol

[c] Hypertext Markup Language [d] High-Tech Multimedia Language

14. The programming language is primarily used for client-side scripting in web Development ……..

[a] Python [b] Java

[c] JavaScript [d] PHP

15. The role of a web server in the context of web technology ……

[a] Rendering web pages in browsers [b] Storing user data on the internet

[c] Hosting and serving web content to clients [d] Protecting against viruses and malware

16. The technology allows for real-time, bidirectional communication between a web server and a client browser ……

[a] HTML [b] CSS

[c] AJAX (Asynchronous JavaScript and XML) [d] WebSockets

17. The primary function of a web browser ……..

[a] To create websites [b] To host websites

[c] To access and display web content [d] To manage database systems

18. The protocol is commonly used for secure data transmission over the internet ……

[a] HTTP [b] HTTPS

[c] FTP [d] SMTP

19. The main purpose of an IP address in internet communication ……..

[a] To specify a website's designed m

[b] To identify the physical location of a server

[c] To uniquely identify devices on a network

[d] To encrypt data transmissions

20. The internet protocol is used for sending and receiving emails ……

[a] HTTP [b] FTP

[c] SMTP [d] DNS

21. The term for the practice of obtaining sensitive information, such as passwords or credit card numbers, by disguising as a trustworthy entity in an electronic communication …….

[a] Hacking [b] Encryption

[c] Phishing [d] Spamming

22. The internet browser is developed by the Mozilla Foundation ……..

[a] Chrome [b] Safari

[c] Firefox [d] Edge

23. The technology is commonly used to create and format web documents ……..

[a] TCP/IP [b] HTML (Hypertext Markup Language)

[c] VPN (Virtual Private Network) [d] JavaScript

24. The primary purpose of a web browser ……

[a] To host websites [b] To send emails

[c] To access and display web content [d] To manage computer files

25. The term for a clickable link on a web page that takes to another web page or resource

……

[a] Web marker [b] Hyperlink

[c] Web token [d] Internet shortcut

26. When was the first successful message sent over ARPANET, the precursor to the modern internet …….

[a] 1960 [b] 1969 [c] 1975 [d] 1985

27. The technology was used to create the first web browser, called "World Wide Web ……..

[a] Mosaic [b] Netscape Navigator

[c] Lynx [d]HTML (Hypertext Markup Language)

28. The term for the practice of connecting different computer networks to form the internet

[a] Internetworking [b] Intranetworking

[c] Interconnecting [d] Intriguing

29. The primary purpose of the original ARPANET, the precursor to the internet …….

[a] To support military communication during wartime

[b] To provide free public internet access

[c] To enable global e-commerce

[d] To serve as a platform for social networking

30. The organization is responsible for managing the allocation of IP addresses and domain names on the Internet ……

[a] ICANN [b] UNESCO

[c] WHO [d] NSA

UNIT 2: CYBER CRIME AND CYBER LAW

1. What is cybercrime? ……

[a] A form of virtual reality gaming

[b] Illegal activities conducted over the internet

[c] A type of computer hardware

[d] Online etiquette guidelines

2. Which of the following is an example of a cybercrime? ……

[a] Playing online video games [b] Sending emails to friends

[c] Hacking into someone's bank account [d] Posting photos on social media

3. The term for a cybercrime in which criminals use deceptive emails or websites to trick individuals into revealing personal information ……..

[a] Phishing [b] Spamming

[c] Hacking [d] Viral marketing

4. The cybercrime involves illegally copying and distributing copyrighted digital material, such as music or movies ……

[a] Hacking [b] Phishing

[c] Cyberbullying [d] Digital piracy

5. What is a "botnet" in the context of cybercrime? …….

[a] A type of computer virus

[b] A network of infected computers controlled by a remote attacker

[c] A secure online shopping website

[d] A social media platform

6. Which of the following is a form of cybercrime that involves harassing, threatening, or targeting individuals online? ……

[a] Hacking [b] Digital piracy

[c] Cyberbullying [d] Phishing

7. The primary motive behind cyber extortion, a common form of cybercrime ……..

[a] Gaining notoriety [b] Seeking revenge

[c] Financial gain [d] Political activism

8. The term for a cybercrime that involves spreading false information about someone with the intent to harm their reputation ……..

[a] Cyberstalking [b] Cyberbullying

[c] Cyberdefamation [d] Cyber hacking

9. The cyber law primarily deal with …….

[a] Laws related to outer space

[b] Legal issues involving computer networks and the internet

[c] Environmental regulations

[d] Criminal law

10. The primary goal of cyber law …….

[a] To prevent all forms of online communication

[b] To regulate social media usage

[c] To establish legal guidelines for internet-related activities

[d] To promote online anonymity

11. The area of cyber law deals with intellectual property rights, copyright infringement, and digital piracy ……

[a] Cybersecurity law [b] Information technology law

[c] Cybercrime law [d] Intellectual property law

12. Type of cybercrime involves unauthorized access to computer systems or networks with the intent to steal, alter, or destroy data ……...

[a] Cyberbullying [b] Hacking

[c] Online fraud [d] Phishing

13. The primary objective of cybercrimes categorized as "financial cybercrimes" ……

[a] Spreading malware [b] Gaining unauthorized access to systems

[c] Financial gain or theft [d] Cyberbullying

14. The term for cybercrimes that involve spreading false or misleading information with the intent to damage a person's reputation or credibility ……

[a] Online fraud [b] Cyberbullying

[c] Defamation [d] Hacking

15. The Type of cybercrime involves distributing malicious software that can damage or compromise computer systems or data …….

[a] Hacking [b] Phishing

[c] Malware distribution [d] Identity theft

16. The term for cybercrimes that target critical infrastructure systems, such as power grids, water supplies, or transportation networks? ……...

[a] Cyberbullying [b] Cyberterrorism

[c] Online fraud [d] Phishing

17. What is financial fraud? …….

[a] Legal financial transactions

[b] Unintentional financial errors

[c] Intentional deceptive practices for financial gain

[d] Financial assistance for those in need

18. Which type of financial fraud involves creating fake financial documents or records to deceive others for financial gain? ……...

[a] Identity theft [b] Money laundering

[c] Forgery [d] Tax evasion

19. Which type of financial fraud involves intentionally providing false or misleading information on tax returns to reduce tax liability? ……

[a] Tax evasion [b] Tax compliance

[c] Tax transparency [d] Tax credits

20. What is "malware"?

[a] A type of computer hardware

[b] A form of online shopping

[c] Malicious software designed to harm or infiltrate computer systems

[d] A computer programming language

21. Which type of malware disguises itself as legitimate software but contains malicious code that can harm your computer or steal your data? ……

[a] Virus [b] Worm

[c] Trojan Horse [d] Spyware

22. What is "ransomware"? …….

[a] Malware that records your keystrokes

[b] A type of online shopping platform

[c] Malware that encrypts your files and demands a ransom for their release

[d] A type of antivirus software

23. The remedial measures in cybersecurity primarily focused on …….

[a] Preventing future cyberattacks

[b] Detecting ongoing cyberattacks

[c] Responding to and recovering from cyberattacks

[d] Promoting ethical hacking

24. The primary purpose of the Information Technology Act of 2000 in India

[a] To regulate the sale of electronic devices

[b] To promote the use of traditional paper-based documents

[c] To provide legal recognition to electronic transactions and digital signatures

[d] To ban the use of computers for financial transactions

25. Which amendment to the Information Technology Act in 2008 introduced provisions related to data protection and privacy in India? ……. [a] Amendment Act of 2005 [b] Amendment Act of 2006

[c] Amendment Act of 2008 [d] Amendment Act of 2010

26. Which amendment to the IT Act introduced provisions related to the punishment for cyberterrorism and cyberattacks on critical infrastructure a …….

[a] Amendment Act of 2005 [b]Amendment Act of 2006

[c]Amendment Act of 2008 [d]Amendment Act of 2010

27. The purpose of the IT (Amendment) Act of 2008's provision related to the blocking of websites …….

[a]To promote free access to all websites

[b]To restrict access to specific websites for security reasons

[c]To ban all online content

[d]To limit access to government websites only

28. Which government agency is responsible for enforcing the provisions of the IT Act 2000 and its amendments in India? ……

[a]Ministry of Finance

[b]Ministry of Health and Family Welfare

[c]Ministry of Electronics and Information Technology

[d]Ministry of Education

29. The legal framework that governs the use of electronic signatures and records in India.

[a] Electronic Transactions Act [b]Electronic Records Act

[c]Information Technology Act [d] Cybersecurity and Privacy Act

30. The legal concept allows individuals to remain silent and avoid self-incrimination when questioned by law enforcement in cybercrime cases ……

[a] Search and seizure [b]Habeas corpus

[c]Right to privacy [d]Right to remain silent

UNIT 3: SOCIAL MEDIA OVERVIEW AND SECURITY

1. The primary purpose of social media …….

[a] Entertainment [b] Communication

[c] Online shopping [d] Weather updates

2. Which social media platform is known for its character limit per tweet? ……..

[a] Facebook [b] Instagram

[c] Twitter [d] LinkedIn

3. The social media platform is primarily focused on professional networking and job searching ……

[a] Facebook [b] Instagram

[c] Twitter [d] LinkedIn

4. The term for content that spreads rapidly and widely on social media ……

[a] Popular content [b] Trending content

[c] Viral content [d] Engaging content

5. What is a "hashtag" used for in social media? ……

[a] To separate paragraphs [b] To mark the beginning of a post

[c] To categorize and link content [d] To hide content from certain users

6. The primary purpose of the "report" or "flag" feature on social media platforms ……..

[a] To send direct messages [b] To make posts private

[c] To report inappropriate content [d] To start a video call

7. The security measure helps protect social media accounts from unauthorized access …….

[a] Using weak passwords

[b] Enabling two-factor authentication (2FA)

[c] Sharing login credentials with friends

[d] Logging in from public computers

8. The potential consequence of oversharing personal information on social media ……

[a] Increased privacy [b] Enhanced security

[c] Identity theft [d] Better online relationships

9. The primary purpose of social networks ……..

[a] Online shopping [b] Business promotion

[c] Global connectivity and communication [d] Entertainment

10. The social network is known for its emphasis on professional networking and job searching ……..

[a] Facebook [b] Instagram [c] Twitter [d] LinkedIn

11. The following is not a popular social networking platform …….

[a] Snapchat [b] Pinterest

[c] YouTube [d] eBay

12. The term for online communities built around shared interests or hobbies on social networks ……

[a] Online clubs [b] Virtual societies

[c] Social groups [d] Online communities

13. The social network is primarily focused on short video content and trends …….

[a] Facebook [b] Instagram

[c] TikTok [d] LinkedIn

14. The type of social media platform primarily focuses on sharing short, 140-character messages called "tweets" ……

[a] Social networking sites [b] Microblogging platforms

[c] Multimedia sharing platforms [d] Professional networking sites

15. The type of social media platform is known for its emphasis on visual content, such as photos and videos ……..

[a] Social networking sites [b] Microblogging platforms

[c] Multimedia sharing platforms [d] Social bookmarking sites

16. The type of social media platform is designed for professionals to connect with colleagues, build their network, and seek job opportunities ……

[a] Social networking sites [b] Microblogging platforms

[c] Multimedia sharing platforms [d] Professional networking sites

17. The type of social media platform focuses on enabling users to discover and share web content with others through bookmarks or links ……..

[a] Social networking sites [b] Microblogging platforms

[c] Multimedia sharing platforms [d] Social bookmarking sites

18. The type of social media platform is primarily used for connecting with friends, family, and acquaintances, and sharing personal updates ……..

[a] Social networking sites [b] Microblogging platforms [c]

Multimedia sharing platforms [d] Professional networking sites

19. The main purpose of Pinterest as a social media platform …….

[a] Sharing short text updates [b] Posting photos and videos

[c] Discovering and sharing visual inspiration [d] Professional networking

20. The primary purpose of LinkedIn as a social media platform ……..

[a] Sharing personal updates and photos

[b] Discovering and sharing recipes

[c] Networking with professionals and seeking job opportunities

[d] Posting short video content

21. The primary function of YouTube as a social media platform ……

[a] Sharing short text updates [b] Posting photos and videos

[c] Networking with professionals [d] Live streaming music concerts

22. The primary purpose of social media monitoring ……..

[a] Creating engaging content [b] Managing advertising campaigns

[c] Tracking and analysing online conversations [d] Building a large follower base

23. The term describes the process of monitoring social media channels for mentions of a brand, product, or keyword …….

[a] Social listening [b] Social engagement

[c] Social posting [d] Social networking

23. Social media metric measures the number of times a post is shared by users …….

[a] Impressions [b] Click-through rate (CTR)

[c] Engagement rate [d] Virality

24. The tool or software is commonly used for social media monitoring and analytics …….

[a] Microsoft Word [b] Photoshop

[c] Google Analytics [d] Hootsuite

25. The hashtag primarily used for on social media platforms ……..

[a] Sharing private messages [b] Categorizing and grouping content

[c] Sending direct messages [d] Editing photos

26. The symbol is commonly used to represent a hashtag ……

[a] @ [c] $ [b] # [d] %

27. The term for a hashtag that is trending and widely used by a large number of users at a specific time ……..

[a] Evergreen hashtag [b] Viral hashtag

[c] Trending hashtag [d] Niche hashtag

28. The character limit for a hashtag on Twitter …….

[a] 10 characters [b] 25 characters

[c] 140 characters [d] 280 characters

29. The term for content that becomes popular through online sharing and is often characterised by its rapid spread …….

[a] Trending content [b] Shareable content

[c] Viral content [d] Sponsored content

30. The term for the practice of creating and publishing content on social media platforms with the aim of engaging and retaining a specific target audience ……

[a] Social media advertising [b] social media monitoring

[c] Social media management [d] Social media listening

MCQs Question

1. What is Cyber Security ?
   a) Cyber Security provides security against malware
   b) Cyber Security provides security against cyber-terrorists
   c) Cyber Security protects a system from cyber attacks
   d) All of these

2. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
   a) Cyber attack
   b) Computer security
   c) Cryptography
   d) Digital hacking

3. Which of the following is a type of cyber security?
   a) Cloud Security
   b) Network Security
   c) Application Security
   d) All of the above

4. Which of the following is not a cybercrime?
   a) Denial of Service
   b) Man in the Middle
   c) Malware
   d) AES

5. Which of the following is a type of cyber attack ?
   a) Phishing
   b) SQL Injections
   c) Password Attack
   d) All of the above

6. "Cyberspace" was coined by _____
   a) Richard Stallman
   b) William Gibson
   c) Andrew Tannenbaum
   d) Scott Fahlman

7. The Inventor of the World Wide Web is _____.
   a) Marks Zuckerberg
   b) Bill Gates
   c) Tim Berners-Lee
   d) John McCarthy

8. What is World Wide Web ?
   a) A collection of interconnected computer networks.
   b) A web browser used for accessing online content.
   c) A collection of websites and web pages accessible over the internet.
   d) A software application for browsing the internet.

9. The standard internet protocol is
   a) TCP/IP
   b) UDP
   c) FTP
   d) WWW

10. Which of these is NOT involved in the CIA Triad ?
   a) Confidentiality
   b) Availability
   c) Integrity
   d) Authenticity

11. Which of the following is not a type of cyber security ?
   a. Data Security
   b. Network Security
   c. System Security
   d. None of these

12. HTTP Stand for
   a. Hypertext Transfer Protocol
   b. Hyper Text Transfer Point
   c. Higher Text Transfer Protocol
   d. High Text Transfer Point

13. Which of the following is not front-end technology ?
   a. HTML
   b. CSS
   c. Bootstrap
   d. None of these

14. ISOC stand for
   a. Internet Secure Operation Control
   b. Internet Society
   c. Internet Securely Operatable Control
   d. None of these

15. ARPANET Full form
   a. Advanced Resolution Projects Agency Network
   b. Address Resolution Packet and Network Encryption Transfer
   c. Advanced Research Projects Agency Network
   d. None of these

16. Which of the following is NOT a common cyber threat ?
   a) Malware
   b) Phishing
   c) Firewalls
   d) Ransomware

17. What is social engineering ?
   a) The use of technology to gain unauthorized access to computer systems.
   b) The process of manipulating individuals to reveal sensitive information or perform actions.

c) The practice of encrypting data to protect it from unauthorized access.
d) The process of analyzing network traffic to detect and prevent attacks.

18. Which of the following is an example of a strong authentication factor ?
a) Using a single password.
b) Using a fingerprint or facial recognition.
c) Using a generic username.
d) Using a publicly available password.

19. Which of the following is not a web technology ?
a) HTML
b) Java
c) CSS
d) PHP

20. Which technology is used for styling web pages ?
a) HTML
b) CSS
c) XML
d) JavaScript

21. Which technology is used for communication between web browsers and servers ?
a) HTML
b) CSS
c) XML
d) HTTP

22. Which technology is used for creating dynamic web pages ?
a) HTML
b) CSS
c) PHP
d) XML

23. The architecture of cyberspace refers to:
a) The physical infrastructure of the internet
b) The layout and design of websites
c) The structure and organization of information in virtual spaces
d) The security protocols used to protect online data

24. Which of the following is an example of an Internet governance organization ?
a) ICANN
b) IEEE
c) NSA
d) FIFA

25. What is a common type of malware ?
a) Firewall
b) Router
c) Virus
d) Encryption

26. What does the term "phishing" refer to in cyber security ?
a) Stealing sensitive information through email or fake websites
b) Denying access to a network or system by flooding it with traffic
c) Modifying or tampering with data in order to disrupt operations
d) Exposing vulnerabilities in computer systems

27. What is the purpose of a firewall in cyber security ?
    a) Protecting against viruses and malware
    b) Preventing unauthorized access to a network or system
    c) Encrypting sensitive data
    d) Monitoring and analyzing network traffic

28. What is a denial-of-service (DoS) attack ?
    a) Gaining unauthorized access to a system or network
    b) Flooding a network or system with traffic to make it unavailable
    c) Encrypting sensitive data to prevent unauthorized access
    d) Manipulating people to disclose sensitive information

29. What is the purpose of regular software updates and patches ?
    a) Enhancing system performance
    b) Adding new features to software
    c) Fixing security vulnerabilities and bugs
    d) Making software compatible with other programs

30. What is multi-factor authentication ?
    a) Authenticating a user based on a single factor, such as a password
    b) Authenticating a user based on multiple factors, such as a password and a fingerprint
    c) Authenticating a user based on biometric data, such as a retina scan
    d) Authenticating a user based on their IP address

MCQs Question

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

2. 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

3. 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

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

5. Cyber Security provide security against what ?
   a. Against Malware
   b. Against cyber-terrorists
   c. Defends a device from threat
   d. All of these

6. _____ means the security of data from tampering by unidentified users.
   a. Confidentiality
   b. Integrity
   c. Authentication
   d. Non-repudiation

7. Tampering with Computer Source Documents is _____ offence.
   a) Bailable
   b) Non-bailable
   c) Non-cognizable
   d) Both (a) and (c)

8. Order passed by Controller is challengeable before
   a) High Court
   b) Cyber Appellate Tribunal
   c) Adjudicatory Officer
   d) Supreme Court

9. Amendment to IT Act 2000 came into effect on _____.
   a) 2008 Oct. 2
   b) 2009 July 3
   c) 2008 June 1
   d) 2009 Oct. 27

10. The term ISP stands for :
   a) International Services Provider
   b) Internet Service Provider
   c) Internet Service Program
   d) Internet Social Policy

11. ICANN stands for :
   a) Internet Corporation for Assigned Names and Numbers
   b) International Commission for Assigned Names and Numbers
   c) International Corporation for Assisted Names and Numbers
   d) Internet Computer Assigned Names and Numbers

12. Which of the following is considered as the unsolicited commercial email ?
   a) Virus
   b) Malware
   c) Spam
   d) All of the above

13. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_____:
   a) Antivirus
   b) Firewall
   c) Cookies
   d) Malware

14. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits ?
   a) Piracy
   b) Plagiarism
   c) Intellectual property rights
   d) All of the above

15. Which one of the following security controls is most effective against zero-day attacks ?
   a. Application control
   b. Signature-based antivirus
   c. Vulnerability scans
   d. Intrusion prevention systems

16. Information Technology Act, 2000 describes the offence of child pornography and prescribed punishment for it :

a) Under Section 67
b) Under Section 67 A
c) Under Section 67 B
d) Under Section 68

17. _____ is a criminal offence of unlawfully obtaining money, property or services from a person, entity or institution, through coercion.

a) Phishing
b) Pornography
c) Net or Cyber Extortion
d) Credit Card Fraud

18. ICERT stands for :

a) Indian Commercial and Economical
b) Indian Commercial Emergency Response Team
c) Indian Computer Emergency Response Team
d) Indian Cyber Emergency Response Team

19. IPC Section 354 D is related to which of the following ?

a) Assault or use of criminal force to woman with intent to disobe
b) stalking
c) Sexual harassment and punishment for sexual harassment
d) Voyeurism

20. Which of the following do not comes under Social Engineering ?

a) Tailgating
b) Phishing
c) Pretexting
d) Spamming

MCQs Question

1. _____ type of sites are known as friend-of-a-friend site.
   a) Chat Messenger
   b) Social networking sites
   c) Tutorial sites
   d) Chat-rooms

2. Which of the following is not an appropriate measure for securing social networking accounts ?
   a) Strong passwords
   b) Link your account with a phone number
   c) Never write your password anywhere
   d) Always maintain a soft copy of all your passwords in your PC

3. Try to keep your passwords without meaning so that _____ attack becomes almost impossible to perform successfully.
   a) social engineering
   b) phishing
   c) password guessing
   d) brute force

4. _____ methods of social network marketing should a company always use.
   a. Blogging the only
   b. Twitter, Blogs, Facebook
   c. YouTube
   d. None of these

5. _____ is the term updates by Twitter users.
   a. Tweets
   b. Tweats
   c. Twinks
   d. Posts

6. What are the different types of social networking ?
   a) Social Connections
   b) Professional Connection
   c) Sharing of Multimedia
   d) All of these

7. What is the primary purpose of hashtags in Social Media ?
   a) To mark keywords or topics for easy searchability
   b) To indicate sarcasm or irony in post
   c) To identify the author of a post
   d) To categorize posts based on their sentiment

8. Ananya adds a video file to his social networking page. Which one of these describes a video that has been watched by a lot of people over a short period of time ?
   a) Digital
   b) Tagged
   c) Viral
   d) Open Source

9. Which was the first social media site ?
   a) Friendster
   b) Six Degrees
   c) LinkedIn
   d) Myspace

10. Knowing the password of a user for hacking is called ?
   a) Sneaking
   b) Spoofing
   c) Cyber stalking
   d) Spamming

11. Which of the following is NOT a Social Media Platform ?
   a) Facebook
   b) Twitter
   c) Instagram
   d) Google

12. Which social media platform is best for B2B marketing ?
   a) LinkedIn
   b) Facebook
   c) Instagram
   d) Twitter

13. In _____, we create our online communication sites through which we can share information, images, ideas, audio and video files, as well as other content with our friends, family members, and business partners.
a. Search Engines
b. Social Media
c. Google Images
d. Google Search

14. What technology field is concerned with social media privacy ?
a) Data Science
b) Cyber Security
c) Ethical Hacking
d) Database Management

15. What are the success factors for Viral content ?
a) Eye-catching title only
b) Focus on one key issue only
c) Surprising contents Only
d) All of these

16. Which of these is usually not kept private on social media ?
a) Photos
b) Username
c) Invitation
d) All of these

17. Which of these social media platforms features end to end encryption ?
a) Facebook
b) Snapchat
c) Instagram
d) Whatsapp

18. Which of these are security issues in social media ?
a) Privacy concern
b) Global connectivity
c) User generated content
d) None of these

19. Which of these are not an inappropriate content ?
a) Obscenity Laws
b) Privacy laws
c) Defamation and libel
d) Unauthorized Access

20. Which of these is not an opportunity in Social media networks ?
a) Global Connectivity
b) Knowledge Sharing
c) Spread of misinformation
d) Business Opportunity

MCQs Question

1. Which of the following describes e-commerce ?
   a. Doing business electronically
   b. Doing business
   c. Sale of goods
   d. All of the above

2. Which one is not the component of E-Commerce ?
   a. Online Storefront
   b. Encryption
   c. Shopping Cart
   d. Payment gateway

3. Which dimension of e-commerce enables commerce beyond the boundaries of the country ?
   a. Richness
   b. Interactivity
   c. Global Reach
   d. Ubiquity

4. Which e-commerce model involves the sale of goods or services from businesses to the general public ?
   a) Business to Government
   b) Business to Consumer
   c) Business to Business
   d) Consumer to Business

5. Which of the following is not a threats of E-Commerce ?
   a. Global reach
   b. Phishing
   c. Malware
   d. Data breaches

6. Which type of e-commerce focuses on consumers dealing with each other ?
   a. B2B
   b. B2C
   c. C2B
   d. C2C

7. Which of the following is advantage of E-Commerce ?
   a. Global Reach
   b. 24/7 availability
   c. Faster & Easier transactions
   d. All of these

8. What is e-payment ?
   a. Electronic payment for buying and selling through the Internet
   b. Payment of online software
   c. Payment of online services
   d. None of the above

9. Which one is not an E-payment method used in India ?
   a. Debit card
   b. Credit card
   c. e-cheque
   d. none

10. Which of the following is the components of Digital payment ?
   a. Point-of-sale
   b. Payment gateway
   c. Mobile Wallets
   d. All of these

11. Debit cards also allow
   a. Purchase on credit
   b. Instant cash withdrawal
   c. Debt repayment
   d. Late payment

12. What is electronic representation of cash ?
   a. E-cash
   b. Electronic cash
   c. Digital Cash
   d. All of these

13. Which of the following is benefits of the Aadhar Enabled payments ?
   a. Security
   b. Convenience
   c. Authenticity
   d. All of these

14. Which of the following must be linked with Aadhar card ?
   a. NEFT
   b. AEPS
   c. IMPS
   d. RTGS

15. USSD stands for
   a. User Sale Service Data
   b. User Supplementary Service Data
   c. Unstructured Supplementary Service Data
   d. Unique Supplementary Service Data

16. Who regulates the Money Market ?

a. SEBI
b. NSDL
c. RBI
d. NABARD

17. Expland UIDAI

a. Unique Identity Department for Aadhar in India
b. Unique Identification Authority of India
c. Uniquely Identification Authority of India
d. Unique Identity Department Authority of India

18. UPI Stand for

a. Unified Payment Interface
b. Unique Payment Interface
c. Unified Payment Interaction
d. Unique Payment Interface

19. Find the common modes of digital payments.

a. Mobile Wallets
b. Credit Card
c. Debit Card
d. All of these

20. POS in digital payment Stand for

a. Payment of System
b. Point of Sale
c. Both of these
d. None of these

MCQs Question

1. Which of the following is a common endpoint device ?
   A) Laptop
   B) Mobile phone
   C) Printer
   D) All of the above

2. What is the primary purpose of endpoint device security ?
   A) To protect sensitive data stored on the device
   B) To prevent unauthorized access to the device
   C) To detect and mitigate malware threats
   D) All of the above

3. What is mobile device management (MDM) ?
   A) A security solution for endpoint devices
   B) A set of policies and tools used to manage mobile devices
   C) A hardware component of endpoint devices
   D) None of the above

4. Which of the following is a common mobile phone security measure ?
   A) Strong passcode or biometric authentication
   B) Remote data wipe in case of loss or theft
   C) Regular software updates
   D) All of the above

5. What is the purpose of a password policy ?
   A) To ensure that all passwords are stored securely
   B) To restrict access to the system for unauthorized users
   C) To enforce strong password practices for enhanced security
   D) To prevent users from changing their password too frequently

6. What is the purpose of security patch management ?
   a) To update software with new features
   b) To improve software performance
   c) To fix vulnerabilities and protect against threats
   d) To add new functionalities to the software

7. Which of the following is a common vulnerability that security patch management aims to address ?
   a) Slow software performance
   b) Outdated user interface
   c) Software crashes
   d) Code vulnerabilities that can be exploited by hackers

8. How often should security patches be applied ?
   a) Once a year
   b) Once a month
   c) Every 6 months
   d) As soon as they become available

9. Which of the following is a benefit of data backup ?
   a) Improved system performance
   b) Increased vulnerability to data loss
   c) Higher likelihood of data corruption
   d) Reduced risk of data loss

10. What is the purpose of data backup ?
   a) To intentionally delete data from a system
   b) To protect data from common threats such as system failures, hardware malfunctions, or human errors
   c) To make data available for multiple users simultaneously
   d) To slow down system performance

11. Which of the following is NOT a commonly used data backup storage medium ?
   a) External hard drives
   b) CDs/DVDs
   c) Magnetic tape
   d) Fax machines

12. What does it mean to download third-party software ?
   a) Downloading software from the internet
   b) Downloading software from a trusted source
   c) Downloading software from a reliable website
   d) Downloading software from an unknown source

13. Why is it important to download third-party software from reliable sources ?
   a) To ensure the software is legitimate and free from malware
   b) To support the creators of the software
   c) To get the latest version of the software
   d) To avoid paying for the software

14. What is the purpose of software updates ?
   a) To add new features and improve functionality
   b) To remove bugs and security vulnerabilities
   c) To optimize performance and speed
   d) To increase compatibility with other programs

15. How can you manage third-party software on your computer ?
   a) Organize software licenses and documentation
   b) Uninstall unnecessary or unused software
   c) Keep all software up to date with the latest versions
   d) All of the above

16. Which of the following is a best practice for device security policy ?
    a) Enabling automatic software updates
    b) Allowing users to install any application
    c) Disabling device encryption
    d) Sharing device passwords with colleagues

17. What is the purpose of device encryption in a security policy ?
    a) To prevent unauthorized access to data on a device
    b) To allow users to easily transfer data between devices
    c) To improve device performance
    d) To enable remote device management

18. Which of the following is a common requirement in a device security policy ?
    a) Regularly backing up device data
    b) Allowing device rooting or jailbreaking
    c) Disabling two-factor authentication
    d) Sharing device login credentials with third parties

19. What is the purpose of implementing strong password policies in a device security policy ?
    a) To enhance the security of device login credentials
    b) To make it easier for users to remember their passwords
    c) To allow users to share login credentials with colleagues
    d) To disable password complexity requirements

20. What is phishing ?
    a) The act of hacking into computer networks or systems.
    b) The use of computer viruses to steal personal information.
    c) The act of tricking individuals into revealing sensitive information through fake emails or websites.
    d) The act of intercepting and reading online communications.

21. What is the purpose of regularly updating software and devices ?
    a) It improves system performance and functionality.
    b) It keeps the systems protected against newly discovered vulnerabilities.
    c) It allows users to access new features and capabilities.
    d) It prevents unauthorized access to systems and data.

22. What is the significance of a host firewall ?
    A. It protects the network infrastructure from external threats
    B. It protects the host from network-based attacks
    C. It prevents unauthorized access to the host
    D. All of the above

23. What is the significance of antivirus software ?
   A. It protects the host from malware and viruses
   B. It detects and removes malicious software
   C. It prevents unauthorized access to the host
   D. All of the above

24. What is Wi-Fi security ?
   (a) It refers to the ease of connecting to a Wi-Fi network.
   (b) It refers to the protection of Wi-Fi networks from unauthorized access.
   (c) It refers to the range of a Wi-Fi network.
   (d) It refers to the speed of a Wi-Fi network.

25. Why is Wi-Fi security important ?
   (a) To prevent hackers from stealing personal and sensitive information.
   (b) To ensure a stable and reliable connection.
   (c) To increase the speed of the Wi-Fi network.
   (d) To connect to multiple devices simultaneously.

26. Which of the following is NOT a common Wi-Fi security protocol ?
   (a) WPA
   (b) WEP
   (c) SSL
   (d) WPA2

27. How can you improve Wi-Fi security ?
   (a) Changing the default router password
   (b) Enabling network encryption
   (c) Hiding the Wi-Fi network name
   (d) All of the above

28. What is the purpose of a Wi-Fi password ?
   (a) To limit the number of devices that can connect to the network.
   (b) To secure the data transmitted over the network.
   (c) To control the speed of the Wi-Fi network.
   (d) To prevent Wi-Fi interference.

29. When configuring access controls, what is the principle of least privilege ?
   a) Giving users access only to the resources they need to perform their job functions
   b) Granting users unrestricted access to all resources
   c) Assigning the same level of access to all users
   d) Only granting access to administrators

30. Which of the following is an example of two-factor authentication ?

a) Using a password and a PIN

b) Using a password and a security question

c) Using a fingerprint and a retina scan

d) Using a username and a password