QUESTION BANK

Cyber Security Vocational Course

Cyber Safety & Awareness Modules

English and Hindi

Module 1

Cyber Crime and Cyber Hygiene

Q1. What is the primary purpose of an operating system?

A. To create websites

B. To manage hardware and software resources

C. To provide internet connectivity only

D. To protect against viruses only

Q2. Which of the following is an example of an input device?

A. Monitor

B. Printer

C. Keyboard

D. Speaker

Q3. What does LAN stand for?

A. Local Access Network

B. Local Area Network

C. Large Area Network

D. Logical Area Network

Q4. Which device is primarily used to connect multiple devices within a LAN?

A. Router

B. Switch

C. Modem

D. Repeater

Q5. How many layers are present in the OSI model?

A. 4

B. 5

C. 6

D. 7

Q6. Which OSI layer is responsible for logical addressing and routing?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Transport Layer

Q7. Which protocol is connection-oriented?

A. UDP

B. TCP

C. IP

D. ARP

Q8. What is the primary function of DNS?

A. Assigning IP addresses automatically

B. Translating domain names into IP addresses

C. Encrypting network traffic

D. Filtering network packets

Q9. Which protocol is used to automatically assign IP addresses to devices?

A. DNS

B. HTTP

C. DHCP

D. FTP

Q10. What is the default port number of HTTPS?

A. 21

B. 80

C. 443

D. 25

Q11. Which of the following is a private IPv4 address?

A. 8.8.8.8

B. 192.168.1.10

C. 1.1.1.1

D. 172.40.10.5

Q12. What is the size of an IPv4 address?

A. 16 bits

B. 32 bits

C. 64 bits

D. 128 bits

Q13. What is the primary function of a MAC address?

A. Identifying a network interface at the Data Link Layer

B. Identifying a website

C. Encrypting network communication

D. Assigning domain names

Q14. Which protocol is used to map an IPv4 address to a MAC address on a local network?

A. DNS

B. DHCP

C. ARP

D. ICMP

Q15. Which command is commonly used to test network connectivity?

A. mkdir

B. ping

C. copy

D. format

Q16. What is the main purpose of a router?

A. To print documents

B. To connect different networks and forward packets

C. To store files

D. To scan computers for viruses

Q17. What is the purpose of subnetting?

A. To increase monitor resolution

B. To divide a network into smaller logical networks

C. To encrypt data

D. To increase CPU speed

Q18. Which technology allows multiple isolated virtual machines to run on one physical computer?

A. Switching

B. Virtualization

C. Routing

D. Subnetting

Q19. Which command-line tool is used to display IP configuration in Windows?

A. ipconfig

B. ifconfig

C. chmod

D. netstat

Q20. What is the primary purpose of a VLAN?

A. To increase internet speed automatically

B. To logically segment a network into separate broadcast domains

C. To replace routers

D. To assign public IP addresses

Module - 2

Social Media Threats & Cyberbullying

1. What is the main objective of a romance scammer?

A. To make friends

B. To steal money or personal information

C. To play online games

D. To promote movies

2. Which of the following may be a sign of online grooming?

A. Asking about hobbies

B. Asking for private photos or secrets

C. Sending memes

D. Talking about school

3. How do romance scammers usually build trust?

A. By showing genuine ID proof

B. By pretending to be in love and giving emotional attention

C. By meeting in person immediately

D. By always sending gifts

4. Why might an online person repeatedly avoid video calls?

A. Their camera is always broken

B. They are shy

C. They may not be the person shown in their photos

D. They prefer messaging

5. What is a common red flag in a romance scam?

A. Correct grammar

B. Asking for money quickly

C. Normal conversation

D. Sharing hobbies

6. How does online grooming often begin?

A. By gradually building friendship and trust

B. By asking for a bank password

C. By meeting the parents

D. By sending official documents

7. What do fake giveaway scammers usually make victims do?

A. Pay a processing fee

B. Collect a free gift

C. Visit a park

D. Join a study group

8. What do cryptocurrency scam promotions usually claim?

A. Low returns

B. Guaranteed very high profits

C. Normal market growth

D. Slow investment

9. What is often used in impersonation scams?

A. Only verified accounts

B. Slightly altered usernames

C. Government websites

D. School IDs

10. In which situation is a giveaway more likely to be fake?

A. It claims to offer a big prize without reliable proof

B. Previous winners are verified

C. Information is available on the official website

D. The terms and conditions are clear

11. What does reverse image search help with?

A. Finding phone numbers

B. Checking whether a profile photo has been taken from somewhere else

C. Improving image quality

D. Creating new pictures

12. What can a username lookup help you find?

A. A person's home address

B. Other online accounts using the same username

C. Mobile recharge offers

D. Offline location

13. What information can a photo's metadata provide?

A. Weather information

B. Hidden information such as the date or time the photo was created

C. Movie files

D. Shopping history

14. Which may be a behavioural red flag of a fake profile?

A. Posting everyday photos

B. Sending the same messages to many people

C. Having old posts

D. Being tagged with family or friends

15. What may commonly be seen in a fake account?

A. Very few posts and an account created recently

B. A long and regular history

C. A real-life network

D. A record of old activity

16. What should you do if an unknown person repeatedly sends harassing messages on social media?

A. Give them your personal information

B. Block and report them

C. Forward their messages to others

D. Continue the conversation

17. What is it called when someone creates a fake identity of another person on social media and sends messages to others?

A. Impersonation

B. Data backup

C. Two-factor authentication

D. Account recovery

18. If your account is hacked, what is the first appropriate step?

A. Create a new account

B. Use the platform's account recovery option

C. Wait for two days

D. Share information with strangers

19. How does two-factor authentication (2FA) help?

A. By making login faster

B. By adding a second layer of security

C. By automatically saving passwords

D. By hiding photos

20. If someone asks you for an OTP to participate in a giveaway, what should you do?

A. Share the OTP immediately

B. Share the OTP only with friends

C. Do not share the OTP and verify the offer

D. Also provide your bank password

Module - 3

Identity Theft & Personal Data Leaks

1. What do cybercriminals do in credential stuffing?

   A. Try stolen passwords on multiple websites

   B. Clean computer screens

   C. Create new email accounts

   D. Increase internet speed

2. What can happen if a person uses the same password on several websites?

   A. If one account's password is leaked, other accounts may also be at risk

   B. All accounts become secure automatically

   C. The internet stops working

   D. The phone battery charges faster

3. Repeated failed login attempts from unfamiliar locations may indicate what?

   A. A credential stuffing attempt

   B. A normal software update

   C. Photo backup

   D. Online shopping

4. Which is a good habit for keeping online accounts secure?

   A. Using the same password on every website

   B. Using strong and different passwords

   C. Sharing passwords with friends

   D. Posting passwords publicly

5. Where might hackers obtain a person's old passwords?

   A. From data breaches at other websites

   B. From weather websites

   C. From online game scores

   D. From a phone screen

6. What does caller ID spoofing mean?

   A. Changing your voice during a call

   B. Displaying a fake number or identity in caller ID

   C. Sending messages without a SIM card

D. Turning off the phone ringtone

7. Whom might a person making a fake customer-care call pretend to represent?

A. A bank or telecommunications company

B. A school classmate

C. A delivery vehicle

D. A weather reporter

8. What should you do if someone claiming to be a bank employee asks for your OTP or PIN over the phone?

A. Tell them your OTP or PIN

B. End the call and contact the bank using its official number

C. Read the OTP message aloud to them

D. Send them your password too

9. What is a safe way to verify a customer-care number?

A. Trust a number found in a social media comment

B. Get the number from the bank's or company's official website/app

C. Ask an unknown person for the number

D. Click any search advertisement

10. Why can caller ID spoofing make it easier to deceive people?

A. The call may display a number that looks like it belongs to a genuine organisation

B. The phone always switches off

C. The call audio is unclear

D. The mobile network becomes stronger

11. When does a personal data leak occur?

A. When information is securely backed up

B. When personal information is exposed without permission

C. When an app is updated

D. When a user changes a password

12. What type of information was reportedly exposed in the Domino's India data leak?

A. Customers' phone numbers and addresses

B. Pizza recipes

C. The price of delivery bikes

D. Store rent

13. What type of user information was included in the BigBasket data leak?

A. Email addresses, passwords and phone numbers

B. Only grocery store timings

C. Only product prices

D. The colours of delivery vehicles

14. What type of information was exposed in the Unacademy data leak?

A. Users' email addresses and passwords

B. Examination centre buildings

C. Teachers' holiday lists

D. Classroom seat numbers

15. What risk may a person face after a data leak?

A. An increased risk of scams and spam messages

B. Increased internet speed

C. Increased phone memory

D. All accounts automatically closing

16. What risk may arise from scanning a suspicious QR code?

A. It may open a website designed to steal personal information

B. The phone becomes secure automatically

C. The battery gets charged

D. The screen brightness increases

17. What should you do if an unfamiliar website opens after scanning a QR code?

A. Immediately enter your bank details

B. Do not proceed without checking the website

C. Enter your OTP

D. Forward the link to all your friends

18. What should you remember to avoid QR-code payment scams?

A. You must always enter a PIN to receive money

B. Check the recipient and amount before paying; do not share your PIN/OTP

C. Every QR code is safe

D. Make payments as instructed by strangers

19. Which is the safest choice when scanning a QR code?

A. A QR code on any unfamiliar poster

B. A QR code from a trusted and verified source

C. Any QR code displayed on the street

D. A QR code sent in an unknown message

20. What risk may arise if someone pastes a fake QR code over a genuine one?

A. The payment may go to the wrong account or a fake link may open

B. The phone screen may break

C. The mobile battery may increase

D. Contacts may be saved automatically

Module - 4

Online Financial Frauds & Digital Payments Security

Q1. What is an online financial fraud?

A. Secure online shopping

B. Cheating someone to steal money through digital platforms

C. Checking bank balance

D. Paying electricity bills online

Q2. What is the full form of UPI?

A. Unified Payment Interface

B. Unified Payments Interface

C. Universal Payment India

D. Unique Payment Identification

Q3. What should you do if someone asks for your UPI PIN to receive money?

A. Share the PIN

B. Send the PIN through WhatsApp

C. Never share your UPI PIN

D. Share only the first two digits

Q4. What is phishing?

A. A method of online shopping

B. A fraud technique used to steal sensitive information through fake messages or websites

C. A secure banking method

D. A method of transferring money

Q5. What is an OTP?

A. One-Time Password

B. Online Transfer Process

C. One Transfer Payment

D. Official Transaction Password

Q6. Should you share your OTP with anyone?

A. Yes, with bank employees

B. Yes, with friends

C. Only over phone calls

D. No, never share your OTP

Q7. Which of the following is a secure practice while making online payments?

A. Using public Wi-Fi for banking

B. Sharing card details with strangers

C. Using trusted and secure websites

D. Clicking unknown payment links

Q8. What is a QR code commonly used for in digital payments?

A. Scanning and making payments

B. Increasing mobile storage

C. Blocking phone calls

D. Downloading antivirus

Q9. What should you do before scanning an unknown QR code?

A. Scan it immediately

B. Verify the source and purpose

C. Share it with friends

D. Enter your banking password

Q10. What is a common sign of a fake banking message?

A. It provides official information

B. It asks you to click an unknown link urgently

C. It comes through your bank's verified application

D. It provides a bank branch address

Q11. What is a debit card used for?

A. Withdrawing money and making payments from a bank account

B. Creating social media accounts

C. Sending emails

D. Increasing internet speed

Q12. What is card skimming?

A. Cleaning an ATM screen

B. Stealing card information using a hidden or unauthorised device

C. Depositing money into an ATM

D. Checking account balance

Q13. Which information should never be shared publicly?

A. Your favourite colour

B. Your bank account balance

C. Your ATM PIN and OTP

D. Your city name

Q14. What should you do if your mobile phone containing banking apps is lost?

A. Ignore it

B. Inform your bank and block access to banking services

C. Share your phone password online

D. Wait for someone to return it

Q15. What is a fake customer care number scam?

A. Calling an official bank number

B. A fraudster pretending to be customer support to steal information or money

C. Checking bank details

D. Receiving a bank statement

Q16. What should you do if you receive an unknown payment link?

A. Click it immediately

B. Forward it to everyone

C. Verify the sender before opening it

D. Enter your UPI PIN

Q17. What does a strong banking password contain?

A. Only your name

B. Your date of birth

C. A combination of letters, numbers and special characters

D. Only 123456

Q18. What is the purpose of two-factor authentication (2FA)?

A. To increase internet speed

B. To provide an additional layer of security

C. To delete bank records

D. To avoid all banking charges

Q19. What should you do after noticing an unauthorised transaction in your bank account?

A. Ignore the transaction

B. Wait for one month

C. Immediately contact your bank and report it

D. Share your OTP with customer care

Q20. Which official helpline number can be used to report cyber financial fraud in India?

A. 100

B. 101

C. 1930

D. 108

Module – 5 Women & Child Online Safety

Question 1. What does the term Digital Landscape refer to?

a) Using computers only

b) The environment of the internet, digital devices, and online platforms

c) Using mobile phones only

d) Using social media only

Question 2. What is the primary objective of online safety?

a) To stop using the internet

b) To delete social media accounts

c) To protect personal information and digital identity

d) To register on every website

Question 3. Which of the following is a common online threat?

a) Phishing

b) Online education

c) Video conferencing

d) Digital payment

Question 4. What should you do if a stranger sends you a suspicious link on social media?

a) Open it immediately

b) Forward it to all friends

c) Enter your personal information

d) Avoid opening it and report the suspicious link

Question 5. What precaution should be taken while sharing personal information on social media?

a) Publicly sharing your home address

b) Sharing only necessary information

c) Sharing bank details

d) Sharing passwords

Question 6. What is cyberbullying?

a) Providing online education

b) Shopping safely on the internet

c) Harassing or humiliating someone through digital platforms

d) Sharing photographs on social media

Question 7. What is the most appropriate action when someone experiences cyberbullying?

a) Preserve evidence and report it to the relevant platform

b) Threaten the person in return

c) Immediately delete all messages

d) Publish personal information online

Question 8. Which of the following may be a sign of cyberbullying?

a) Increased interest in online studies

b) Making new friends

c) Improved internet speed

d) Feeling anxious or distressed after online activities

Question 9. What does cyberstalking mean?

a) Searching for educational content online

b) Repeatedly following or monitoring someone through digital platforms

c) Playing online games

d) Having normal conversations on social media

Question 10. What is a common objective of fake matrimony and dating scams?

a) Providing online education

b) Making new friends

c) Fraudulently obtaining money or personal information

d) Promoting digital literacy

Question 11. What is the best way to protect children from online dangers such as the Blue Whale and Momo challenges?

a) Maintaining appropriate supervision and awareness of children's online activities

b) Encouraging children to communicate with strangers

c) Ignoring all suspicious messages

d) Allowing children to use the internet without supervision

Question 12. Which of the following is an example of personal information?

a) General weather information

b) Public news

c) General educational articles

d) Home address and mobile number

Question 13. What should users do to maintain online privacy?

a) Share passwords with everyone

b) Use strong passwords and privacy settings

c) Make all social media posts public

d) Send personal photographs to strangers

Question 14. What should parents do to protect children's online privacy?

a) Allow children to share information freely on all websites

b) Make children's passwords public

c) Use age-appropriate safe platforms and parental controls

d) Ignore children's online activities

Question 15. What should you do if you suspect a hidden camera in a hotel room?

a) Examine the suspicious object or device, move to a safe place, and inform the appropriate authorities

b) Break the camera immediately

c) Take the suspicious device home

d) Completely ignore the incident

Question 16. What should a person do when experiencing online harassment?

a) Share personal information with the harasser

b) Respond to threats with threats

c) Delete all evidence immediately

d) Preserve evidence, block the offender, and file a complaint

Question 17. What is a key characteristic of a safe online community?

a) Encouraging abusive comments

b) Promoting respectful behaviour and safe communication

c) Making personal information public

d) Ignoring cyberbullying

Question 18. What should users do when they encounter harmful content on an online platform?

a) Spread it to more people

b) Share it without verification

c) Report it through the platform

d) Provide personal information in response

Question 19. Which is an effective way to improve online safety awareness?

a) Regular cybersecurity awareness training and education

b) Completely stopping internet usage

c) Sharing passwords

d) Opening suspicious links

Question 20. How can users build a positive online community?

a) By harassing others

b) By spreading misinformation

c) By using abusive language

d) By promoting respect, responsibility, and safe behaviour

Module – 6 Dark Web, Cyber Terrorism & Illegal Activities

Question 1. What is the Dark Web?

a) The normal and publicly accessible part of the internet

b) A part of the internet that cannot be easily accessed through standard search engines

c) A collection of social media websites only

d) A collection of educational websites only

Question 2. Which browser is commonly used to access the Dark Web?

a) Google Chrome

b) Microsoft Edge

c) Tor Browser

d) Internet Explorer

Question 3. What is the main difference between the Deep Web and the Dark Web?

a) The Deep Web includes pages not indexed by standard search engines, while the Dark Web may require specialized software or configurations

b) Both are exactly the same

c) The Dark Web is used only for government websites

d) The Deep Web is limited to social media only

Question 4. What is the primary purpose of the Tor network?

a) To increase internet speed

b) To encrypt files

c) To increase computer storage

d) To help maintain user anonymity and privacy while browsing

Question 5. In which year was Operation Onymous conducted?

a) 2012

b) 2014

c) 2017

d) 2021

Question 6. What was the primary objective of Operation Onymous?

a) To promote online education

b) To increase internet speed

c) To take action against illegal Dark Web marketplaces and related activities

d) To create social media accounts

Question 7. Emotet is primarily known as which type of threat?

a) Malware and botnet

b) Antivirus software

c) Web browser

d) Data backup tool

Question 8. In which year was the international operation conducted to disrupt the Emotet botnet?

a) 2015

b) 2017

c) 2019

d) 2021

Question 9. In which year did the WannaCry ransomware attack occur?

a) 2014

b) 2017

c) 2020

d) 2022

Question 10. What does Cyber Terrorism mean?

a) Performing normal online shopping

b) Sharing photographs on social media

c) Attacking digital systems to create fear or disruption for political or ideological purposes

d) Providing online education

Question 11. Which of the following can be a potential target of cyber terrorism?

a) Critical government and public infrastructure

b) Personal photographs only

c) Entertainment websites only

d) Online games only

Question 12. Which of the following could be an example of cyber terrorism?

a) Creating a secure website

b) Performing online banking

c) Updating software

d) Conducting a destructive cyberattack against a critical government network

Question 13. Which of the following is an example of illegal activity on the Dark Web?

a) Online education

b) Trading illegal goods and services

c) Government information portals

d) Digital libraries

Question 14. What types of activities may cybercriminals conduct on Dark Web marketplaces?

a) Providing online courses

b) Sharing public news

c) Trading stolen data and illegal services

d) Promoting government schemes

Question 15. How can stolen personal data available on the Dark Web be misused?

a) Identity theft and financial fraud

b) Online education

c) Increasing internet speed

d) Creating data backups

Question 16. What does a botnet mean in cybercrime?

a) A secure computer network

b) A normal group of computers

c) A group of antivirus tools only

d) A group of infected devices that can be remotely controlled by an attacker

Question 17. Which open-source resource can be useful for searching and monitoring information related to the Dark Web?

a) Microsoft Word

b) Ahmia Search Engine

c) Paint

d) Calculator

Question 18. What is the most important safety precaution when investigating suspicious Dark Web activities?

a) Downloading unknown files

b) Sharing personal information

c) Conducting only authorized investigations in a secure and controlled environment

d) Clicking suspicious links

Question 19. What can be the impact of Dark Web crimes and cyber terrorism on society?

a) Financial losses, security risks, and public fear

b) Increased internet speed

c) Automatic improvement in digital literacy

d) Improved data security

Question 20. Which is an effective approach to combating Dark Web threats and cyber terrorism?

a) Ignoring cybercrimes

b) Sharing suspicious activities

c) Disabling security updates

d) Cybersecurity awareness, law enforcement, and international cooperation

Module -7 Cyber Hygiene

Q1. What is Cyber Hygiene?

A. Cleaning a computer physically

B. Following regular practices to keep digital devices and information secure

C. Increasing internet speed

D. Installing games on a computer

Q2. Which of the following is a strong password?

A. 123456

B. password

C. Rahul123

D. R@h7#Lq92!

Q3. How often should you update your software and operating system?

A. Never

B. Only when the computer stops working

C. Regularly, whenever security updates are available

D. Once in five years

Q4. What is the purpose of antivirus software?

A. To increase screen brightness

B. To detect, prevent and remove malicious software

C. To increase internet speed

D. To create documents

Q5. What should you do before clicking a link received from an unknown sender?

A. Click immediately

B. Forward it to friends

C. Verify the sender and check the link

D. Enter your password

Q6. What is Multi-Factor Authentication (MFA)?

A. Using multiple computers

B. Using two or more verification methods to access an account

C. Using multiple email accounts

D. Changing the computer password daily

Q7. Why should you avoid using the same password for multiple accounts?

A. It increases internet usage

B. If one account is compromised, other accounts may also be at risk

C. It reduces computer performance

D. It deletes your files

Q8. What should you do when leaving your computer unattended?

A. Keep it unlocked

B. Turn off the antivirus

C. Lock the computer screen

D. Share your password

Q9. What is phishing?

A. A method of securing a computer

B. A cyberattack that tricks users into revealing sensitive information

C. A method of backing up data

D. A type of computer hardware

Q10. Why is regular data backup important?

A. To increase screen resolution

B. To recover data in case of accidental deletion, system failure or cyberattack

C. To increase battery life

D. To improve typing speed

Q11. Which of the following is a safe practice while using public Wi-Fi?

A. Accessing banking websites without protection

B. Sharing passwords over public Wi-Fi

C. Avoiding sensitive transactions on unsecured public Wi-Fi

D. Disabling all security settings

Q12. What should you do if you receive an unexpected email attachment?

A. Open it immediately

B. Download and execute it

C. Verify the sender before opening it

D. Forward it to everyone

Q13. What is the purpose of a firewall?

A. To control incoming and outgoing network traffic

B. To increase storage capacity

C. To improve display quality

D. To delete temporary files

Q14. Which information should not be shared on social media?

A. Favourite movie

B. Public news

C. Passwords, OTPs and sensitive personal information

D. General hobbies

Q15. Why should you download applications only from trusted sources?

A. To get more advertisements

B. To reduce the risk of installing malicious applications

C. To increase phone weight

D. To improve camera quality

Q16. What should you do if you suspect that your email account has been hacked?

A. Ignore the situation

B. Share your password with friends

C. Change your password immediately and enable MFA

D. Delete all your contacts

Q17. What is the purpose of screen lock on mobile phones?

A. To increase internet speed

B. To prevent unauthorised access to the device

C. To increase storage

D. To improve camera performance

Q18. Which of the following is an example of sensitive personal information?

A. Favourite sport

B. Favourite colour

C. Bank account details and identity information

D. Favourite television programme

Q19. What should you do before connecting a USB drive received from an unknown person?

A. Open all files immediately

B. Scan it using updated security software

C. Disable antivirus

D. Copy all files to your computer

Q20. Which of the following is the best example of good cyber hygiene?

A. Using weak passwords

B. Ignoring software updates

C. Regularly updating devices, using strong passwords and taking data backups

D. Sharing OTPs with others

Module - 8 Awareness Ransomware

Question 1. What is ransomware?

a) Software used to improve system performance

b) Malware that encrypts files and demands ransom

c) Software used for data backup

d) Antivirus software

Question 2. What is the primary objective of ransomware?

a) To improve network speed

b) To delete temporary files

c) To monitor system performance

d) To restrict access to data and demand money

Question 3. Which of the following is a type of ransomware?

a) Crypto ransomware

b) Firewall ransomware

c) Browser ransomware

d) Backup ransomware

Question 4. Which of the following is a common ransomware infection vector?

a) Software updates

b) Data backup

c) Malicious email attachments

d) Antivirus scanning

Question 5. What is phishing in the context of ransomware attacks?

a) Tricking users into opening malicious links or sharing sensitive information

b) Encrypting backup files

c) Installing security updates

d) Monitoring network traffic

Question 6. What does RDP stand for?

a) Remote Data Protection

b) Remote Desktop Protocol

c) Restricted Data Process

d) Real-time Data Processing

Question 7. Which security weakness can make RDP a target for ransomware attackers?

a) Using offline backups

b) Performing regular software updates

c) Using strong authentication

d) Exposing RDP to the internet with weak credentials

Question 8. What is a drive-by download?

a) Downloading files from a trusted website

b) Manually installing antivirus software

c) Downloading malicious software without the user's clear knowledge or consent

d) Creating a backup of files

Question 9. What is a major impact of ransomware on an organization?

a) Data unavailability and business disruption

b) Improved system performance

c) Increased storage capacity

d) Improved network connectivity

Question 10. Which ransomware attack occurred globally in 2017?

a) NotPetya

b) WannaCry

c) CryptoLocker

d) LockBit

Question 11. What was a major feature of the WannaCry ransomware attack?

a) It only affected mobile phones

b) It improved system security

c) It spread across vulnerable Windows systems

d) It only targeted social media accounts

Question 12. What is another name for the AIDS Trojan?

a) WannaCry

b) CryptoLocker

c) LockBit

d) PC Cyborg

Question 13. What is the primary purpose of regular security patching?

a) To fix known security vulnerabilities

b) To increase file size

c) To disable antivirus software

d) To remove user accounts

Question 14. Which password practice helps prevent unauthorized access?

a) Using the same password everywhere

b) Using strong and unique passwords

c) Sharing passwords with colleagues

d) Writing passwords in public places

Question 15. What should a user do after receiving a suspicious email attachment?

a) Open it immediately

b) Forward it to everyone

c) Verify the sender and report the suspicious email

d) Disable the antivirus

Question 16. What is the primary role of Endpoint Detection and Response (EDR)?

a) To increase internet speed

b) To manage office attendance

c) To create user passwords

d) To detect, investigate, and respond to endpoint threats

Question 17. Why is network segmentation important for ransomware defense?

a) It limits the spread of malware across network segments

b) It eliminates the need for backups

c) It increases password length

d) It disables network security

Question 18. What is the purpose of the 3-2-1 backup rule?

a) To maintain three user accounts

b) To install three antivirus programs

c) To maintain multiple copies of data on different media, including one offsite copy

d) To create three network connections

Question 19. Why should organizations maintain offline backups?

a) To increase internet speed

b) To protect backup data from ransomware encryption

c) To reduce employee attendance

d) To disable system updates

Question 20. Why are organization-wide cybersecurity awareness trainings important?

a) To increase unnecessary software installations

b) To eliminate the need for security tools

c) To allow employees to share passwords

d) To help employees identify and prevent cyber threats

Module 1

Cyber Crime and Cyber Hygiene

1) ऑपरेटिंग सिस्टम का मुख्य उद्देश्य क्या है?

a) वेबसाइट बनाना

b) हार्डवेयर और सॉफ्टवेयर संसाधनों का प्रबंधन करना

c) केवल इंटरनेट कनेक्टिविटी प्रदान करना

d) केवल वायरस से सुरक्षा प्रदान करना

2) निम्नलिखित में से कौन-सा इनपुट डिवाइस है?

a) मॉनिटर

b) प्रिंटर

c) कीबोर्ड

d) स्पीकर

3) LAN का पूरा नाम क्या है?

a) लोकल एक्सेस नेटवर्क

b) लोकल एरिया नेटवर्क

c) लार्ज एरिया नेटवर्क

d) लॉजिकल एरिया नेटवर्क

4) LAN में कई डिवाइसों को आपस में जोड़ने के लिए मुख्य रूप से किस डिवाइस का उपयोग किया जाता है?

a) राउटर

b) स्विच

c) मॉडेम

d) रिपीटर

5) OSI मॉडल में कितनी लेयर्स होती हैं?

a) 4

b) 5

c) 6

d) 7

6) OSI मॉडल की कौन-सी लेयर लॉजिकल एड्रेसिंग और रूटिंग के लिए जिम्मेदार होती है?

a) फिजिकल लेयर

b) डेटा लिंक लेयर

c) नेटवर्क लेयर

d) ट्रांसपोर्ट लेयर

7) निम्नलिखित में से कौन-सा कनेक्शन-ओरिएंटेड प्रोटोकॉल है?

a) UDP

b) TCP

c) IP

d) ARP

8) DNS का मुख्य कार्य क्या है?

a) IP एड्रेस को स्वचालित रूप से आवंटित करना

b) डोमेन नेम को IP एड्रेस में बदलना

c) नेटवर्क ट्रैफिक को एन्क्रिप्ट करना

d) नेटवर्क पैकेट को फिल्टर करना

9) डिवाइसों को स्वचालित रूप से IP एड्रेस देने के लिए किस प्रोटोकॉल का उपयोग किया जाता है?

a) DNS

b) HTTP

c) DHCP

d) FTP

10) HTTPS का डिफॉल्ट पोर्ट नंबर क्या है?

a) 21

b) 80

c) 443

d) 25

11) निम्नलिखित में से कौन-सा प्राइवेट IPv4 एड्रेस है?

a) 8.8.8.8

b) 192.168.1.10

c) 1.1.1.1

d) 172.40.10.5

12) IPv4 एड्रेस का आकार कितना होता है?

a) 16 बिट

b) 32 बिट

c) 64 बिट

d) 128 बिट

13) MAC एड्रेस का मुख्य कार्य क्या है?

a) डेटा लिंक लेयर पर नेटवर्क इंटरफेस की पहचान करना

b) वेबसाइट की पहचान करना

c) नेटवर्क कम्युनिकेशन को एन्क्रिप्ट करना

d) डोमेन नेम आवंटित करना

14) लोकल नेटवर्क में IPv4 एड्रेस को MAC एड्रेस से मैप करने के लिए किस प्रोटोकॉल का उपयोग किया जाता है?

a) DNS

b) DHCP

c) ARP

d) ICMP

15) नेटवर्क कनेक्टिविटी की जाँच करने के लिए सामान्यतःकिस कमांड का उपयोग किया जाता है?

a) MKDIR

b) PING

c) COPY

d) FORMAT

16) राउटर का मुख्य कार्य क्या है?

a) डॉक्यूमेंट प्रिंट करना

b) अलग-अलग नेटवर्क को जोड़ना और पैकेट फॉरवर्ड करना

c) फाइल स्टोर करना

d) कंप्यूटर में वायरस स्कैन करना

17) सबनेटिंग का मुख्य उद्देश्य क्या है?

a) मॉनिटर का रेजोल्यूशन बढ़ाना

b) एक नेटवर्क को छोटे लॉजिकल नेटवर्क में विभाजित करना

c) डेटा को एन्क्रिप्ट करना

d) CPU की स्पीड बढ़ाना

18) कौन-सी तकनीक एक ही फिजिकल कंप्यूटर पर कई अलग-अलग वर्चुअल मशीन चलाने की सुविधा देती है?

a) स्विचिंग

b) वर्चुअलाइजेशन

c) रूटिंग

d) सबनेटिंग

19) विंडोज़ में IP कॉन्फ़िगरेशन देखने के लिए किस कमांड का उपयोग किया जाता है?

a) IPCONFIG

b) IFCONFIG

c) CHMOD

d) NETSTAT

20) VLAN का मुख्य उद्देश्य क्या है?

a) इंटरनेट की स्पीड अपने आप बढ़ाना

b) नेटवर्क को अलग-अलग ब्रॉडकास्ट डोमेन्स में विभाजित करना

c) राउटर को पूरी तरह बदलना

d) पब्लिक IP एड्रेस आवंटित करना

Module - 2

Social Media Threats & Cyberbullying

1. रोमांस स्कैमर का मुख्य उद्देश्य क्या होता है?

A. दोस्ती करना

B. पैसे या व्यक्तिगत जानकारी चुराना

C. ऑनलाइन गेम खेलना

D. फिल्मों का प्रचार करना

2. ऑनलाइन ग्रूमिंग का कौन-सा संकेत हो सकता है?

A. शौक के बारे में पूछना

B. निजी फोटो या राज़ मांगना

C. मीम भेजना

D. स्कूल के बारे में बात करना

3. रोमांस स्कैमर भरोसा बनाने के लिए आम तौर पर क्या करते हैं?

A. असली ID प्रूफ दिखाते हैं

B. प्यार का नाटक करके भावनात्मक ध्यान देते हैं

C. तुरंत सामने मिलते हैं

D. हमेशा उपहार भेजते हैं

4. कोई ऑनलाइन व्यक्ति वीडियो कॉल करने से लगातार क्यों बच सकता है?

A. कैमरा हमेशा खराब होता है

B. वह शर्माता है

C. वह तस्वीरों में दिख रहे व्यक्ति से अलग हो सकता है

D. उसे मैसेज करना पसंद है

5. रोमांस स्कैम का सामान्य रेड फ्लैग क्या है?

A. सही व्याकरण

B. जल्दी पैसे की मांग करना

C. सामान्य बातचीत

D. शौक साझा करना

6. ऑनलाइन ग्रूमिंग अक्सर किस तरह शुरू होती है?

A. धीरे-धीरे दोस्ती और भरोसा बनाकर

B. बैंक पासवर्ड मांगकर

C. माता-पिता से मिलकर

D. आधिकारिक दस्तावेज भेजकर

7. नकली गिवअवे स्कैमर आम तौर पर पीड़ित से क्या करवाते हैं?

A. प्रोसेसिंग फीस भरवाना

B. मुफ्त उपहार लेना

C. पार्क जाना

D. स्टडी ग्रुप में शामिल होना

8. क्रिप्टो स्कैम प्रमोशन आम तौर पर क्या दावा करते हैं?

A. कम रिटर्न

B. गारंटीड बहुत अधिक मुनाफा

C. सामान्य मार्केट ग्रोथ

D. धीमा निवेश

9. इम्पर्सोनेशन स्कैम में अक्सर किसका उपयोग किया जाता है?

A. केवल वेरिफाइड अकाउंट

B. थोड़े बदले हुए यूज़रनेम

C. सरकारी वेबसाइट

D. स्कूल ID

10. किस स्थिति में गिवअवे नकली होने की आशंका अधिक होती है?

A. बिना भरोसेमंद प्रमाण के बड़े इनाम का दावा किया जाए

B. पिछले विजेताओं की पुष्टि हो

C. आधिकारिक वेबसाइट पर जानकारी हो

D. नियम और शर्तें स्पष्ट हों

11. रिवर्स इमेज सर्च किस काम में मदद करता है?

A. फोन नंबर ढूँढने में

B. यह जांचने में कि प्रोफाइल फोटो कहीं से ली गई है या नहीं

C. इमेज की क्वालिटी सुधारने में

D. नई तस्वीर बनाने में

12. यूज़रनेम लुकअप से क्या पता लगाने में मदद मिल सकती है?

A. व्यक्ति का घर का पता

B. वही यूज़रनेम इस्तेमाल करने वाले अन्य ऑनलाइन अकाउंट

C. मोबाइल रिचार्ज ऑफर

D. ऑफलाइन लोकेशन

13. तस्वीर का मेटाडेटा क्या जानकारी दे सकता है?

A. मौसम की जानकारी

B. तस्वीर बनने की तारीख या समय जैसी छुपी जानकारी

C. मूवी फाइल

D. शॉपिंग हिस्ट्री

14. नकली प्रोफाइल का व्यवहारिक रेड फ्लैग कौन-सा हो सकता है?

A. रोजमर्रा की फोटो पोस्ट करना

B. बहुत से लोगों को एक जैसे मैसेज भेजना

C. पुराने पोस्ट होना

D. परिवार या दोस्तों के साथ टैग होना

15. फेक अकाउंट में आम तौर पर कौन-सी बात दिखाई दे सकती है?

A. बहुत कम पोस्ट और हाल ही में बनाया गया अकाउंट

B. लंबा और नियमित इतिहास

C. वास्तविक जीवन का नेटवर्क

D. पुरानी गतिविधियों का रिकॉर्ड

16. यदि कोई अनजान व्यक्ति सोशल मीडिया पर लगातार परेशान करने वाले संदेश भेजता है, तो क्या करना चाहिए?

A. उसे व्यक्तिगत जानकारी देना

B. उसे ब्लॉक और रिपोर्ट करना

C. उसके संदेश आगे भेजना

D. बातचीत जारी रखना

17. सोशल मीडिया पर किसी व्यक्ति की नकली पहचान बनाकर दूसरों को संदेश भेजना क्या कहलाता है?

A. इम्पर्सोनेशन

B. डेटा बैकअप

C. टू-फैक्टर ऑथेंटिकेशन

D. अकाउंट रिकवरी

18. यदि अकाउंट हैक हो जाए, तो पहला उचित कदम क्या है?

A. नया अकाउंट बना लेना

B. प्लेटफॉर्म का अकाउंट रिकवरी विकल्प इस्तेमाल करना

C. दो दिन इंतजार करना

D. अजनबियों को जानकारी देना

19. टू-फैक्टर ऑथेंटिकेशन (2FA) किस तरह मदद करता है?

A. लॉगिन तेज बनाकर

B. सुरक्षा की दूसरी परत जोड़कर

C. पासवर्ड अपने-आप सेव करके

D. फोटो छुपाकर

20. यदि किसी गिवअवे में भाग लेने के लिए आपसे OTP मांगा जाए, तो क्या करना चाहिए?

A. तुरंत OTP साझा करना

B. OTP केवल दोस्तों को देना

C. OTP साझा न करना और ऑफर की जांच करना

D. बैंक पासवर्ड भी देना

Module - 3

Identity Theft & Personal Data Leaks

1. क्रेडेंशियल स्टफिंग में साइबर अपराधी क्या करते हैं?

A. चोरी किए गए पासवर्ड को कई वेबसाइटों पर आज़माते हैं

B. कंप्यूटर की स्क्रीन साफ करते हैं

C. नया ईमेल अकाउंट बनाते हैं

D. इंटरनेट की गति बढ़ाते हैं

2. यदि कोई व्यक्ति कई वेबसाइटों पर एक ही पासवर्ड इस्तेमाल करता है, तो क्या खतरा हो सकता है?

A. एक अकाउंट का पासवर्ड लीक होने पर दूसरे अकाउंट भी खतरे में आ सकते हैं

B. सभी अकाउंट अपने-आप सुरक्षित हो जाते हैं

C. इंटरनेट बंद हो जाता है

D. फोन की बैटरी जल्दी चार्ज होती है

3. कई बार अनजान स्थानों से लॉगिन के असफल प्रयास दिखाई देना किसका संकेत हो सकता है?

A. क्रेडेंशियल स्टफिंग का प्रयास

B. सामान्य सॉफ्टवेयर अपडेट

C. फोटो बैकअप

D. ऑनलाइन खरीदारी

4. ऑनलाइन अकाउंट सुरक्षित रखने के लिए कौन-सी आदत सही है?

A. हर वेबसाइट पर एक ही पासवर्ड रखना

B. मजबूत और अलग-अलग पासवर्ड रखना

C. पासवर्ड दोस्तों को बताना

D. पासवर्ड को सार्वजनिक पोस्ट करना

5. हैकर्स को किसी व्यक्ति के पुराने पासवर्ड कहाँ से मिल सकते हैं?

A. दूसरी वेबसाइटों के डेटा ब्रीच से

B. मौसम की वेबसाइट से

C. ऑनलाइन गेम के स्कोर से

D. फोन की स्क्रीन से

6. कॉल स्पूफिंग का क्या अर्थ है?

A. कॉल में आवाज़ बदलना

B. कॉलर ID में नकली नंबर या पहचान दिखाना

C. बिना सिम कार्ड के संदेश भेजना

D. फोन की घंटी बंद करना

7. फर्जी कस्टमर केयर कॉल करने वाला व्यक्ति किसका रूप धारण कर सकता है?

A. बैंक या टेलीकॉम कंपनी के प्रतिनिधि का

B. स्कूल के सहपाठी का

C. डिलीवरी वाहन का

D. मौसम रिपोर्टर का

8. यदि कोई कथित बैंक कर्मचारी फोन पर OTP या PIN मांगे, तो क्या करना चाहिए?

A. उसे OTP या PIN बता देना

B. कॉल काटकर बैंक के आधिकारिक नंबर से संपर्क करना

C. OTP मैसेज उसे पढ़कर सुनाना

D. अपना पासवर्ड भी भेज देना

9. किसी कस्टमर केयर नंबर की सत्यता जांचने का सुरक्षित तरीका क्या है?

A. सोशल मीडिया कमेंट में मिले नंबर पर भरोसा करना

B. बैंक या कंपनी की आधिकारिक वेबसाइट/ऐप से नंबर लेना

C. अनजान व्यक्ति से नंबर मांगना

D. किसी भी सर्च विज्ञापन पर क्लिक करना

10. कॉलर ID स्पूफिंग से धोखा देना आसान क्यों हो सकता है?

A. कॉल पर असली संस्था जैसा नंबर दिखाई दे सकता है

B. फोन हमेशा बंद हो जाता है

C. कॉल की आवाज़ साफ नहीं आती

D. मोबाइल में नेटवर्क बढ़ जाता है

11. व्यक्तिगत डेटा लीक किस स्थिति में होता है?

A. जानकारी का सुरक्षित बैकअप बनने पर

B. व्यक्तिगत जानकारी बिना अनुमति उजागर होने पर

C. ऐप अपडेट होने पर

D. उपयोगकर्ता पासवर्ड बदलने पर

12. डोमिनोज़ इंडिया से जुड़े डेटा लीक में किस तरह की जानकारी उजागर होने की खबर थी?

A. ग्राहकों के फोन नंबर और पते

B. पिज्जा बनाने की रेसिपी

C. डिलीवरी बाइक की कीमत

D. स्टोर का किराया

13. बिगबास्केट डेटा लीक में किस प्रकार की उपयोगकर्ता जानकारी शामिल थी?

A. ईमेल, पासवर्ड और फोन नंबर

B. केवल किराने की दुकान का समय

C. केवल उत्पादों की कीमत

D. डिलीवरी वाहनों का रंग

14. अनएकेडमी डेटा लीक में किस प्रकार की जानकारी उजागर हुई थी?

A. उपयोगकर्ताओं के ईमेल और पासवर्ड

B. परीक्षा केंद्रों की इमारतें

C. शिक्षकों की छुट्टियों की सूची

D. कक्षा की सीटों की संख्या

15. डेटा लीक के बाद व्यक्ति को किस खतरे का सामना करना पड़ सकता है?

A. स्कैम और स्पैम संदेशों का खतरा बढ़ना

B. इंटरनेट की गति बढ़ना

C. फोन की मेमोरी बढ़ना

D. सभी अकाउंट अपने-आप बंद होना

16. किसी संदिग्ध QR कोड को स्कैन करने पर क्या खतरा हो सकता है?

A. व्यक्तिगत जानकारी चुराने वाली वेबसाइट खुल सकती है

B. फोन अपने-आप सुरक्षित हो जाता है

C. बैटरी चार्ज हो जाती है

D. स्क्रीन की चमक बढ़ जाती है

17. QR कोड स्कैन करने के बाद यदि कोई अनजान वेबसाइट खुले, तो क्या करना चाहिए?

A. उसमें तुरंत अपनी बैंक जानकारी भरना

B. वेबसाइट की जांच किए बिना आगे न बढ़ना

C. OTP दर्ज करना

D. लिंक को सभी दोस्तों को भेजना

18. QR कोड के जरिए पेमेंट स्कैम से बचने के लिए क्या याद रखना चाहिए?

A. पैसे प्राप्त करने के लिए हमेशा PIN डालना जरूरी है

B. पेमेंट करने से पहले प्राप्तकर्ता और राशि जांचें; PIN/OTP साझा न करें

C. हर QR कोड सुरक्षित होता है

D. अनजान व्यक्ति के निर्देश पर पेमेंट करें

19. QR कोड स्कैन करने के लिए सबसे सुरक्षित विकल्प कौन-सा है?

A. किसी भी अनजान पोस्टर का QR कोड

B. विश्वसनीय और सत्यापित स्रोत से मिला QR कोड

C. सड़क पर लगा कोई भी QR कोड

D. अनजान संदेश में भेजा गया QR कोड

20. यदि किसी ने असली QR कोड के ऊपर नकली QR कोड चिपका दिया हो, तो क्या जोखिम हो सकता है?

A. पेमेंट गलत खाते में जा सकता है या नकली लिंक खुल सकता है

B. फोन की स्क्रीन टूट सकती है

C. मोबाइल की बैटरी बढ़ सकती है

D. कॉन्टैक्ट अपने-आप सेव हो सकते हैं

Module - 4

Online Financial Frauds & Digital Payments Security

प्रश्न 1. ऑनलाइन वित्तीय धोखाधड़ी (Online Financial Fraud) क्या है?

a) सुरक्षित ऑनलाइन खरीदारी

b) डिजिटल प्लेटफॉर्म के माध्यम से किसी को धोखा देकर पैसे चुराना

c) बैंक बैलेंस चेक करना

d) ऑनलाइन बिजली बिल का भुगतान करना

प्रश्न 2. UPI का पूरा नाम क्या है?

a) यूनिफाइड पेमेंट इंटरफेस

b) यूनिफाइड पेमेंट्स इंटरफेस

c) यूनिवर्सल पेमेंट इंडिया

d) यूनिक पेमेंट आइडेंटिफिकेशन

प्रश्न 3. यदि कोई व्यक्ति पैसे प्राप्त करने के लिए आपका UPI PIN मांगता है, तो आपको क्या करना चाहिए?

a) अपना PIN साझा करना चाहिए

b) WhatsApp पर PIN भेज देना चाहिए

c) अपना UPI PIN कभी साझा नहीं करना चाहिए

d) केवल PIN के पहले दो अंक बताने चाहिए

प्रश्न 4. फिशिंग (Phishing) क्या है?

a) ऑनलाइन खरीदारी का एक तरीका

b) नकली संदेशों या वेबसाइटों के माध्यम से गोपनीय जानकारी चुराने की धोखाधड़ी

c) सुरक्षित बैंकिंग का तरीका

d) पैसे ट्रांसफर करने का तरीका

प्रश्न 5. OTP का पूरा नाम क्या है?

a) वन टाइम पासवर्ड

b) ऑनलाइन ट्रांसफर प्रोसेस

c) वन ट्रांसफर पेमेंट

d) ऑफिशियल ट्रांजैक्शन पासवर्ड

प्रश्न 6. क्या आपको अपना OTP किसी के साथ साझा करना चाहिए?

a) हाँ, बैंक कर्मचारियों के साथ

b) हाँ, दोस्तों के साथ

c) केवल फोन कॉल पर

d) नहीं, अपना OTP कभी साझा नहीं करना चाहिए

प्रश्न 7. ऑनलाइन भुगतान करते समय कौन-सी सुरक्षित आदत है?

a) बैंकिंग के लिए सार्वजनिक Wi-Fi का उपयोग करना

b) अनजान लोगों के साथ कार्ड की जानकारी साझा करना

c) विश्वसनीय और सुरक्षित वेबसाइटों का उपयोग करना

d) अनजान पेमेंट लिंक पर क्लिक करना

प्रश्न 8. डिजिटल भुगतान में QR कोड का सामान्य उपयोग किस लिए किया जाता है?

a) स्कैन करके भुगतान करने के लिए

b) मोबाइल स्टोरेज बढ़ाने के लिए

c) फोन कॉल ब्लॉक करने के लिए

d) एंटीवायरस डाउनलोड करने के लिए

प्रश्न 9. किसी अनजान QR कोड को स्कैन करने से पहले आपको क्या करना चाहिए?

a) तुरंत स्कैन करना चाहिए

b) उसके स्रोत और उद्देश्य की जांच करनी चाहिए

c) उसे दोस्तों के साथ साझा करना चाहिए

d) अपना बैंकिंग पासवर्ड डालना चाहिए

प्रश्न 10. नकली बैंकिंग संदेश की सामान्य पहचान क्या है?

a) उसमें आधिकारिक जानकारी दी गई हो

b) उसमें तुरंत किसी अनजान लिंक पर क्लिक करने के लिए कहा गया हो

c) वह बैंक के सत्यापित एप्लिकेशन से आया हो

d) उसमें बैंक शाखा का पता दिया गया हो

प्रश्न 11. डेबिट कार्ड का उपयोग किस लिए किया जाता है?

a) बैंक खाते से पैसे निकालने और भुगतान करने के लिए

b) सोशल मीडिया अकाउंट बनाने के लिए

c) ईमेल भेजने के लिए

d) इंटरनेट की गति बढ़ाने के लिए

प्रश्न 12. कार्ड स्किमिंग (Card Skimming) क्या है?

a) ATM की स्क्रीन साफ करना

b) छिपे हुए या अनधिकृत उपकरण से कार्ड की जानकारी चुराना

c) ATM में पैसे जमा करना

d) खाते का बैलेंस चेक करना

प्रश्न 13. निम्नलिखित में से कौन-सी जानकारी सार्वजनिक रूप से साझा नहीं करनी चाहिए?

a) आपका पसंदीदा रंग

b) आपके बैंक खाते का बैलेंस

c) आपका ATM PIN और OTP

d) आपके शहर का नाम

प्रश्न 14. यदि बैंकिंग ऐप वाला आपका मोबाइल फोन खो जाता है, तो आपको क्या करना चाहिए?

a) इसे नजरअंदाज करना चाहिए

b) बैंक को सूचित करके बैंकिंग सेवाओं का एक्सेस ब्लॉक करवाना चाहिए

c) अपने फोन का पासवर्ड ऑनलाइन साझा करना चाहिए

d) किसी के फोन लौटाने का इंतजार करना चाहिए

प्रश्न 15. नकली कस्टमर केयर नंबर स्कैम क्या है?

a) बैंक के आधिकारिक नंबर पर कॉल करना

b) धोखेबाज व्यक्ति द्वारा कस्टमर सपोर्ट बनकर जानकारी या पैसे चुराना

c) बैंक की जानकारी चेक करना

d) बैंक स्टेटमेंट प्राप्त करना

प्रश्न 16. यदि आपको कोई अनजान पेमेंट लिंक प्राप्त होता है, तो आपको क्या करना चाहिए?

a) तुरंत उस पर क्लिक करना चाहिए

b) उसे सभी लोगों को फॉरवर्ड करना चाहिए

c) खोलने से पहले भेजने वाले की जांच करनी चाहिए

d) अपना UPI PIN डालना चाहिए

प्रश्न 17. एक मजबूत बैंकिंग पासवर्ड में क्या होना चाहिए?

a) केवल आपका नाम

b) आपकी जन्मतिथि

c) अक्षरों, संख्याओं और विशेष चिन्हों का संयोजन

d) केवल 123456

प्रश्न 18. टू-फैक्टर ऑथेंटिकेशन (2FA) का उद्देश्य क्या है?

a) इंटरनेट की गति बढ़ाना

b) सुरक्षा की एक अतिरिक्त परत प्रदान करना

c) बैंक रिकॉर्ड हटाना

d) सभी बैंकिंग शुल्क समाप्त करना

प्रश्न 19. यदि आपको अपने बैंक खाते में कोई अनधिकृत लेन-देन दिखाई देता है, तो आपको क्या करना चाहिए?

a) लेन-देन को नजरअंदाज करना चाहिए

b) एक महीने तक इंतजार करना चाहिए

c) तुरंत बैंक से संपर्क करके शिकायत दर्ज करनी चाहिए

d) कस्टमर केयर को अपना OTP बताना चाहिए

प्रश्न 20. भारत में साइबर वित्तीय धोखाधड़ी की शिकायत करने के लिए कौन-सा आधिकारिक हेल्पलाइन नंबर उपयोग किया जा सकता है?

a) 100

b) 101

c) 1930

d) 108

प्रश्न 1. डिजिटल परिवेश (Digital Landscape) से क्या तात्पर्य है?

a) केवल कंप्यूटर का उपयोग करना

b) इंटरनेट, डिजिटल उपकरणों और ऑनलाइन प्लेटफॉर्म का वातावरण

c) केवल मोबाइल फोन का उपयोग करना

d) केवल सोशल मीडिया का उपयोग करना

प्रश्न 2. ऑनलाइन सुरक्षा का मुख्य उद्देश्य क्या है?

a) इंटरनेट का उपयोग बंद करना

b) सोशल मीडिया अकाउंट हटाना

c) व्यक्तिगत जानकारी और डिजिटल पहचान की सुरक्षा करना

d) सभी वेबसाइटों पर पंजीकरण करना

प्रश्न 3. निम्नलिखित में से कौन-सा एक सामान्य ऑनलाइन खतरा है?

a) फ़िशिंग

b) ऑनलाइन शिक्षा

c) वीडियो कॉन्फ्रेंसिंग

d) डिजिटल भुगतान

प्रश्न 4. सोशल मीडिया पर किसी अजनबी द्वारा भेजे गए संदिग्ध लिंक के साथ क्या करना चाहिए?

a) तुरंत खोलना चाहिए

b) सभी दोस्तों को भेजना चाहिए

c) उस पर अपनी व्यक्तिगत जानकारी दर्ज करनी चाहिए

d) लिंक खोलने से बचना चाहिए और उसकी रिपोर्ट करनी चाहिए

प्रश्न 5. सोशल मीडिया पर व्यक्तिगत जानकारी साझा करते समय क्या सावधानी रखनी चाहिए?

a) घर का पता सार्वजनिक करना

b) केवल आवश्यक जानकारी साझा करना

c) बैंक विवरण साझा करना

d) पासवर्ड साझा करना

प्रश्न 6. साइबरबुलिंग (Cyberbullying) क्या है?

a) ऑनलाइन शिक्षा प्रदान करना

b) इंटरनेट पर सुरक्षित खरीदारी करना

c) डिजिटल माध्यमों से किसी व्यक्ति को परेशान या अपमानित करना

d) सोशल मीडिया पर फोटो साझा करना

प्रश्न 7. साइबरबुलिंग का शिकार होने पर सबसे उचित कदम क्या है?

a) सबूत सुरक्षित रखना और संबंधित प्लेटफॉर्म पर रिपोर्ट करना

b) बदले में धमकी देना

c) सभी संदेशों को तुरंत डिलीट करना

d) अपनी निजी जानकारी सार्वजनिक करना

प्रश्न 8. साइबरबुलिंग के संकेतों में से कौन-सा एक संकेत हो सकता है?

a) ऑनलाइन पढ़ाई में रुचि बढ़ना

b) नए दोस्तों से मिलना

c) इंटरनेट की गति बढ़ना

d) ऑनलाइन गतिविधियों के बाद डर या तनाव महसूस करना

प्रश्न 9. साइबरस्टॉकिंग (Cyberstalking) का क्या अर्थ है?

a) इंटरनेट पर शैक्षणिक सामग्री खोजना

b) डिजिटल माध्यमों से किसी व्यक्ति का बार-बार पीछा करना या निगरानी करना

c) ऑनलाइन गेम खेलना

d) सोशल मीडिया पर सामान्य बातचीत करना

प्रश्न 10. फर्जी विवाह (Fake Matrimony) और डेटिंग स्कैम का मुख्य उद्देश्य क्या हो सकता है?

a) लोगों को ऑनलाइन शिक्षा देना

b) नए दोस्त बनाना

c) धोखाधड़ी से पैसे या व्यक्तिगत जानकारी प्राप्त करना

d) डिजिटल साक्षरता बढ़ाना

प्रश्न 11. Blue Whale और Momo Challenge जैसे ऑनलाइन खतरों से बच्चों को बचाने का सबसे अच्छा तरीका क्या है?

a) बच्चों की ऑनलाइन गतिविधियों पर उचित निगरानी और जागरूकता रखना

b) बच्चों को अजनबियों से बात करने के लिए प्रोत्साहित करना

c) सभी संदिग्ध संदेशों को अनदेखा करना

d) बच्चों को बिना निगरानी के इंटरनेट इस्तेमाल करने देना

प्रश्न 12. व्यक्तिगत जानकारी (Personal Information) का उदाहरण कौन-सा है?

a) सामान्य मौसम की जानकारी

b) सार्वजनिक समाचार

c) सामान्य शैक्षणिक लेख

d) घर का पता और मोबाइल नंबर

प्रश्न 13. ऑनलाइन गोपनीयता (Online Privacy) बनाए रखने के लिए क्या करना चाहिए?

a) पासवर्ड सभी के साथ साझा करना

b) मजबूत पासवर्ड और प्राइवेसी सेटिंग्स का उपयोग करना

c) सभी सोशल मीडिया पोस्ट सार्वजनिक रखना

d) अजनबियों को व्यक्तिगत फोटो भेजना

प्रश्न 14. बच्चों की ऑनलाइन गोपनीयता की सुरक्षा के लिए माता-पिता को क्या करना चाहिए?

a) बच्चों को सभी वेबसाइटों पर स्वतंत्र रूप से जानकारी साझा करने देना

b) बच्चों के पासवर्ड सार्वजनिक करना

c) उम्र के अनुसार सुरक्षित प्लेटफॉर्म और पैरेंटल कंट्रोल का उपयोग करना

d) ऑनलाइन गतिविधियों पर कोई ध्यान न देना

प्रश्न 15. होटल के कमरे में छिपे हुए कैमरे का संदेह होने पर क्या करना चाहिए?

a) संदिग्ध वस्तु या उपकरण की जांच करना, सुरक्षित स्थान पर जाना और संबंधित अधिकारियों को सूचित करना

b) कैमरे को तोड़ देना

c) संदिग्ध उपकरण को घर ले जाना

d) घटना को पूरी तरह अनदेखा करना

प्रश्न 16. ऑनलाइन उत्पीड़न (Online Harassment) का सामना करने पर क्या करना चाहिए?

a) उत्पीड़क को व्यक्तिगत जानकारी देना

b) धमकी का जवाब धमकी से देना

c) सभी सबूत तुरंत मिटा देना

d) सबूत सुरक्षित रखना, ब्लॉक करना और शिकायत दर्ज करना

प्रश्न 17. एक सुरक्षित ऑनलाइन समुदाय (Safe Online Community) की विशेषता क्या है?

a) अपमानजनक टिप्पणियों को बढ़ावा देना

b) सम्मानजनक व्यवहार और सुरक्षित संवाद को प्रोत्साहित करना

c) व्यक्तिगत जानकारी सार्वजनिक करना

d) साइबरबुलिंग को अनदेखा करना

प्रश्न 18. ऑनलाइन प्लेटफॉर्म पर हानिकारक सामग्री (Harmful Content) मिलने पर क्या करना चाहिए?

a) उसे अधिक लोगों तक पहुंचाना

b) उसे बिना जांचे साझा करना

c) प्लेटफॉर्म पर उसकी रिपोर्ट करना

d) उस पर अपनी व्यक्तिगत जानकारी देना

प्रश्न 19. ऑनलाइन सुरक्षा के बारे में जागरूकता बढ़ाने का एक प्रभावी तरीका क्या है?

a) नियमित साइबर सुरक्षा जागरूकता प्रशिक्षण और शिक्षा

b) इंटरनेट का उपयोग पूरी तरह बंद करना

c) पासवर्ड साझा करना

d) संदिग्ध लिंक खोलना

प्रश्न 20. ऑनलाइन समुदाय में सकारात्मक वातावरण बनाने के लिए क्या करना चाहिए?

a) दूसरों को परेशान करना

b) गलत जानकारी फैलाना

c) अपमानजनक भाषा का उपयोग करना

d) सम्मान, जिम्मेदारी और सुरक्षित व्यवहार को बढ़ावा देना

Module – 6 Dark Web, Cyber Terrorism & Illegal Activities

प्रश्न 1. डार्क वेब (Dark Web) क्या है?

a) इंटरनेट का सामान्य और सार्वजनिक हिस्सा

b) इंटरनेट का ऐसा हिस्सा जिसे सामान्य सर्च इंजन से आसानी से एक्सेस नहीं किया जा सकता

c) केवल सोशल मीडिया वेबसाइटों का समूह

d) केवल शैक्षणिक वेबसाइटों का समूह

प्रश्न 2. डार्क वेब तक पहुंचने के लिए सामान्यतःकिस ब्राउज़र का उपयोग किया जाता है?

a) Google Chrome

b) Microsoft Edge

c) Tor Browser

d) Internet Explorer

प्रश्न 3. Deep Web और Dark Web के बीच मुख्य अंतर क्या है?

a) Deep Web में सामान्य सर्च इंजन से इंडेक्स नहीं किए गए पेज शामिल होते हैं, जबकि Dark Web के लिए विशेष सॉफ्टवेयर या कॉन्फ़िगरेशन की आवश्यकता हो सकती है

b) दोनों बिल्कुल समान हैं

c) Dark Web केवल सरकारी वेबसाइटों के लिए होता है

d) Deep Web केवल सोशल मीडिया तक सीमित है

प्रश्न 4. Tor नेटवर्क का मुख्य उद्देश्य क्या है?

a) इंटरनेट की गति बढ़ाना

b) फाइलों को एन्क्रिप्ट करना

c) कंप्यूटर की स्टोरेज बढ़ाना

d) उपयोगकर्ता की पहचान और इंटरनेट गतिविधियों की गोपनीयता बनाए रखने में मदद करना

प्रश्न 5. Operation Onymous किस वर्ष आयोजित किया गया था?

a) 2012

b) 2014

c) 2017

d) 2021

प्रश्न 6. Operation Onymous का मुख्य उद्देश्य क्या था?

a) ऑनलाइन शिक्षा को बढ़ावा देना

b) इंटरनेट की गति बढ़ाना

c) डार्क वेब पर अवैध मार्केटप्लेस और संबंधित गतिविधियों के विरुद्ध कार्रवाई करना

d) सोशल मीडिया अकाउंट बनाना

प्रश्न 7. Emotet को मुख्य रूप से किस प्रकार के खतरे के रूप में जाना जाता है?

a) मैलवेयर और बॉटनेट

b) एंटीवायरस सॉफ्टवेयर

c) वेब ब्राउज़र

d) डेटा बैकअप टूल

प्रश्न 8. Emotet बॉटनेट को निष्क्रिय करने के लिए अंतरराष्ट्रीय स्तर पर कार्रवाई किस वर्ष की गई थी?

a) 2015

b) 2017

c) 2019

d) 2021

प्रश्न 9. WannaCry रैनसमवेयर हमला किस वर्ष हुआ था?

a) 2014

b) 2017

c) 2020

d) 2022

प्रश्न 10. साइबर आतंकवाद (Cyber Terrorism) का क्या अर्थ है?

a) सामान्य ऑनलाइन खरीदारी करना

b) सोशल मीडिया पर फोटो साझा करना

c) राजनीतिक या वैचारिक उद्देश्यों से डिजिटल प्रणालियों पर हमला करके भय या व्यवधान उत्पन्न करना

d) ऑनलाइन शिक्षा प्रदान करना

प्रश्न 11. साइबर आतंकवाद का संभावित लक्ष्य कौन-सा हो सकता है?

a) महत्वपूर्ण सरकारी और सार्वजनिक अवसंरचना

b) केवल व्यक्तिगत फोटो

c) केवल मनोरंजन वेबसाइटें

d) केवल ऑनलाइन गेम

प्रश्न 12. निम्नलिखित में से कौन-सी गतिविधि साइबर आतंकवाद का उदाहरण हो सकती है?

a) सुरक्षित वेबसाइट बनाना

b) ऑनलाइन बैंकिंग करना

c) सॉफ्टवेयर अपडेट करना

d) महत्वपूर्ण सरकारी नेटवर्क पर विनाशकारी साइबर हमला करना

प्रश्न 13. डार्क वेब पर अवैध गतिविधियों का एक उदाहरण क्या है?

a) ऑनलाइन शिक्षा

b) अवैध वस्तुओं और सेवाओं का व्यापार

c) सरकारी सूचना पोर्टल

d) डिजिटल लाइब्रेरी

प्रश्न 14. डार्क वेब मार्केटप्लेस पर साइबर अपराधी किस प्रकार की गतिविधियां कर सकते हैं?

a) ऑनलाइन पाठ्यक्रम उपलब्ध कराना

b) सार्वजनिक समाचार साझा करना

c) चोरी किए गए डेटा और अवैध सेवाओं का व्यापार करना

d) सरकारी योजनाओं का प्रचार करना

प्रश्न 15. डार्क वेब पर चोरी किए गए व्यक्तिगत डेटा का दुरुपयोग किसलिए किया जा सकता है?

a) पहचान की चोरी और वित्तीय धोखाधड़ी

b) ऑनलाइन शिक्षा

c) इंटरनेट की गति बढ़ाना

d) डेटा बैकअप बनाना

प्रश्न 16. साइबर अपराध में बॉटनेट (Botnet) का क्या अर्थ है?

a) सुरक्षित कंप्यूटर नेटवर्क

b) कंप्यूटरों का एक सामान्य समूह

c) केवल एंटीवायरस उपकरणों का समूह

d) संक्रमित उपकरणों का समूह जिसे हमलावर दूर से नियंत्रित कर सकता है

प्रश्न 17. डार्क वेब से संबंधित खतरों की निगरानी के लिए कौन-सा ओपन-सोर्स टूल उपयोगी हो सकता है?

a) Microsoft Word

b) Ahmia Search Engine

c) Paint

d) Calculator

प्रश्न 18. डार्क वेब पर संदिग्ध गतिविधियों की जांच करते समय सबसे महत्वपूर्ण सुरक्षा सावधानी क्या है?

a) अज्ञात फाइलें डाउनलोड करना

b) व्यक्तिगत जानकारी साझा करना

c) सुरक्षित और नियंत्रित वातावरण में केवल अधिकृत जांच करना

d) संदिग्ध लिंक पर क्लिक करना

प्रश्न 19. साइबर आतंकवाद और डार्क वेब अपराधों का समाज पर क्या प्रभाव हो सकता है?

a) आर्थिक नुकसान, सुरक्षा जोखिम और सार्वजनिक भय

b) इंटरनेट की गति में वृद्धि

c) डिजिटल साक्षरता में स्वतःसुधार

d) डेटा की सुरक्षा में वृद्धि

प्रश्न 20. डार्क वेब और साइबर आतंकवाद से निपटने का प्रभावी तरीका कौन-सा है?

a) साइबर अपराधों को अनदेखा करना

b) संदिग्ध गतिविधियों को साझा करना

c) सुरक्षा अपडेट बंद करना

d) साइबर सुरक्षा जागरूकता, कानून प्रवर्तन और अंतरराष्ट्रीय सहयोग

Module -7 Cyber Hygiene

प्रश्न 1. साइबर हाइजीन (Cyber Hygiene) क्या है?

a) कंप्यूटर की बाहरी सफाई करना

b) डिजिटल उपकरणों और जानकारी को सुरक्षित रखने के लिए नियमित सुरक्षा उपाय अपनाना

c) इंटरनेट की गति बढ़ाना

d) कंप्यूटर में गेम इंस्टॉल करना

प्रश्न 2. निम्नलिखित में से कौन-सा एक मजबूत पासवर्ड है?

a) 123456

b) password

c) Rahul123

d) R@h7#Lq92!

प्रश्न 3. आपको अपने सॉफ्टवेयर और ऑपरेटिंग सिस्टम को कितनी बार अपडेट करना चाहिए?

a) कभी नहीं

b) केवल तब जब कंप्यूटर काम करना बंद कर दे

c) नियमित रूप से, जब भी सुरक्षा अपडेट उपलब्ध हों

d) पांच साल में एक बार

प्रश्न 4. एंटीवायरस सॉफ्टवेयर का उद्देश्य क्या है?

a) स्क्रीन की ब्राइटनेस बढ़ाना

b) हानिकारक सॉफ्टवेयर का पता लगाना, उसे रोकना और हटाना

c) इंटरनेट की गति बढ़ाना

d) डॉक्यूमेंट बनाना

प्रश्न 5. किसी अनजान व्यक्ति से प्राप्त लिंक पर क्लिक करने से पहले आपको क्या करना चाहिए?

a) तुरंत क्लिक करना चाहिए

b) दोस्तों को फॉरवर्ड करना चाहिए

c) भेजने वाले की पहचान और लिंक की जांच करनी चाहिए

d) अपना पासवर्ड डालना चाहिए

प्रश्न 6. मल्टी-फैक्टर ऑथेंटिकेशन (MFA) क्या है?

a) कई कंप्यूटरों का उपयोग करना

b) किसी अकाउंट में लॉगिन करने के लिए दो या अधिक सत्यापन तरीकों का उपयोग करना

c) कई ईमेल अकाउंट बनाना

d) रोजाना कंप्यूटर का पासवर्ड बदलना

प्रश्न 7. एक ही पासवर्ड का उपयोग कई अकाउंट में क्यों नहीं करना चाहिए?

a) इससे इंटरनेट का उपयोग बढ़ता है

b) यदि एक अकाउंट हैक हो जाता है, तो अन्य अकाउंट भी खतरे में पड़ सकते हैं

c) इससे कंप्यूटर की कार्यक्षमता कम हो जाती है

d) इससे आपकी फाइलें डिलीट हो जाती हैं

प्रश्न 8. कंप्यूटर को बिना देखरेख के छोड़ते समय आपको क्या करना चाहिए?

a) उसे अनलॉक छोड़ देना चाहिए

b) एंटीवायरस बंद कर देना चाहिए

c) कंप्यूटर की स्क्रीन लॉक कर देनी चाहिए

d) अपना पासवर्ड साझा करना चाहिए

प्रश्न 9. फिशिंग (Phishing) क्या है?

a) कंप्यूटर को सुरक्षित करने का तरीका

b) साइबर हमला जिसमें उपयोगकर्ता को धोखा देकर गोपनीय जानकारी प्राप्त की जाती है

c) डेटा बैकअप लेने का तरीका

d) कंप्यूटर हार्डवेयर का एक प्रकार

प्रश्न 10. नियमित रूप से डेटा बैकअप लेना क्यों जरूरी है?

a) स्क्रीन का रिजॉल्यूशन बढ़ाने के लिए

b) डेटा गलती से डिलीट होने, सिस्टम खराब होने या साइबर हमले की स्थिति में उसे वापस प्राप्त करने के लिए

c) बैटरी की लाइफ बढ़ाने के लिए

d) टाइपिंग की गति बढ़ाने के लिए

प्रश्न 11. सार्वजनिक Wi-Fi का उपयोग करते समय कौन-सी सुरक्षित आदत है?

a) बिना सुरक्षा के बैंकिंग वेबसाइट खोलना

b) सार्वजनिक Wi-Fi पर पासवर्ड साझा करना

c) असुरक्षित सार्वजनिक Wi-Fi पर संवेदनशील लेन-देन से बचना

d) सभी सुरक्षा सेटिंग बंद कर देना

प्रश्न 12. यदि आपको ईमेल में कोई अनपेक्षित अटैचमेंट प्राप्त होता है, तो आपको क्या करना चाहिए?

a) तुरंत खोलना चाहिए

b) डाउनलोड करके चलाना चाहिए

c) खोलने से पहले भेजने वाले की पहचान सत्यापित करनी चाहिए

d) सभी को फॉरवर्ड करना चाहिए

प्रश्न 13. फायरवॉल (Firewall) का उद्देश्य क्या है?

a) नेटवर्क में आने और जाने वाले ट्रैफिक को नियंत्रित करना

b) स्टोरेज क्षमता बढ़ाना

c) डिस्प्ले की गुणवत्ता बढ़ाना

d) अस्थायी फाइलें डिलीट करना

प्रश्न 14. सोशल मीडिया पर निम्नलिखित में से कौन-सी जानकारी साझा नहीं करनी चाहिए?

a) पसंदीदा फिल्म

b) सार्वजनिक समाचार

c) पासवर्ड, OTP और संवेदनशील व्यक्तिगत जानकारी

d) सामान्य रुचियां

प्रश्न 15. एप्लिकेशन केवल विश्वसनीय स्रोतों से ही डाउनलोड क्यों करनी चाहिए?

a) अधिक विज्ञापन प्राप्त करने के लिए

b) हानिकारक एप्लिकेशन इंस्टॉल होने के खतरे को कम करने के लिए

c) फोन का वजन बढ़ाने के लिए

d) कैमरे की गुणवत्ता बढ़ाने के लिए

प्रश्न 16. यदि आपको संदेह है कि आपका ईमेल अकाउंट हैक हो गया है, तो आपको क्या करना चाहिए?

a) स्थिति को नजरअंदाज करना चाहिए

b) अपना पासवर्ड दोस्तों के साथ साझा करना चाहिए

c) तुरंत पासवर्ड बदलना चाहिए और MFA चालू करना चाहिए

d) अपने सभी कॉन्टैक्ट डिलीट कर देने चाहिए

प्रश्न 17. मोबाइल फोन में स्क्रीन लॉक का क्या उद्देश्य है?

a) इंटरनेट की गति बढ़ाना

b) डिवाइस को अनधिकृत उपयोग से सुरक्षित रखना

c) स्टोरेज बढ़ाना

d) कैमरे की कार्यक्षमता बढ़ाना

प्रश्न 18. निम्नलिखित में से कौन-सी संवेदनशील व्यक्तिगत जानकारी का उदाहरण है?

a) पसंदीदा खेल

b) पसंदीदा रंग

c) बैंक खाते का विवरण और पहचान संबंधी जानकारी

d) पसंदीदा टेलीविजन कार्यक्रम

प्रश्न 19. किसी अनजान व्यक्ति से प्राप्त USB ड्राइव को कंप्यूटर से जोड़ने से पहले आपको क्या करना चाहिए?

a) सभी फाइलें तुरंत खोलनी चाहिए

b) अपडेटेड सुरक्षा सॉफ्टवेयर से उसे स्कैन करना चाहिए

c) एंटीवायरस बंद कर देना चाहिए

d) सभी फाइलें कंप्यूटर में कॉपी कर लेनी चाहिए

प्रश्न 20. निम्नलिखित में से कौन-सा साइबर हाइजीन का सबसे अच्छा उदाहरण है?

A. कमजोर पासवर्ड का उपयोग करना

B. सॉफ्टवेयर अपडेट को नजरअंदाज करना

C. डिवाइस को नियमित रूप से अपडेट करना, मजबूत पासवर्ड का उपयोग करना और डेटा बैकअप लेना

D. दूसरों के साथ OTP साझा करना

प्रश्न 1. रैनसमवेयर क्या है?

a) सिस्टम की कार्यक्षमता बढ़ाने वाला सॉफ्टवेयर

b) फाइलों को एन्क्रिप्ट करके फिरौती मांगने वाला मैलवेयर

c) डेटा बैकअप के लिए उपयोग किया जाने वाला सॉफ्टवेयर

d) एंटीवायरस सॉफ्टवेयर

प्रश्न 2. रैनसमवेयर का मुख्य उद्देश्य क्या है?

a) नेटवर्क की गति बढ़ाना

b) अस्थायी फाइलों को हटाना

c) सिस्टम के प्रदर्शन की निगरानी करना

d) डेटा तक पहुंच रोककर पैसे मांगना

प्रश्न 3. निम्नलिखित में से कौन-सा रैनसमवेयर का एक प्रकार है?

a) क्रिप्टो रैनसमवेयर

b) फायरवॉल रैनसमवेयर

c) ब्राउज़र रैनसमवेयर

d) बैकअप रैनसमवेयर

प्रश्न 4. रैनसमवेयर संक्रमण का सामान्य माध्यम कौन-सा है?

a) सॉफ्टवेयर अपडेट

b) डेटा बैकअप

c) दुर्भावनापूर्ण ईमेल अटैचमेंट

d) एंटीवायरस स्कैनिंग

प्रश्न 5. रैनसमवेयर हमलों में फ़िशिंग का क्या अर्थ है?

a) उपयोगकर्ताओं को धोखा देकर दुर्भावनापूर्ण लिंक खोलने या जानकारी साझा करने के लिए प्रेरित करना

b) बैकअप फाइलों को एन्क्रिप्ट करना

c) सुरक्षा अपडेट इंस्टॉल करना

d) नेटवर्क ट्रैफिक की निगरानी करना

प्रश्न 6. RDP का पूर्ण रूप क्या है?

a) रिमोट डेटा प्रोटेक्शन

b) रिमोट डेस्कटॉप प्रोटोकॉल

c) प्रतिबंधित डेटा प्रक्रिया

d) वास्तविक समय डेटा प्रसंस्करण

प्रश्न 7. कौन-सी सुरक्षा कमजोरी RDP को रैनसमवेयर हमलावरों का लक्ष्य बना सकती है?

a) ऑफलाइन बैकअप का उपयोग करना

b) नियमित सॉफ्टवेयर अपडेट करना

c) मजबूत प्रमाणीकरण का उपयोग करना

d) कमजोर पासवर्ड के साथ RDP को इंटरनेट पर खुला रखना

प्रश्न 8. ड्राइव-बाय डाउनलोड क्या है?

a) विश्वसनीय वेबसाइट से फाइल डाउनलोड करना

b) एंटीवायरस सॉफ्टवेयर को मैन्युअल रूप से इंस्टॉल करना

c) उपयोगकर्ता की स्पष्ट जानकारी या सहमति के बिना दुर्भावनापूर्ण सॉफ्टवेयर डाउनलोड होना

d) फाइलों का बैकअप बनाना

प्रश्न 9. किसी संगठन पर रैनसमवेयर का प्रमुख प्रभाव क्या होता है?

a) डेटा अनुपलब्धता और व्यावसायिक कार्यों में बाधा

b) सिस्टम के प्रदर्शन में सुधार

c) स्टोरेज क्षमता में वृद्धि

d) नेटवर्क कनेक्टिविटी में सुधार

प्रश्न 10. वर्ष 2017 में विश्वभर में किस रैनसमवेयर ने बड़े पैमाने पर साइबर हमला किया था?

a) नॉटपेट्या

b) वानाक्राई

c) क्रिप्टोलॉकर

d) लॉकबिट

प्रश्न 11. WannaCry रैनसमवेयर हमले की प्रमुख विशेषता क्या थी?

a) इसने केवल मोबाइल फोन को प्रभावित किया

b) इसने सिस्टम की सुरक्षा में सुधार किया

c) यह कमजोर Windows सिस्टमों में फैल गया

d) इसने केवल सोशल मीडिया खातों को निशाना बनाया

प्रश्न 12. AIDS Trojan को किस नाम से भी जाना जाता है?

a) वानाक्राई

b) क्रिप्टोलॉकर

c) लॉकबिट

d) पीसी साइबॉर्ग

प्रश्न 13. नियमित सुरक्षा पैचिंग का मुख्य उद्देश्य क्या है?

a) ज्ञात सुरक्षा कमजोरियों को ठीक करना

b) फाइल का आकार बढ़ाना

c) एंटीवायरस सॉफ्टवेयर को बंद करना

d) उपयोगकर्ता खातों को हटाना

प्रश्न 14. अनधिकृत पहुंच को रोकने के लिए कौन-सी पासवर्ड आदत अपनानी चाहिए?

a) हर जगह एक ही पासवर्ड का उपयोग करना

b) मजबूत और अलग-अलग पासवर्ड का उपयोग करना

c) सहकर्मियों के साथ पासवर्ड साझा करना

d) सार्वजनिक स्थानों पर पासवर्ड लिखना

प्रश्न 15. संदिग्ध ईमेल अटैचमेंट प्राप्त होने पर उपयोगकर्ता को क्या करना चाहिए?

a) उसे तुरंत खोलना चाहिए

b) उसे सभी को भेजना चाहिए

c) भेजने वाले की पुष्टि करके संदिग्ध ईमेल की रिपोर्ट करनी चाहिए

d) एंटीवायरस बंद कर देना चाहिए

प्रश्न 16. Endpoint Detection and Response (EDR) की मुख्य भूमिका क्या है?

a) इंटरनेट की गति बढ़ाना

b) कार्यालय की उपस्थिति प्रबंधित करना

c) उपयोगकर्ता पासवर्ड बनाना

d) एंडपॉइंट खतरों का पता लगाना, जांच करना और उनका जवाब देना

प्रश्न 17. रैनसमवेयर से बचाव के लिए नेटवर्क सेगमेंटेशन क्यों महत्वपूर्ण है?

a) नेटवर्क के विभिन्न हिस्सों में मैलवेयर के प्रसार को सीमित करने के लिए

b) बैकअप की आवश्यकता समाप्त करने के लिए

c) पासवर्ड की लंबाई बढ़ाने के लिए

d) नेटवर्क सुरक्षा बंद करने के लिए

प्रश्न 18. 3-2-1 बैकअप नियम का उद्देश्य क्या है?

a) तीन उपयोगकर्ता खाते बनाए रखना

b) तीन एंटीवायरस प्रोग्राम इंस्टॉल करना

c) अलग-अलग माध्यमों पर डेटा की कई प्रतियां रखना, जिनमें एक ऑफसाइट कॉपी भी शामिल हो

d) तीन नेटवर्क कनेक्शन बनाना

प्रश्न 19. संगठनों को ऑफलाइन बैकअप क्यों बनाए रखना चाहिए?

a) इंटरनेट की गति बढ़ाने के लिए

b) बैकअप डेटा को रैनसमवेयर एन्क्रिप्शन से सुरक्षित रखने के लिए

c) कर्मचारियों की उपस्थिति कम करने के लिए

d) सिस्टम अपडेट बंद करने के लिए

प्रश्न 20. संगठन-स्तरीय साइबर सुरक्षा जागरूकता प्रशिक्षण क्यों महत्वपूर्ण है?

a) अनावश्यक सॉफ्टवेयर इंस्टॉलेशन बढ़ाने के लिए

b) सुरक्षा उपकरणों की आवश्यकता समाप्त करने के लिए

c) कर्मचारियों को पासवर्ड साझा करने की अनुमति देने के लिए

d) कर्मचारियों को साइबर खतरों की पहचान करने और उन्हें रोकने में सक्षम बनाने के लिए

Module 1

Cyber Crime and Cyber Hygiene

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	7	B	13	A	19	A
2	C	8	B	14	C	20	B
3	B	9	C	15	B		
4	B	10	C	16	B		
5	D	11	B	17	B		
6	C	12	B	18	B		

Module - 2

Social Media Threats & Cyberbullying

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	7	A	13	B	19	B
2	B	8	B	14	B	20	C
3	B	9	B	15	A		
4	C	10	A	16	B		
5	B	11	B	17	A		
6	A	12	B	18	B		

Module - 3

Identity Theft & Personal Data Leaks

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	A	7	A	13	A	19	B
2	A	8	B	14	A	20	A
3	A	9	B	15	A		
4	B	10	A	16	A		
5	A	11	B	17	B		
6	B	12	A	18	B		

Module - 4 Online Financial Frauds & Digital Payments Security

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	7	C	13	C	19	C
2	B	8	A	14	B	20	C
3	C	9	B	15	B		
4	B	10	B	16	C		
5	A	11	A	17	C		
6	D	12	B	18	B		

Module – 5 Women & Child Online Safety

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	6	C	11	A	16	D
2	C	7	A	12	D	17	B
3	A	8	D	13	B	18	C
4	D	9	B	14	C	19	A
5	B	10	C	15	A	20	D

Module – 6 Dark Web, Cyber Terrorism & Illegal Activities

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	6	C	11	A	16	D
2	C	7	A	12	D	17	B
3	A	8	D	13	B	18	C
4	D	9	B	14	C	19	A
5	B	10	C	15	A	20	D

Module -7 Best Practices for Cyber Hygiene

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	7	B	13	A	19	B
2	D	8	C	14	C	20	C
3	C	9	B	15	B		
4	B	10	B	16	C		
5	C	11	C	17	B		
6	B	12	C	18	C		

Module - 8 Awareness Ransomware

ANSWER KEY

Question No.	Answer	Question No.	Answer	Question No.	Answer	Question No.	Answer
1	B	6	B	11	C	16	D
2	D	7	D	12	D	17	A
3	A	8	C	13	A	18	C
4	C	9	A	14	B	19	B
5	A	10	B	15	C	20	D