E-mail: coeoffice@csjmu.ac.in

☎🖷: 0512-2246609
☎🖷: 0512-2246608

छत्रपति शाहू जी महाराज विश्वविद्यालय, कानपुर

CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

राष्ट्रीय मूल्यांकन एवं प्रत्यायन परिषद् द्वारा A++ ग्रेड प्राप्त विश्वविद्यालय
(पूर्ववर्ती कानपुर विश्वविद्यालय, कानपुर)
(Formerly Known as Kanpur University, Kanpur-208024)

संo: सी.एस.जे.एम.वि.वि./सी.ओ.ई./359/2026 दिनांक : 15/04/2026

सेवा में,

प्राचार्य/प्राचार्या,
समस्त सम्बद्ध महाविद्यालय,
छत्रपति शाहू जी महाराज विश्वविद्यालय,
कानपुर।

विषयः **सत्र 2025–26 के बी.ए., बी.एससी., बी.कॉम. एवं बी.एससी. (बायोटेक्नोलॉजी) पाठ्यक्रम के द्वितीय सेमेस्टर में अध्ययनरत समस्त छात्र–छात्राओं हेतु साइबर सुरक्षा (Cyber Security) रोजगारपरक पाठ्यक्रम की परीक्षा के सम्बन्ध में।**

महोदया,

कृपया उपर्युक्त विषयक विश्वविद्यालय के पत्रांक सीoएसoजेoएमoविoविo/एकेडमिक/378/2025 दिनांक 23.12.2025 द्वारा विश्वविद्यालय से सम्बद्ध सभी महाविद्यालयों में सत्र 2025–26 हेतु बी.ए., बी.एससी., बी.कॉम. एवं बी.एससी. (बायोटेक्नोलॉजी) के द्वितीय सेमेस्टर में अध्ययनरत समस्त छात्र–छात्राओं हेतु **साइबर सुरक्षा (Cyber Security)** पाठ्यक्रम में लागिन कराये जाने के निर्देश दिये गये है। उक्त पाठ्यक्रम का पूर्णांक 100 अंकों का होगा, जिसमें 40 अंक आंतरिक मूल्यांकन तथा 60 अंक लिखित परीक्षा के आधार पर दिये जायेगें। इसके साथ विश्वविद्यालय द्वारा 60 अंकों की लिखित परीक्षा वस्तुनिष्ठ प्रकार (Objective Type) से सम्पन्न करायी जायेगी। छात्र/छात्राओं की सुविधा के दृष्टिगत विश्वविद्यालय द्वारा **साइबर सुरक्षा (Cyber Security)** की लिखित परीक्षा से सम्बन्धित **Question Bank** विश्वविद्यालय की वेबसाइट पर उपलब्ध कराया जा रहा है।

अतः आदेशानुसार आपसे अनुरोध है कि उक्त से अपने महाविद्यालय के समस्त सम्बन्धित छात्र/छात्राओं को अवगत कराने का कष्ट करें।

(राकेश कुमार)
परीक्षा नियंत्रक

प्रतिलिपि : निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित :–

1. डीन एकेडमिक्स, सीoएसoजेoएमoविoविo, कानपुर।
2. डीन, छत्रपति शाहू जी महाराज विश्वविद्यालय इनोवेशन फाउंडेशन।
3. निजी सचिव कुलपति, माo कुलपति जी के अवलोकनार्थ।
4. वैयo सहायक, कुलसचिव/वित्त अधिकारी।
5. पीoएमoयूo सेल/प्रभारी, कोडिंग।
6. सम्बन्धित पत्रावली।

15/04/26
(अंजलि मौर्या)
उप कुलसचिव (परीक्षा)

Module 1

Cyber Crime and Cyber Hygiene

1. Digital evidence is admissible in court under:
a) IPC 420
b) Section 70
c) IT Act Section 66C
d) Evidence Act 65B

2. Cyberstalking mostly targets:
a) Banking servers
b) Government databases
c) Individuals for monitoring, harassment, or intimidation
d) ATM machines

3. Which of the following is a major impact of cyber-crime on individuals?
a) Emotional and financial loss
b) Faster browsing speed
c) Higher salary
d) Social media promotions

4. Which cyber-crime involves cloning ATM or credit card information?
a) Cryptojacking
b) Skimming
c) Cyber bullying
d) Doxxing

5. Interpol's "Purple Notice" is issued to:
a) Arrest criminals without warrants
b) Monitor missing children
c) Issue travel restrictions
d) Share information on new cyber-crime techniques

6. Victims in Digital Arrest scams are typically manipulated by:

a) Offering free giveaways
b) Sending entertainment videos
c) Impersonating police/CID and pressuring them to transfer money
d) Sharing online shopping discounts

7. Which emotion is most exploited in phishing attacks?
a) Joy
b) Fear of losing access or money
c) Sleepiness
d) Romance

8. Which section of the IT Act 2000 deals with identity theft?
a) Section 66C
b) Section 66F
c) Section 67
d) Section 70

9. Ransomware is mainly classified under:
a) Cyber terrorism
b) Financial cyber crime
c) Cyberstalking
d) Child exploitation

10. One of the major tools used by scammers in digital arrest fraud is:
a) Online news channels
b) VPN discount coupons
c) Remote desktop apps and video calls pretending to be police
d) Photo editing filters

11. According to FBI IC3 reports, which attack causes the highest financial loss worldwide?
a) Cryptocurrency mining
b) Social media hacks
c) Game account hacking
d) Business Email Compromise (BEC)

12. Why is cross-border cyber-crime hard to investigate?
a) Criminals and victims belong to different legal jurisdictions
b) Police do not use computers
c) All hackers live in the USA

d) India has no cyber law

13. Which of the following best defines cyber-crime?
a) Physical robbery
b) Crime committed using digital systems and networks
c) Renting hardware online
d) Use of mobile phones for gaming

14. Social engineering succeeds primarily because:
a) Human psychology is easier to exploit than technical systems
b) Computers are weak machines
c) Hackers don't like technical attacks
d) Internet speed is very high

15. The main psychological trigger used in Digital Arrest scams is:
a) Humour
b) Motivation
c) Fear and urgency
d) Greed only

16. Which IPC section is frequently used in online harassment and defamation cases?
a) IPC 509 / 499
b) IPC 302
c) IPC 144
d) IPC 118

17. Identity theft occurs when:
a) A person steals hardware from an office
b) A user deletes their own email
c) Hackers attack only government websites
d) Someone steals another's personal information for misuse

18. Which category of cyber-crime causes emotional and psychological harm in personal relationships?
a) Cyberstalking
b) Code injection

c) Packet sniffing
d) SQL injection

19. Which attack category directly demands payment to restore encrypted data?
a) Doxxing
b) Cyber bullying
c) Ransomware
d) Credential stuffing

20. Which is the most effective organization-level defense against social engineering?
a) Removing computers from office
b) Sharing passwords in teams for transparency
c) Allowing USB drives in all systems
d) Security awareness training for employees

Module - 2

Social Media Threats & Cyberbullying

1. What is the main goal 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 sign often indicates online grooming?
A. Asking about hobbies
B. Asking for private photos or secrets
C. Sending memes
D. Talking about school

3. Romance scammers usually build trust by:
A. Showing real ID proof
B. Pretending love and giving emotional attention
C. Meeting immediately in person
D. Sending gifts

4. A scammer may avoid video calls because:
A. Their camera is broken
B. They are shy
C. They are not the person in the photos
D. They prefer texting

5. A common red flag in romance scams is:
A. Proper grammar
B. Asking for urgent money
C. Normal conversation
D. Sharing hobbies

6. Online grooming often begins with:
A. Slow friendship-building
B. Asking for bank passwords
C. Meeting parents
D. Sending official documents

7. Fake giveaway scammers usually ask victims to:
A. Pay a “processing fee”
B. Take free gifts
C. Visit a park
D. Join a study group

8. Crypto scam promotions often promise:
A. Low returns
B. Guaranteed high profits
C. Normal market growth
D. Slow investment

9. Impersonation scams often use:
A. Verified accounts only
B. Slightly changed usernames
C. Government websites
D. School IDs

10. A giveaway is likely fake when the page:
A. Has no verified badge but claims big prizes
B. Shows previous winners
C. Has many real comments
D. Has proper website links

11. Reverse image search helps to:
A. Find phone numbers
B. Check if profile photos are stolen
C. Fix image quality
D. Make new photos

12. Username lookup helps you find:
A. The person’s address
B. Accounts using the same username
C. Mobile recharge offers
D. Offline locations

13. Metadata can reveal:
A. Weather details
B. Hidden information like date/time an image was created
C. Movie files
D. Shopping history

14. A behavioral red flag for a fake profile is:
A. Posting daily life photos
B. Messaging many people the same lines
C. Having old posts
D. Having friends and family tagged

15. Fake accounts usually show:
A. Very few posts and recent creation
B. Long history
C. Real-life network
D. Consistent background

16. First step if your account is hacked:
A. Create a new account
B. Use the platform's "Account Recovery" option
C. Wait 2 days
D. Inform strangers

17. Trusted contacts in account recovery are:
A. Random people online
B. Friends chosen by you to help recover your account
C. Police officers
D. Tech support agents

18. Two-factor authentication (2FA) helps by:
A. Allowing faster logins
B. Adding a second layer of security
C. Saving passwords automatically
D. Hiding your photos

19. Reviewing recent login history helps you:
A. Learn time management
B. Check if someone logged in from unknown devices
C. Increase followers
D. Find new friends

20. If a hacker changed your password, you should:
A. Give up
B. Use "Forgot Password" recovery steps
C. Create a new email
D. Logout from all devices

Module - 3

Identity Theft & Personal Data Leaks

1. Credential stuffing means:
A. Sending emails to friends
B. Using stolen passwords on many websites
C. Changing passwords daily
D. Resetting old accounts

2. This attack happens because people often:
A. Use the same password everywhere
B. Play games
C. Travel a lot
D. Forget usernames

3. A sign of credential stuffing is:
A. Multiple failed login attempts
B. Slow internet
C. Long videos
D. High electricity bill

4. To stay safe, users should:
A. Reuse old passwords
B. Use strong & unique passwords
C. Share passwords with friends
D. Remove 2FA

5. Hackers get leaked passwords from:
A. Movies
B. Data breaches on other websites
C. YouTube
D. Weather apps

6. Call spoofing means:
A. Calling with a funny voice
B. Displaying a fake caller ID
C. Calling without network
D. Calling from a landline

7. Scammers pretend to be:
A. Car drivers
B. Bank or telecom customer care

C. School teachers
D. Game streamers

8. Fake customer care scams usually ask for:
A. TV channel list
B. Your OTP or PIN
C. Food orders
D. Movie tickets

9. A safe practice is:
A. Trusting unknown callers
B. Calling the official customer care number yourself
C. Giving details on random calls
D. Sharing OTP to verify your identity

10. Spoofed calls are dangerous because:
A. They are long calls
B. They look like genuine bank numbers
C. They have jokes
D. They use loud music

11. A data leak happens when:
A. Data is safely backed up
B. User information is exposed without permission
C. Apps update themselves
D. Users change passwords

12. Dominos India leak exposed:
A. Pizza recipes
B. Customer phone numbers & addresses
C. Delivery bikes
D. Store timings

13. BigBasket data leak involved:
A. Rice and vegetables
B. User emails, passwords, phone numbers
C. Grocery cart history only
D. Store rent details

14. Unacademy leak exposed:
A. Teachers' salaries
B. Emails and passwords of users
C. Exam papers
D. Course fees

15. Data leaks affect citizens by:
A. Giving free gift vouchers
B. Making people vulnerable to scams & spam
C. Increasing internet speed
D. Helping in job search

16. Malicious QR codes can:
A. Improve phone speed
B. Steal personal data
C. Clean your phone screen
D. Charge your battery

17. A dangerous QR code often:
A. Opens unknown suspicious links
B. Shows a wallpaper
C. Opens camera
D. Plays music

18. Payment scams using QR codes usually:
A. Add money to your account
B. Take money from your account
C. Give cashback
D. Show your balance

19. To stay safe, users should scan:
A. QR codes from random walls
B. Only QR codes from trusted sources
C. Any QR during emergencies
D. Faded QR codes

20. QR code identity theft can happen when:
A. Scammer replaces original QR with a fake one
B. You scan school ID cards
C. You scan TV screens
D. You scan event banners

Module - 4

Online Financial Frauds & Digital Payments Security

1. Which of the following is a common online financial fraud?

A. Phishing
B. Gardening
C. Online gaming
D. Grocery shopping

2. A fake call pretending to be from a bank asking for OTP is known as:

A. Farming
B. Vishing
C. Surfing
D. DDoS

3. Which detail should you NEVER share with anyone?

A. Name
B. Registered mobile number
C. OTP
D. Email ID

4. Skimming fraud involves:

A. Using mobile banking
B. Cloning card data through devices
C. Requesting bank statements
D. Closing bank accounts

5. Which of the following is a secure digital payment method?

A. Using official banking apps
B. Installing random APK files
C. Entering card details on pop-up ads
D. Using shared accounts

6. What should you check before scanning a QR code for payment?

A. QR design
B. Merchant’s name
C. QR color
D. Phone brightness

7. If someone sends you a payment request on UPI:

A. Accept without thinking
B. Decline and verify the person
C. Enter random PIN
D. Call the number in the request

8. Fake shopping websites mainly aim to:

A. Sell original products
B. Steal money and personal information
C. Improve customer service
D. Provide cashback

9. What is the right action if you detect unauthorized transactions?

A. Do nothing
B. Immediately report to bank
C. Share details with strangers
D. Close your UPI app

10. Which practice improves digital payment security?

A. Storing PIN in notes
B. Using strong passwords
C. Clicking unknown links
D. Posting card photos online

11. A fake banking website has HTTPS enabled. Which method can still help detect it?

A. Check for padlock symbol only
B. Verify the certificate issuer and domain spelling
C. Test loading speed
D. Use public Wi-Fi for testing

12. Why is covering the keypad while entering ATM PIN still important on chip-enabled ATMs?

A. Prevents network hacking
B. Avoids shoulder surfing or hidden camera capture
C. Speeds up transaction
D. Bypasses OTP

13. CERT-IN regularly issues early alerts to which of the following sectors?

A. Insurance only
B. Only mobile companies
C. Government, banks, and corporates
D. Travel and hotel industry

14. What's the core reason UPI frauds happen when users click unknown payment links?

A. Server error
B. App crash
C. Phishing and social engineering
D. Network delay

15. Why is using chip-enabled or contactless cards safer than magnetic stripe cards?

A. They never get blocked
B. They are cheaper
C. Data is encrypted and dynamic
D. No PIN needed

16. Which digital fraud targets emotional urgency like 'limited slots left'?

A. Skimming fraud
B. SIM cloning fraud
C. Job/investment scam
D. ATM spoofing

17. What is the key legal body in India that provides technical help in cyber attacks and phishing?

A. RBI
B. MeitY
C. CERT-IN
D. UIDAI

18. A user received a network signal loss and stopped getting OTPs. What should be her immediate first action?

A. Wait and restart phone
B. Complain to TRAI
C. Contact the mobile provider to verify SIM status
D. Reinstall UPI app

19. Who can complain to the RBI Ombudsman?

A. Only businessmen
B. Anyone having a banking issue
C. Only NRIs
D. Only RBI staff

20. How can you protect your mobile from SIM swapping?

A. Use basic phone
B. Share number online

C. Set SIM lock or telecom PIN
D. Never charge phone

Module – 5: Women & Child Online Safety

Q1. What is a common tactic used in fake matrimony or dating scams?

A) Asking for help with wedding arrangements
B) Gaining trust and then asking for money under emotional pretenses
C) Asking about your hobbies
D) Sending expensive gifts

Q2. How can schools and communities contribute to online safety?

A) By organizing awareness programs and digital literacy training
B) By letting children handle issues alone
C) By banning internet use
D) By blocking all websites

Q3. Which of the following is safe online practice?

A) Clicking unknown links in emails
B) Sharing passwords with friends
C) Posting home address publicly
D) Using strong and unique passwords

Q4. What is the danger of oversharing on social media?

A) It may lead to data misuse, stalking, or financial fraud
B) It helps you gain more followers
C) It makes your posts more popular
D) It improves internet connectivity

Q5. What should you do first if you or someone you know is cyberbullied?

A) Retaliate with mean comments
B) Ignore it completely
C) Delete your account immediately
D) Save evidence and report to a trusted adult or authority

Q6. Which of the following best describes the term 'Digital Landscape'?

A) The overall environment of online platforms, services, and interactions
B) Satellite views of cities
C) The physical layout of computer hardware
D) A software for drawing websites

Q7. Which of the following best explains why online groomers appear kind, caring, and funny at the beginning?

A) To create harmless online friendships
B) To build trust, lower suspicion, and emotionally trap the target
C) To entertain people online
D) To improve their popularity on social media Q8.

Q8. What is phishing?

A) Sending fake messages tricks people into sharing personal information
B) A type of online game
C) A way to fix computer viruses
D) Programming language

Q9. What is an effective strategy to protect your online privacy?

A) Sharing passwords with friends
B) Keeping strong, unique passwords and enabling 2FA
C) Accepting all cookies on websites
D) Using public Wi-Fi for bank transactions

Q10. Which is a sign that a website is secure for transactions?

A) It has colorful ads
B) It opens on full screen
C) It has a lock icon and 'https' in the address bar
D) The URL starts with 'http'

Q11. Which of the following is an example of cyberstalking?

A) Writing online blogs
B) Sending a job offer
C) Repeatedly messaging someone despite them asking to stop
D) Playing games together

Q12. Which of the following can be considered a sign that someone is being cyberbullied?

A) Increased interest in social media
B) Becoming withdrawn or anxious after being online
C) Using new apps
D) Laughing loudly at their phone

Q13. What is the best way to identify fake news online?

A) Verify the source and check multiple reliable sites
B) Forward it quickly
C) Read only the headline
D) Believe what friends share

Q14. How can we respond to negative or harmful content on a community platform?

- Post a sarcastic reply
- Report it and avoid engagement
- Argue aggressively
- Share it widely

Q15. Which of the following is an example of personal information?

A) Type of internet browser
B) Phone number and home address
C) Favorite food
D) Favorite movie

Q16. Why is personal information valuable in the digital world?

A) It can be sold or misused for fraud, identity theft, or scams
B) It helps in watching movies
C) It increases internet speed
D) It gives access to free shopping

Q17. Which of these actions is a safe response to cyberbullying?

A) Create a fake account to fight back
B) Block and report the bully on the platform
C) Keep it a secret
D) Share bullying post with others

Q18. How can users encourage safe sharing within a community?

A) Post private images
B) Share personal stories without consent
C) Ask strangers for details
D) Promote verified information and set good examples

Q19. Why is it important to involve parents, teachers, and guardians in digital safety efforts?

A) They can provide guidance, set boundaries, and monitor harmful behavior
B) They can restrict internet completely
C) They stop all online fun
D) They can create viral videos

Q20. Which emotional hook is commonly used by groomers to build false trust with victims?

A) Giving homework assignments
B) Strict warnings
C) Only you understand me
D) Sharing technical tutorials

Module – 6: Dark Web, Cyber Terrorism & Illegal Activities

Q1. What does 'Digital Underground' refer to?

A) A video game
B) Hidden digital communities and markets beyond the surface web
C) Metro train system
D) Secret tunnels in a city

Q2. Who are often the actors behind cyber terrorism?

A) State-sponsored hackers or extremist groups
B) Shopkeepers
C) College students doing homework
D) Digital artists

Q3. What is the first step in combating dark web threats?

A) Deleting social media
B) Understanding the digital landscape and online behaviors
C) Ignoring cyber incidents
D) Turning off the computer

Q4. Who are typically the 'Residents of the Hidden Alleys'?

A) Only police officers
B) Gardeners
C) Hackers, criminals, whistleblowers, journalists, and curious users
D) School teachers

Q5. Which type of online activity is most vulnerable to cyber threats?

A) Watching cartoons
B) Online banking and digital transactions without security measures
C) Private browsing
D) Using offline calculators

Q6. Which of the following is a common online threat linked to dark web activities?

A) Watching YouTube
B) Online bill payments
C) Phishing scams and identity theft
D) Reading e-books

Q7. Which of the following is a cybercrime often initiated through dark web services?

A) Online banking
B) Social networking
C) Online shopping
D) Phishing kits and hacking tools distribution

Q8. Which critical sectors are often targeted in cyber terrorism?

A) Movie theatres
B) Power grids, airports, banks, and government websites
C) Schools only
D) Cafes

Q9. What type of currency is commonly used for transactions on the Dark Web?

A) Debit card
B) Cryptocurrency (e.g., Bitcoin)
C) Credit card
D) Indian Rupees

Q10. What is meant by the term 'Marketplace of Shadows'?

A) Hidden websites that sell illegal goods and services
B) A legal e-commerce site
C) A place to watch dark movies
D) A video game store

Q11. Which of the following is a common weapon or tool used in cyber terrorism?

A) Firewall
B) YouTube
C) Antivirus
D) Malware or ransomware

Q12. What is the safest way to use social media platforms?

A) Accept all friend requests
B) Keep profiles private and avoid sharing personal details
C) Share everything publicly
D) Post passwords for backup

Q13. What is one major risk of visiting dark web sites?

A) Free gaming
B) Better education
C) Improved Wi-Fi speed
D) Exposure to scams, illegal content, and surveillance

Q14. What is the 'Dark Web'?

A) The part of the internet is not indexed by regular search engines
B) A secret part of space
C) A type of computer virus
D) A website for kids

Q15. Why is cyber terrorism called an 'invisible threat'?
Because attackers operate anonymously and attacks are hard to detect

A) Because attackers operate anonymously and attacks are hard to detect
B) Because it comes from space
C) Because it cannot be photograph
D) Because it affects only phones

Q16. What is cyber terrorism?

A) Online banking
B) Using the internet to watch movies
C) Using digital tools to cause fear, damage, or disrupt national security
D) A video game competition

Q17. What is the most common tool used to access the dark web?

A) TOR (The Onion Router) browser
B) WhatsApp
C) Google Chrome
D) Safari

Q18. Digital extortion on social media usually begins when attackers:

A) Ask for game recommendations
B) Gain access to private photos, chats, or accounts
C) Request to join online study groups
D) Offer emojis and filters for free

Q19. Which of the following is an effective preventive measure against cyber terrorism?

A) Ignoring updates
B) Clicking unknown ads
C) Regularly updating software and practicing digital hygiene
D) Using outdated antivirus

Q20. What type of human-related crimes are often reported on the dark web?

A) Lost-and-found websites
B) Food delivery scams
C) Job interviews
D) Human trafficking, child exploitation, and illegal pornographic content

Module 7 -Cyber Hygiene

1. Which of the following is a basic cyber hygiene practice?

A. Using the same password everywhere
B. Regularly updating software
C. Ignoring system alerts
D. Using public Wi-Fi for banking

2. Why are software updates important?

A. They slow down devices
B. They only change UI
C. They fix security vulnerabilities
D. They delete old data

3. Which of the following is an example of a phishing attack?

A. Unexpected emails asking for login details
B. Downloading updates from official sites
C. Using strong passwords
D. Logging out after use

4. Backing up important data helps to:

A. Prevent power failures
B. Recover data after attacks
C. Avoid internet usage
D. Increase device speed

5. Which of the following habits should be avoided?

A. Regular scanning for viruses
B. Using outdated software
C. Updating passwords
D. Taking backups

6. Firewalls help in:

A. Cooling down computers
B. Stopping unauthorized access
C. Increasing storage
D. Speeding up processors

7. Cyber hygiene means:

A. Cleaning your computer physically
B. Following safe online practices
C. Deleting all files

D. Installing random apps

8. Email attachments should be opened only when:

A. They are from unknown senders
B. You are curious
C. They are expected and from known sources
D. They contain .exe files

9. Which of the following improves device security?

A. Disabling automatic updates
B. Using pirated software
C. Enabling firewall
D. Sharing passwords

10. Good cyber hygiene protects you from:

A. Only physical theft
B. Online threats and cyberattacks
C. Weather changes
D. Hardware manufacturing defects

11. Before clicking a link, you should:

A. Click instantly
B. Check the sender
C. Forward it to friends
D. Ignore warnings

12. Antivirus helps in:

A. Hacking
B. Protecting from malware
C. Playing games
D. Increasing Wi-Fi speed

13.. Which of the following protects online accounts?

A. Using old passwords
B. Sharing passwords
C. Multi-factor authentication (MFA)
D. Using others' devices

14. Public Wi-Fi is:

A. Unsafe for banking
B. Always safe
C. Good for passwords

D. Best for confidential work

15. Which is a sign of malware infection?

A. Fast device
B. Healthy battery
C. New ringtone
D. Unknown apps appearing

16. Which activity is unsafe?

A. Using official apps
B. Downloading from trusted stores
C. Installing apps from unknown sources
D. Enabling screen lock

17. Screens locks such as PIN or pattern help:

A. Slow down phone
B. Protect device access
C. Delete photos
D. Increase RAM

18. Screens locks such as PIN or pattern help:

A. Slow down phone
B. Protect device access
C. Delete photos
D. Increase RAM

19. What should you do if you receive a strange link?

A. Click it
B. Delete or report it
C. Download everything
D. Share it widely

20. A secure website starts with:

A. http://
B. mailto://
C. ftp://
D. https://

Module - 8

Awareness Ransomware

1. Which malware displays unwanted advertisements on a system?
   a) Spyware
   b) Adware
   c) Worm
   d) Rootkit
2. Scareware usually tricks users by:
   a) Showing fake threat warnings
   b) Silently monitoring keystrokes
   c) Stealing credentials
   d) Encrypting all files
3. Spyware mainly aims to:
   a) Destroy hardware
   b) Monitor user activities
   c) Flood the system with pop-ups
   d) Spread through USB drives
4. A Trojan Horse requires the user to:
   a) Open a malicious file
   b) Connect to RDP
   c) Install antivirus
   d) Disable firewall
5. Which malware can self-replicate without human action?
   a) Virus
   b) Worm
   c) Trojan
   d) Spyware
6. Which malware hides deep inside the operating system to avoid detection?
   a) Rootkit
   b) Adware
   c) Scareware
   d) Virus
7. A collection of compromised machines controlled remotely is called a:
   a) Worm network
   b) Botnet
   c) Trojan group
   d) Spy cluster
8. A computer virus can spread only when:
   a) There is user action
   b) The system is encrypted
   c) The firewall is disabled
   d) Data backup is removed
9. Payload download usually happens after:
   a) User restarts laptop
   b) The malicious file executes

c) Antivirus updates
d) System backup finishes

10. Privilege escalation helps attackers to:
    a) Print documents
    b) Gain admin-level control
    c) Disconnect the internet
    d) Improve system performance

11. Which stage of ransomware locks the files?
    a) Infection
    b) Encryption
    c) Payload drop
    d) Reconnaissance

12. Deletion of backups is performed so that:
    a) System becomes faster
    b) Victim cannot restore data easily
    c) Files can be uploaded to cloud
    d) Antivirus becomes inactive

13. RDP compromise generally happens due to:
    a) Strong passwords
    b) Default or weak credentials
    c) Two-factor authentication
    d) Firewall monitoring

14. Which of the following is most commonly used by attackers to deliver initial malware?
    a) Corporate intranet
    b) Malicious email attachment
    c) Google search results
    d) Printer drivers

15. File encryption in ransomware uses:
    a) Random formatting
    b) Cryptographic algorithms
    c) BIOS overwrite
    d) Browser extensions

16. What should be done immediately when ransomware is detected?
    a) Restart the system
    b) Disconnect from the network
    c) Delete all logs
    d) Pay the ransom first

17. Why is system isolation important?
    a) To increase performance
    b) To prevent lateral spread

c) To allow attackers to reconnect
d) To remove old backups

18. Evidence preservation includes:
    a) Wiping hard disk
    b) Capturing logs and memory
    c) Deleting infected folders
    d) Resetting firewall

19. Who must be informed during an incident as per best practice?
    a) Neighbours
    b) Relevant internal teams
    c) Social media followers
    d) Cab drivers

20. Recovery from ransomware should start only after:
    a) Attackers send a friendly message
    b) Infection is fully contained
    c) Antivirus is uninstalled
    d) Users run random scripts

मॉड्यूल – 1

साइबर क्राइम और साइबर हाइजीन

1) **डिजिटल साक्ष्य अदालत में किसके तहत स्वीकार्य है?**
   a) आईपीसी 420
   b) धारा 70
   c) आईटी एक्ट धारा 66C
   d) एविडेंस एक्ट 65B

2) **साइबरस्टॉकिंग मुख्य रूप से किसे निशाना बनाती है?**
   a) बैंकिंग सर्वर
   b) सरकारी डेटाबेस
   c) व्यक्तियों को मॉनिटरिंग, उत्पीड़न या डराने के लिए
   d) एटीएम मशीनें

3) **व्यक्तियों पर साइबर क्राइम का प्रमुख प्रभाव क्या है?**
   a) भावनात्मक और आर्थिक नुकसान
   b) तेज़ ब्राउज़िंग स्पीड
   c) अधिक वेतन
   d) सोशल मीडिया प्रमोशन

4) **कौन-सा साइबर क्राइम एटीएम या क्रेडिट कार्ड जानकारी की क्लोनिंग से जुड़ा है?**
   a) क्रिप्टोजैकिंग
   b) स्किमिंग
   c) साइबर बुलिंग
   d) डॉक्सिंग

5) **इंटरपोल की "पर्पल नोटिस" किसके लिए जारी की जाती है?**
   a) बिना वारंट अपराधियों की गिरफ्तारी के लिए
   b) लापता बच्चों की निगरानी के लिए
   c) यात्रा पाबंदियाँ जारी करने के लिए
   d) नए साइबर क्राइम तरीकों की जानकारी साझा करने के लिए

6) **डिजिटल अरेस्ट स्कैम में पीड़ितों को कैसे फंसाया जाता है?**
   a) मुफ्त गिवअवे देकर
   b) मनोरंजन वीडियो भेजकर
   c) पुलिस/सीआईडी बनकर दबाव डालकर पैसे ट्रांसफर करवाना
   d) ऑनलाइन शॉपिंग डिस्काउंट भेजकर

7) **फ़िशिंग हमलों में सबसे अधिक किस भावना का शोषण किया जाता है?**
   a) खुशी
   b) एक्सेस या पैसे खोने का डर
   c) नींद
   d) रोमांस

8) **आईटी एक्ट 2000 की कौन सी धारा पहचान की चोरी से संबंधित है?**
   a) धारा 66C
   b) धारा 66F
   c) धारा 67
   d) धारा 70

9) **रैनसमवेयर मुख्य रूप से किस श्रेणी में आता है?**
   a) साइबर आतंकवाद
   b) वित्तीय साइबर क्राइम
   c) साइबरस्टॉकिंग
   d) बाल शोषण

10) **डिजिटल अरेस्ट फ्रॉड में स्कैमर आम तौर पर किस उपकरण का उपयोग करते हैं?**

a) ऑनलाइन न्यूज़ चैनल

b) वीपीएन डिस्काउंट कूपन

c) रिमोट डेस्कटॉप ऐप्स और पुलिस बनकर वीडियो कॉल

d) फोटो एडिटिंग फ़िल्टर

11) **FBI IC3 रिपोर्ट के अनुसार, दुनिया में सबसे अधिक वित्तीय नुकसान किस हमले से होता है?**

a) क्रिप्टोकरेंसी माइनिंग

b) सोशल मीडिया हैक

c) गेम अकाउंट हैकिंग

d) बिजनेस ईमेल कॉम्प्रोमाइज (BEC)

12) **सीमा-पार साइबर क्राइम की जांच कठिन क्यों होती है?**

a) अपराधी और पीड़ित अलग-अलग कानूनी क्षेत्रों के होते हैं

b) पुलिस कंप्यूटर का उपयोग नहीं करती

c) सभी हैकर USA में रहते हैं

d) भारत में साइबर कानून नहीं है

13) **निम्न में से साइबर क्राइम की सबसे सही परिभाषा क्या है?**

a) शारीरिक चोरी

b) डिजिटल सिस्टम और नेटवर्क का उपयोग करके किया गया अपराध

c) हार्डवेयर किराए पर देना

d) मोबाइल फोन से गेम खेलना

14) **सोशल इंजीनियरिंग मुख्य रूप से क्यों सफल होती है?**

a) मानव मनोविज्ञान को तकनीकी सिस्टम की तुलना में आसानी से धोखा दिया जा सकता है

b) कंप्यूटर कमजोर मशीनें हैं

c) हैकर्स तकनीकी हमले पसंद नहीं करते

d) इंटरनेट स्पीड बहुत तेज है

15) **डिजिटल अरेस्ट स्कैम में मुख्य मनोवैज्ञानिक ट्रिगर क्या होता है?**

a) हास्य

b) प्रेरणा

c) डर और तात्कालिकता

d) केवल लालच

16) **ऑनलाइन उत्पीड़न और मानहानि मामलों में अक्सर कौन-सी IPC धारा लागू होती है?**

a) IPC 509 / 499

b) IPC 302

c) IPC 144

d) IPC 118

17) **पहचान की चोरी कब होती है?**

a) जब कोई ऑफिस से हार्डवेयर चुरा ले

b) जब उपयोगकर्ता खुद अपना ईमेल डिलीट करे

c) जब हैकर्स केवल सरकारी वेबसाइट पर हमला करें

d) जब किसी की व्यक्तिगत जानकारी चुराकर उसका दुरुपयोग किया जाए

18) **व्यक्तिगत संबंधों में भावनात्मक और मानसिक नुकसान किस साइबर क्राइम से जुड़ा है?**

a) साइबरस्टॉकिंग

b) कोड इंजेक्शन

c) पैकेट स्निफिंग

d) SQL इंजेक्शन

19) **कौन-सा हमला भुगतान की मांग करता है ताकि एन्क्रिप्टेड डेटा वापस मिल सके?**

a) डॉक्सिंग

b) साइबर बुलिंग
c) रैनसमवेयर
d) क्रेडेंशियल स्टफ़िंग

20) **सोशल इंजीनियरिंग से बचने के लिए संगठन-स्तर पर सबसे प्रभावी उपाय क्या है?**
a) ऑफिस से कंप्यूटर हटाना
b) पारदर्शिता के लिए टीम में पासवर्ड साझा करना
c) सभी सिस्टम में USB ड्राइव की अनुमति देना
d) कर्मचारियों के लिए सुरक्षा जागरूकता प्रशिक्षण

मॉड्यूल – 2
सोशल मीडिया खतरे और साइबरबुलिंग

1. **रोमांस स्कैमर का मुख्य उद्देश्य क्या होता है?**
A. दोस्त बनाना
B. पैसे या व्यक्तिगत जानकारी चुराना
C. ऑनलाइन गेम खेलना
D. फिल्मों का प्रचार करना

2. **ऑनलाइन ग्रूमिंग का कौन-सा संकेत आम तौर पर देखा जाता 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 स्कैमर्स भरोसा कैसे बनाते हैं?**
   A. असली आईडी प्रूफ दिखाकर
   B. प्यार का नाटक करके और भावनात्मक ध्यान देकर
   C. तुरंत सामने मिलकर
   D. उपहार भेजकर
4. **स्कैमर वीडियो कॉल से क्यों बच सकता है?**
   A. कैमरा खराब है
   B. वे शर्माते हैं
   C. वे तस्वीरों में दिख रहे व्यक्ति नहीं हैं
   D. उन्हें मैसेज करना पसंद है
5. **रोमांस स्कैम में एक सामान्य रेड फ़्लैग क्या है?**
   A. सही व्याकरण
   B. तुरंत पैसे की मांग करना
   C. सामान्य बातचीत
   D. शौक साझा करना
6. **ऑनलाइन ग्रूमिंग अक्सर कैसे शुरू होती है?**
   A. धीरे-धीरे दोस्ती बनाकर
   B. बैंक पासवर्ड मांगकर
   C. माता-पिता से मिलकर
   D. आधिकारिक दस्तावेज भेजकर
7. **नकली गिवअवे स्कैमर सामान्यतः पीड़ितों से क्या करवाते हैं?**
   A. "प्रोसेसिंग फीस" भरवाना
   B. मुफ्त गिफ्ट लेना
   C. पार्क जाना
   D. स्टडी ग्रुप में शामिल होना

8. **क्रिप्टो स्कैम प्रमोशन्स आम तौर पर क्या दावा करते हैं?**
   A. कम रिटर्न
   B. गारंटीड बहुत अधिक मुनाफा
   C. सामान्य मार्केट ग्रोथ
   D. धीमा निवेश

9. **इम्पर्सोनेशन स्कैम्स में अक्सर क्या उपयोग किया जाता है?**
   A. केवल वेरिफाइड अकाउंट
   B. थोड़े बदले हुए यूज़रनेम
   C. सरकारी वेबसाइट
   D. स्कूल आईडी
10. **गिवअवे नकली होने की संभावना कब होती है?**
    A. पेज पर वेरिफाइड बैज नहीं है लेकिन बड़े इनाम का दावा है
    B. पिछले विजेताओं को दिखाया गया हो
    C. बहुत से असली कमेंट हों
    D. सही वेबसाइट लिंक हों
11. **रिवर्स इमेज सर्च किसमें मदद करता है?**
    A. फोन नंबर ढूँढने में
    B. यह जांचने में कि प्रोफ़ाइल फोटो चोरी तो नहीं है
    C. इमेज की क्वालिटी सुधारने में
    D. नई तस्वीरें बनाने में

12. **यूज़रनेम लुकअप से आप क्या पता कर सकते हैं?**
    A. व्यक्ति का पता
    B. वही यूज़रनेम उपयोग करने वाले अन्य अकाउंट
    C. मोबाइल रिचार्ज ऑफ़र
    D. ऑफलाइन लोकेशन
13. **मेटाडेटा क्या बता सकता है?**
    A. मौसम की जानकारी
    B. तस्वीर कब/किस समय बनाई गई, ऐसी छुपी जानकारी
    C. मूवी फाइल
    D. शॉपिंग हिस्ट्री
14. **नकली प्रोफाइल का व्यवहारिक रेड फ़्लैग कौन सा है?**
    A. रोज़मर्रा की फोटो पोस्ट करना
    B. बहुत से लोगों को एक जैसे मैसेज भेजना
    C. पुराने पोस्ट होना
    D. परिवार/दोस्तों के साथ टैग होना
15. **फेक अकाउंट्स आम तौर पर क्या दिखाते हैं?**
    A. बहुत कम पोस्ट और हाल ही में बनाया हुआ अकाउंट
    B. लंबा इतिहास
    C. वास्तविक जीवन का नेटवर्क
    D. एक जैसा बैकग्राउंड
16. **यदि आपका अकाउंट हैक हो जाए तो पहला कदम क्या होना चाहिए?**
    A. नया अकाउंट बना लें
    B. प्लेटफ़ॉर्म का "अकाउंट रिकवरी" विकल्प उपयोग करें
    C. 2 दिन प्रतीक्षा करें
    D. अजनबियों को जानकारी दें
17. **अकाउंट रिकवरी में ट्रस्टेड कॉन्टैक्ट्स कौन होते हैं?**
    A. ऑनलाइन मिले रैंडम लोग
    B. आपके द्वारा चुने गए दोस्त जो अकाउंट वापस पाने में मदद करते हैं
    C. पुलिस अधिकारी
    D. टेक सपोर्ट एजेंट

18. **टू-फैक्टर ऑथेंटिकेशन (2FA) कैसे मदद करता है?**
    A. लॉगिन तेज बनाकर
    B. सुरक्षा की दूसरी परत जोड़कर
    C. पासवर्ड अपने-आप सेव करके
    D. आपकी फोटो छुपाकर
19. **हाल की लॉगिन हिस्ट्री देखने से क्या फायदा होता है?**
    A. समय प्रबंधन सीखने में
    B. पता चलता है कि किसी ने अनजान डिवाइस से लॉगिन किया या नहीं
    C. फॉलोअर्स बढ़ाने में
    D. नए दोस्त ढूँढने में
20. **यदि हैकर ने आपका पासवर्ड बदल दिया हो तो क्या करना चाहिए?**
    A. हार मान लें
    B. "फ़ॉरगॉट पासवर्ड" रिकवरी स्टेप्स का उपयोग करें
    C. नया ईमेल बनाएँ
    D. सभी डिवाइस से लॉगआउट करें

मॉड्यूल – 3
पहचान की चोरी और व्यक्तिगत डेटा लीक

1. **क्रेडेंशियल स्टफ़िंग का मतलब क्या है?**
   A. दोस्तों को ईमेल भेजना
   B. चोरी किए गए पासवर्ड को कई वेबसाइटों पर आज़माना
   C. रोज पासवर्ड बदलना
   D. पुराने अकाउंट रीसेट करना
2. **यह हमला इसलिए होता है क्योंकि लोग अक्सर:**
   A. हर जगह एक ही पासवर्ड का उपयोग करते हैं
   B. गेम खेलते हैं
   C. बहुत यात्रा करते हैं
   D. यूज़रनेम भूल जाते हैं
3. **क्रेडेंशियल स्टफ़िंग का एक संकेत क्या है?**
   A. कई बार लॉगिन फ़ेल होना
   B. इंटरनेट स्लो होना
   C. लंबे वीडियो
   D. बिजली का ज्यादा बिल
4. **सुरक्षित रहने के लिए उपयोगकर्ताओं को क्या करना चाहिए?**
   A. पुराने पासवर्ड दोबारा उपयोग करना
   B. मजबूत और अलग-अलग पासवर्ड का उपयोग करना
   C. पासवर्ड दोस्तों के साथ साझा करना
   D. 2FA हटाना
5. **हैकर्स पासवर्ड कहाँ से प्राप्त करते हैं?**
   A. फिल्मों से
   B. अन्य वेबसाइटों में डेटा ब्रीच से
   C. यूट्यूब से
   D. वेदर ऐप से
6. **कॉल स्पूफिंग का मतलब क्या है?**
   A. मज़ाकिया आवाज़ में कॉल करना

B. नकली कॉलर आईडी दिखाना

C. बिना नेटवर्क कॉल करना

D. लैंडलाइन से कॉल करना

7. **स्कैमर किसका रूप धारण करते हैं?**

A. कार ड्राइवर

B. बैंक या टेलीकॉम कस्टमर केयर

C. स्कूल शिक्षक

D. गेम स्ट्रीमर

8. **फर्जी कस्टमर केयर स्कैम्स आमतौर पर क्या मांगते हैं?**

A. टीवी चैनल सूची

B. आपका ओटीपी या पिन

C. खाना ऑर्डर

D. मूवी टिकट

9. **सुरक्षित प्रथा क्या है?**

A. अजनबी कॉलर्स पर भरोसा करना

B. खुद आधिकारिक कस्टमर केयर नंबर पर कॉल करना

C. रैंडम कॉल पर विवरण देना

D. अपनी पहचान साबित करने के लिए ओटीपी शेयर करना

10. **स्पूफ़ की गई कॉल खतरनाक क्यों होती हैं?**

A. वे लंबे कॉल होते हैं

B. वे असली बैंक नंबर जैसी दिखती हैं

C. उनमें चुटकुले होते हैं

D. तेज़ म्यूजिक होता है

11. **डेटा लीक कब होता है?**

A. डेटा सुरक्षित रूप से बैकअप होता है

B. जब उपयोगकर्ता की जानकारी बिना अनुमति के उजागर हो जाती है

C. ऐप अपने-आप अपडेट होते हैं

D. यूज़र पासवर्ड बदलते हैं

12. **डोमिनोज़ इंडिया लीक में क्या उजागर हुआ?**

A. पिज्जा रेसिपी

B. ग्राहक के फोन नंबर और पते

C. डिलीवरी बाइक

D. स्टोर टाइमिंग

13. **बिगबास्केट डेटा लीक में क्या शामिल था?**

A. चावल और सब्जियाँ

B. उपयोगकर्ताओं के ईमेल, पासवर्ड, फोन नंबर

C. सिर्फ ग्रोसरी कार्ट हिस्ट्री

D. स्टोर किराया विवरण

14. **अनएकेडमी लीक में क्या उजागर हुआ?**

A. शिक्षकों की सैलरी

B. उपयोगकर्ताओं के ईमेल और पासवर्ड

C. परीक्षा पेपर

D. कोर्स फीस

15. **डेटा लीक नागरिकों को कैसे प्रभावित करता है?**

A. मुफ्त गिफ्ट वाउचर देकर

B. लोगों को स्कैम और स्पैम के प्रति असुरक्षित बनाकर

C. इंटरनेट स्पीड बढ़ाकर

D. नौकरी खोजने में मदद करके

16. **मैलिशियस क्यूआर कोड क्या कर सकते हैं?**
    A. फोन की स्पीड बढ़ाना
    B. व्यक्तिगत जानकारी चुराना
    C. फोन स्क्रीन साफ करना
    D. बैटरी चार्ज करना
17. **खतरनाक क्यूआर कोड अक्सर:**
    A. अज्ञात और संदिग्ध लिंक खोलते हैं
    B. वॉलपेपर दिखाते हैं
    C. कैमरा खोलते हैं
    D. संगीत चलाते हैं
18. **क्यूआर कोड का उपयोग करके पेमेंट स्कैम कैसे होता है?**
    A. आपके अकाउंट में पैसे जोड़ते हैं
    B. आपके अकाउंट से पैसे निकाल लेते हैं
    C. कैशबैक देते हैं
    D. बैलेंस दिखाते हैं
19. **सुरक्षित रहने के लिए उपयोगकर्ताओं को किसे स्कैन करना चाहिए?**
    A. किसी भी दीवार पर लगे क्यूआर कोड
    B. केवल विश्वसनीय स्रोतों से क्यूआर कोड
    C. इमरजेंसी में कोई भी क्यूआर
    D. फीके पड़े क्यूआर
20. **क्यूआर कोड पहचान चोरी कब हो सकती है?**
    A. जब स्कैमर असली क्यूआर कोड की जगह नकली लगा दे
    B. जब आप स्कूल आईडी स्कैन करें
    C. जब आप टीवी स्क्रीन स्कैन करें
    D. जब आप इवेंट बैनर स्कैन करें

मॉड्यूल – 4

ऑनलाइन वित्तीय धोखाधड़ी और डिजिटल भुगतान सुरक्षा – एमसीक्यू

1. **निम्नलिखित में से कौन सा एक आम ऑनलाइन वित्तीय धोखाधड़ी है?**
   A. फ़िशिंग
   B. बागवानी
   C. ऑनलाइन गेमिंग
   D. किराने की खरीदारी
2. **बैंक से होने का नाटक करके ओ.टी.पी. माँगने वाली नकली कॉल को क्या कहा जाता है?**
   A. खेती-बाड़ी
   B. विषिंग
   C. सर्फिंग
   D. डीडीओएस
3. **आपको कौन सा विवरण कभी किसी के साथ साझा नहीं करना चाहिए?**
   A. नाम
   B. पंजीकृत मोबाइल नंबर
   C. ओ.टी.पी.
   D. ईमेल आईडी
4. **स्किमिंग धोखाधड़ी में क्या शामिल है?**
   A. मोबाइल बैंकिंग का उपयोग करना
   B. उपकरणों के माध्यम से डेटा कार्ड की क्लोनिंग करना
   C. बैंक विवरणों का अनुरोध करना
   D. बैंक खाते बंद करना
5. **निम्नलिखित में से कौन सी एक सुरक्षित डिजिटल भुगतान विधि है?**
   A. आधिकारिक बैंक ऐप्स का उपयोग करना
   B. यादृच्छिक APK फाइल इंस्टॉल करना
   C. पॉप-अप विज्ञापनों पर कार्ड विवरण दर्ज करना
   D. साझा खातों का उपयोग करना
6. **भुगतान के लिए क्यूआर कोड स्कैन करने से पहले आपको क्या देखना चाहिए?**
   A. क्यूआर डिज़ाइन
   B. मर्चेंट का नाम
   C. क्यूआर रंग
   D. फोन की चमक
7. **अगर कोई आपको UPI पर पेमेंट रिक्वेस्ट भेजता है:**
   A. सोचे बिना स्वीकार करें
   B. अस्वीकार करें और व्यक्ति को सत्यापित करें
   C. यादृच्छिक पिन दर्ज करें
   D. अनुरोध नंबर पर कॉल करें
8. **नकली खरीदारी वेबसाइटों का मुख्य उद्देश्य क्या है?**
   A. मूल उत्पाद बेचना
   B. पैसे और व्यक्तिगत जानकारी की चोरी
   C. ग्राहक सेवा में सुधार
   D. कैशबैक प्रदान करना

9. **यदि आपको अनधिकृत लेन-देन दिखे तो सही कार्रवाई क्या है?**
   A. कुछ न करें
   B. तुरंत बैंक को रिपोर्ट करें
   C. अजनबियों के साथ विवरण साझा करें
   D. अपना UPI ऐप बंद करें

10. **कौन-सी प्रथा डिजिटल भुगतान सुरक्षा में सुधार करती है?**
   A. नोट में पिन लिखकर रखना
   B. मजबूत पासवर्ड का उपयोग करना
   C. अज्ञात लिंक पर क्लिक करना
   D. कार्ड की तस्वीरें ऑनलाइन पोस्ट करना

11. **यदि नकली बैंकिंग वेबसाइट में HTTPS सक्षम हो, तो उसे कैसे पहचाना जा सकता है?**
   A. केवल पैडलॉक प्रतीक की जांच करें
   B. प्रमाणपत्र जारीकर्ता और डोमेन स्पेलिंग की पुष्टि करें
   C. लोडिंग स्पीड जांचें
   D. टेस्टिंग के लिए सार्वजनिक वाई-फाई उपयोग करें

12. **ATM पिन दर्ज करते समय कीपैड को कवर करना क्यों महत्वपूर्ण है?**
   A. नेटवर्क हैकिंग रोकने के लिए
   B. शोल्डर-सर्फिंग या छुपे कैमरों से बचाव के लिए
   C. तेज़ ट्रांजैक्शन के लिए
   D. OTP बायपास करने के लिए

13. **CERT-IN नियमित रूप से किस क्षेत्र के लिए शुरुआती अलर्ट जारी करता है?**
   A. केवल बीमा
   B. केवल मोबाइल कंपनियाँ
   C. सरकार, बैंक और कॉर्पोरेट्स
   D. यात्रा और होटल उद्योग

14. **UPI धोखाधड़ी का मुख्य कारण क्या है जब उपयोगकर्ता अज्ञात पेमेंट लिंक पर क्लिक करते हैं?**
   A. सर्वर त्रुटि
   B. ऐप क्रैश
   C. फिशिंग और सोशल इंजीनियरिंग
   D. नेटवर्क विलंब

15. **चिप-सक्षम या संपर्क रहित कार्ड, मैग्नेटिक स्ट्रिप कार्ड से अधिक सुरक्षित क्यों हैं?**
   A. ये कभी ब्लॉक नहीं होते
   B. ये सस्ते होते हैं
   C. डेटा एन्क्रिप्टेड और डायनामिक होता है
   D. पिन की ज़रूरत नहीं होती

16. **कौन सी डिजिटल धोखाधड़ी 'सीमित स्लॉट्स बचे हैं' जैसी इमोशनल अर्जेंसी को निशाना बनाती है?**
   A. स्किमिंग धोखाधड़ी
   B. सिम क्लोनिंग धोखाधड़ी
   C. नौकरी/निवेश धोखाधड़ी
   D. ATM स्पूफिंग

17. **भारत में साइबर हमलों और फिशिंग में तकनीकी सहायता देने वाला मुख्य कानूनी निकाय कौन है?**
   A. RBI
   B. MeitY
   C. CERT-IN
   D. UIDAI

18. **एक उपयोगकर्ता को नेटवर्क सिग्नल लॉस मिला और OTP आना बंद हो गया। पहला कदम क्या होना चाहिए?**
   A. प्रतीक्षा करें और फोन रीस्टार्ट करें
   B. TRAI से शिकायत करें

C. मोबाइल प्रदाता से संपर्क कर सिम की स्थिति जांचें

D. UPI ऐप पुनः इंस्टॉल करें

19. **RBI ओम्बड्समैन से शिकायत कौन कर सकता है?**

A. केवल व्यवसायी

B. कोई भी व्यक्ति जिसे बैंकिंग समस्या हो

C. केवल NRI

D. केवल RBI कर्मचारी

20. **आप अपने मोबाइल को सिम स्वैपिंग से कैसे सुरक्षित कर सकते हैं?**

A. बेसिक फोन का उपयोग करें

B. ऑनलाइन नंबर साझा करें

C. सिम लॉक या टेलिकॉम पिन सेट करें

D. कभी भी फोन चार्ज न करें

मॉड्यूल – 5

महिला एवं बाल ऑनलाइन सुरक्षा

1. **नकली मैट्रिमोनी या डेटिंग स्कैम में आम तौर पर कौन-सी रणनीति उपयोग होती है?**

A) शादी की तैयारियों में मदद माँगना

B) भरोसा जीतकर भावनात्मक कारणों से पैसे माँगना

C) आपके शौक पूछना

D) महंगे गिफ्ट भेजना

2. **स्कूल और समुदाय ऑनलाइन सुरक्षा में कैसे योगदान दे सकते हैं?**

A) जागरूकता कार्यक्रम और डिजिटल साक्षरता प्रशिक्षण आयोजित करके

B) बच्चों को अकेले संभालने देना

C) इंटरनेट उपयोग पर प्रतिबंध लगाना

D) सभी वेबसाइट ब्लॉक करना

3. **निम्नलिखित में से कौन-सी सुरक्षित ऑनलाइन प्रैक्टिस है?**

A) ईमेल में अज्ञात लिंक पर क्लिक करना

B) पासवर्ड दोस्तों से साझा करना

C) घर का पता सार्वजनिक रूप से पोस्ट करना

D) मजबूत और अलग-अलग पासवर्ड का उपयोग करना

4. **सोशल मीडिया पर अत्यधिक जानकारी साझा करने का खतरा क्या है?**

A) डेटा का दुरुपयोग, स्टॉकिंग या वित्तीय धोखाधड़ी

B) अधिक फॉलोअर्स मिलना

C) पोस्ट ज्यादा लोकप्रिय होना

D) इंटरनेट कनेक्टिविटी बढ़ना

5. **यदि आप या कोई परिचित साइबर बुलिंग का शिकार हो तो पहला कदम क्या होना चाहिए?**

A) बदले में बुरा कमेंट करना

B) पूरी तरह अनदेखा करना

C) तुरंत अकाउंट डिलीट करना

D) सबूत सुरक्षित कर विश्वसनीय वयस्क या प्राधिकरण को रिपोर्ट करना

6. **'डिजिटल लैंडस्केप' शब्द का सबसे सही वर्णन क्या है?**

A) ऑनलाइन प्लेटफॉर्म, सेवाओं और इंटरैक्शन का संपूर्ण वातावरण

B) शहरों के सैटेलाइट दृश्य

C) कंप्यूटर हार्डवेयर की भौतिक संरचना

D) वेबसाइट बनाने का सॉफ्टवेयर

7. **ऑनलाइन ग्रूमर्स शुरुआत में दयालु, caring और मज़ेदार क्यों दिखते हैं?**

A) निर्दोष ऑनलाइन दोस्ती बनाने के लिए

B) भरोसा बनाने, शक कम करने और भावनात्मक रूप से फँसाने के लिए

C) लोगों का मनोरंजन करने के लिए

D) सोशल मीडिया पर पॉपुलर बनने के लिए

8. **फ़िशिंग क्या है?**

A) नकली संदेश भेजकर लोगों से निजी जानकारी ठगना

B) एक प्रकार का ऑनलाइन गेम

C) कंप्यूटर वायरस ठीक करने का तरीका

D) एक प्रोग्रामिंग भाषा

9. **ऑनलाइन प्राइवेसी सुरक्षित रखने की प्रभावी रणनीति क्या है?**

A) पासवर्ड दोस्तों से साझा करना

B) मजबूत, यूनिक पासवर्ड रखना और 2FA सक्षम करना

C) सभी वेबसाइटों पर कुकीज़ स्वीकार करना

D) बैंक ट्रांजैक्शन के लिए पब्लिक वाई-फाई इस्तेमाल करना

10. **कौन-सा संकेत बताता है कि वेबसाइट ट्रांजैक्शन के लिए सुरक्षित है?**

A) रंगीन विज्ञापन दिखना

B) फुल स्क्रीन में खुलना

C) एड्रेस बार में लॉक आइकॉन और 'https' होना

D) URL का 'http' से शुरू होना

11. **निम्न में से साइबरस्टॉकिंग का उदाहरण कौन-सा है?**

A) ऑनलाइन ब्लॉग लिखना

B) जॉब ऑफर भेजना

C) किसी को बार-बार मैसेज करना जबकि वह रुकने को कहे

D) साथ में गेम खेलना

12. **कौन-सा संकेत बता सकता है कि कोई साइबर बुलिंग का शिकार हो रहा है?**
    A) सोशल मीडिया में बढ़ती रुचि
    B) ऑनलाइन रहने के बाद उदास या चिंतित दिखना
    C) नए ऐप इस्तेमाल करना
    D) फोन देखकर ज़ोर से हँसना
13. **ऑनलाइन फेक न्यूज़ पहचानने का सबसे अच्छा तरीका क्या है?**
    A) स्रोत की जांच करना और विश्वसनीय साइटों से मिलान करना
    B) तुरंत उसे फॉरवर्ड करना
    C) केवल हेडलाइन पढ़ना
    D) दोस्तों द्वारा शेयर की बात मान लेना
14. **समुदाय प्लेटफ़ॉर्म पर नकारात्मक या हानिकारक कंटेंट पर कैसे प्रतिक्रिया देनी चाहिए?**
    A) व्यंग्यात्मक टिप्पणी करना
    B) रिपोर्ट करना और आगे प्रतिक्रिया से बचना
    C) आक्रामक बहस करना
    D) उसे व्यापक रूप से साझा करना
15. **निम्नलिखित में से व्यक्तिगत जानकारी का उदाहरण कौन है?**
    A) इंटरनेट ब्राउज़र का प्रकार
    B) फोन नंबर और घर का पता
    C) पसंदीदा खाना
    D) पसंदीदा मूवी
16. **डिजिटल दुनिया में व्यक्तिगत जानकारी क्यों मूल्यवान है?**
    A) इसे बेचा जा सकता है या ठगी, पहचान चोरी और स्कैम में प्रयोग किया जा सकता है
    B) इससे फिल्में देखी जा सकती हैं
    C) यह इंटरनेट स्पीड बढ़ाती है
    D) इससे फ्री शॉपिंग मिलती है
17. **साइबर बुलिंग के प्रति सुरक्षित प्रतिक्रिया क्या है?**
    A) फेक अकाउंट बनाकर पलटवार करना
    B) बुली को ब्लॉक और रिपोर्ट करना
    C) इसे गुप्त रखना
    D) बुलींग पोस्ट दूसरों से साझा करना
18. **उपयोगकर्ता समुदाय में सुरक्षित शेयरिंग कैसे बढ़ावा दे सकते हैं?**
    A) निजी तस्वीरें पोस्ट करना
    B) बिना अनुमति निजी बातें साझा करना
    C) अजनबियों से विवरण माँगना
    D) सत्यापित जानकारी साझा करना और अच्छा उदाहरण प्रस्तुत करना
19. **डिजिटल सुरक्षा प्रयासों में माता-पिता, शिक्षक और अभिभावकों की भूमिका क्यों महत्वपूर्ण है?**
    A) वे मार्गदर्शन दे सकते हैं, सीमाएँ तय कर सकते हैं और हानिकारक व्यवहार पर नज़र रख सकते हैं
    B) वे इंटरनेट पूरी तरह बंद कर देते हैं
    C) वे सभी ऑनलाइन मज़ा रोकते हैं
    D) वे वायरल वीडियो बना सकते हैं
20. **ग्रूमर्स पीड़ितों के साथ झूठा भरोसा बनाने के लिए कौन-सा भावनात्मक हुक सबसे अधिक उपयोग करते हैं?**
    A) होमवर्क देना
    B) सख्त चेतावनी
    C) "सिर्फ तुम ही मुझे समझते हो"
    D) तकनीकी ट्यूटोरियल साझा करना

मॉड्यूल – 6
डार्क वेब, साइबर आतंकवाद एवं अवैध गतिविधियाँ

1. **'डिजिटल अंडरग्राउंड' किसे कहा जाता है?**
   A) एक वीडियो गेम
   B) सतही वेब से परे छिपे डिजिटल समुदाय और मार्केट
   C) मेट्रो ट्रेन सिस्टम
   D) शहर की गुप्त सुरंगें
2. **साइबर आतंकवाद के पीछे अक्सर कौन होते हैं?**
   A) राज्य-प्रायोजित हैकर्स या उग्रवादी समूह
   B) दुकानदार
   C) होमवर्क करने वाले कॉलेज छात्र
   D) डिजिटल आर्टिस्ट
3. **डार्क वेब खतरों से निपटने का पहला कदम क्या है?**
   A) सोशल मीडिया डिलीट करना
   B) डिजिटल वातावरण और ऑनलाइन व्यवहार को समझना
   C) साइबर घटना को अनदेखा करना
   D) कंप्यूटर बंद कर देना
4. **'हिडन एलीज़ के निवासी' आमतौर पर कौन होते हैं?**
   A) केवल पुलिस अधिकारी
   B) माली
   C) हैकर्स, अपराधी, व्हिसलब्लोअर, पत्रकार और जिज्ञासु उपयोगकर्ता
   D) स्कूल शिक्षक
5. **कौन-सी ऑनलाइन गतिविधि साइबर हमलों के लिए सबसे अधिक संवेदनशील है?**
   A) कार्टून देखना

B) सुरक्षा उपायों के बिना ऑनलाइन बैंकिंग और डिजिटल लेन-देन

C) प्राइवेट ब्राउज़िंग

D) ऑफलाइन कैलकुलेटर उपयोग करना

6. **निम्नलिखित में से कौन डार्क वेब से जुड़ा सामान्य ऑनलाइन खतरा है?**

A) यूट्यूब देखना

B) ऑनलाइन बिल भुगतान

C) फ़िशिंग स्कैम और पहचान की चोरी

D) ई-बुक पढ़ना

7. **कौन-सा साइबर अपराध अक्सर डार्क वेब सेवाओं के माध्यम से शुरू होता है?**

A) ऑनलाइन बैंकिंग

B) सोशल नेटवर्किंग

C) ऑनलाइन शॉपिंग

D) फ़िशिंग किट और हैकिंग टूल्स का वितरण

8. **साइबर आतंकवाद में किन क्षेत्रों को अधिक निशाना बनाया जाता है?**

A) मूवी थिएटर

B) पावर ग्रिड, एयरपोर्ट, बैंक और सरकारी वेबसाइटें

C) केवल स्कूल

D) कैफ़े

9. **डार्क वेब पर लेन-देन में आम तौर पर कौन-सी मुद्रा उपयोग होती है?**

A) डेबिट कार्ड

B) क्रिप्टोकरेंसी (जैसे बिटकॉइन)

C) क्रेडिट कार्ड

D) भारतीय रुपये

10. **'मार्केटप्लेस ऑफ शैडोज़' का क्या अर्थ है?**

A) अवैध सामान और सेवाएँ बेचने वाली छिपी वेबसाइटें

B) एक वैध ई-कॉमर्स साइट

C) डार्क मूवी देखने का स्थान

D) वीडियो गेम की दुकान

11. **साइबर आतंकवाद में आम तौर पर कौन-सा हथियार/उपकरण उपयोग होता है?**

A) फ़ायरवॉल

B) यूट्यूब

C) एंटीवायरस

D) मैलवेयर या रैनसमवेयर

12. **सोशल मीडिया प्लेटफ़ॉर्म का सुरक्षित उपयोग कैसे किया जा सकता है?**

A) सभी फ्रेंड रिक्वेस्ट स्वीकार करके

B) प्रोफ़ाइल प्राइवेट रखकर और व्यक्तिगत जानकारी साझा न करके

C) सब कुछ सार्वजनिक पोस्ट करके

D) पासवर्ड बैकअप के लिए पोस्ट करके

13. **डार्क वेब साइटों पर जाने का एक बड़ा जोखिम क्या है?**

A) मुफ्त गेमिंग

B) बेहतर शिक्षा

C) तेज़ वाई-फाई

D) स्कैम, अवैध सामग्री और निगरानी का सामना करना

14. **'डार्क वेब' क्या है?**

A) इंटरनेट का वह हिस्सा जो सामान्य सर्च इंजन से इंडेक्स नहीं होता

B) अंतरिक्ष का एक रहस्यमय भाग

C) कंप्यूटर वायरस

D) बच्चों की वेबसाइट

15. **साइबर आतंकवाद को 'अदृश्य खतरा' क्यों कहा जाता है?**

A) क्योंकि हमलावर गुमनाम रहते हैं और हमलों का पता लगाना कठिन होता है

B) क्योंकि यह अंतरिक्ष से आता है

C) क्योंकि इसकी तस्वीर नहीं ली जा सकती

D) क्योंकि यह केवल फोन को प्रभावित करता है

16. **साइबर आतंकवाद क्या है?**

A) ऑनलाइन बैंकिंग

B) इंटरनेट पर फिल्में देखना

C) डिजिटल माध्यमों का उपयोग कर भय, नुकसान या राष्ट्रीय सुरक्षा में व्यवधान पैदा करना

D) वीडियो गेम प्रतियोगिता

17. **डार्क वेब तक पहुँचने के लिए सबसे अधिक उपयोग किया जाने वाला टूल क्या है?**

A) TOR (The Onion Router) ब्राउज़र

B) व्हाट्सऐप

C) गूगल क्रोम

D) सफारी

18. **सोशल मीडिया पर डिजिटल एक्सटॉर्शन आमतौर पर कब शुरू होता है?**

A) जब कोई गेम की सलाह माँगे

B) जब हमलावर निजी फोटो, चैट या अकाउंट तक पहुँच हासिल कर लें

C) जब कोई स्टडी ग्रुप में शामिल होने को कहे

D) जब कोई मुफ्त इमोजी और फ़िल्टर दे

19. **साइबर आतंकवाद से बचाव का प्रभावी उपाय क्या है?**

A) अपडेट्स को अनदेखा करना

B) अज्ञात विज्ञापनों पर क्लिक करना

C) सॉफ़्टवेयर अपडेट रखना और डिजिटल हाइजीन अपनाना

D) पुराने एंटीवायरस का उपयोग करना

20. **डार्क वेब पर कौन-से मानव-संबंधित अपराध अक्सर देखे जाते हैं?**

A) खोया-पाया वेबसाइटें

B) फ़ूड डिलीवरी स्कैम

C) जॉब इंटरव्यू

D) मानव तस्करी, बाल शोषण और अवैध पोर्नोग्राफ़िक सामग्री

मॉड्यूल – 7
साइबर हाइजीन

1. **निम्नलिखित में से कौन-सी साइबर हाइजीन की बुनियादी प्रैक्टिस है?**
   A. हर जगह एक ही पासवर्ड उपयोग करना
   B. नियमित रूप से सॉफ़्टवेयर अपडेट करना
   C. सिस्टम अलर्ट को अनदेखा करना
   D. बैंकिंग के लिए पब्लिक वाई-फाई का उपयोग करना
2. **सॉफ़्टवेयर अपडेट क्यों महत्वपूर्ण हैं?**
   A. यह डिवाइस को धीमा कर देते हैं
   B. ये केवल UI बदलते हैं
   C. ये सुरक्षा कमजोरियों को ठीक करते हैं
   D. ये पुराना डेटा डिलीट करते हैं
3. **फ़िशिंग हमले का उदाहरण कौन-सा है?**
   A. अप्रत्याशित ईमेल जो लॉगिन विवरण मांगते हैं
   B. आधिकारिक साइटों से अपडेट डाउनलोड करना
   C. मजबूत पासवर्ड उपयोग करना
   D. उपयोग के बाद लॉगआउट करना
4. **महत्वपूर्ण डेटा का बैकअप लेने से क्या फायदा होता है?**
   A. बिजली कटौती रोकने में
   B. हमलों के बाद डेटा वापस पाने में
   C. इंटरनेट उपयोग से बचने में
   D. डिवाइस स्पीड बढ़ाने में
5. **निम्न में से किस आदत से बचना चाहिए?**
   A. नियमित वायरस स्कैन
   B. पुराना सॉफ़्टवेयर उपयोग करना
   C. पासवर्ड अपडेट करना
   D. बैकअप लेना
6. **फ़ायरवॉल किसमें मदद करता है?**
   A. कंप्यूटर ठंडा रखने में
   B. अनधिकृत एक्सेस रोकने में
   C. स्टोरेज बढ़ाने में
   D. प्रोसेसर तेज़ करने में
7. **साइबर हाइजीन का अर्थ क्या है?**
   A. कंप्यूटर को शारीरिक रूप से साफ करना
   B. सुरक्षित ऑनलाइन आदतों का पालन करना
   C. सभी फाइलें डिलीट कर देना
   D. रैंडम ऐप्स इंस्टॉल करना
8. **ईमेल अटैचमेंट कब खोलना चाहिए?**
   A. जब वे अजनबियों से आए हों

B. जब आपको जिज्ञासा हो

C. जब वे अपेक्षित हों और विश्वसनीय स्रोत से आए हों

D. जब वे .exe फाइलें हों

9. **कौन-सा विकल्प डिवाइस सुरक्षा में सुधार करता है?**

A. ऑटो-अपडेट बंद करना

B. पायरेटेड सॉफ़्टवेयर उपयोग करना

C. फ़ायरवॉल सक्षम करना

D. पासवर्ड साझा करना

10. **अच्छी साइबर हाइजीन आपको किससे बचाती है?**

A. केवल भौतिक चोरी

B. ऑनलाइन खतरे और साइबर हमले

C. मौसम परिवर्तन

D. हार्डवेयर खराबी

11. **किसी लिंक पर क्लिक करने से पहले क्या करना चाहिए?**

A. तुरंत क्लिक करना

B. भेजने वाले की जांच करना

C. दोस्तों को फॉरवर्ड करना

D. चेतावनी अनदेखी करना

12. **एंटीवायरस किसमें मदद करता है?**

A. हैकिंग

B. मैलवेयर से सुरक्षा

C. गेम खेलने में

D. वाई-फाई स्पीड बढ़ाने में

13. **ऑनलाइन अकाउंट की सुरक्षा कौन-सा विकल्प करता है?**

A. पुराने पासवर्ड उपयोग करना

B. पासवर्ड साझा करना

C. मल्टी-फैक्टर ऑथेंटिकेशन (MFA)

D. दूसरों के डिवाइस उपयोग करना

14. **पब्लिक वाई-फाई कैसा होता है?**

A. बैंकिंग के लिए असुरक्षित

B. हमेशा सुरक्षित

C. पासवर्ड के लिए अच्छा

D. गोपनीय काम के लिए सर्वोत्तम

15. **मैलवेयर संक्रमण का कौन-सा संकेत है?**

A. तेज़ डिवाइस

B. बैटरी अच्छी चलना

C. नई रिंगटोन

D. अज्ञात ऐप्स दिखाई देना

16. **कौन-सी गतिविधि असुरक्षित है?**

A. आधिकारिक ऐप्स का उपयोग

B. विश्वसनीय स्टोर से डाउनलोड

C. अनजान स्रोतों से ऐप इंस्टॉल करना

D. स्क्रीन लॉक सक्षम करना

17. **स्क्रीन लॉक जैसे PIN या पैटर्न किसमें मदद करते हैं?**

A. फोन धीमा करना

B. डिवाइस एक्सेस की सुरक्षा करना

C. फोटो डिलीट करना

D. RAM बढ़ाना

18. **स्क्रीन लॉक जैसे PIN या पैटर्न किसमें मदद करते हैं?**

A. फोन धीमा करना

B. डिवाइस एक्सेस की सुरक्षा करना

C. फोटो डिलीट करना

D. RAM बढ़ाना

19. **यदि आपको कोई संदिग्ध लिंक मिले तो क्या करें?**

A. उसे क्लिक करें

B. डिलीट या रिपोर्ट करें

C. सबकुछ डाउनलोड करें

D. इसे व्यापक रूप से शेयर करें

20. **सुरक्षित वेबसाइट किस प्रकार शुरू होती है?**

A. http://

B. mailto://

C. ftp://

D. https://

मॉड्यूल – 8

रैनसमवेयर जागरूकता – एमसीक्यू

1. **कौन-सा मैलवेयर सिस्टम पर अनचाहे विज्ञापन दिखाता है?**

a) स्पायवेयर

b) एडवेयर

c) वर्म

d) रूटकिट

2. **स्केयरवेयर आमतौर पर उपयोगकर्ताओं को कैसे धोखा देता है?**
   a) नकली खतरे की चेतावनियाँ दिखाकर
   b) चुपचाप कीस्ट्रोक मॉनिटर करके
   c) क्रेडेंशियल चोरी करके
   d) सभी फाइल एन्क्रिप्ट करके
3. **स्पायवेयर का मुख्य उद्देश्य क्या है?**
   a) हार्डवेयर नष्ट करना
   b) उपयोगकर्ता की गतिविधियों की निगरानी करना
   c) पॉप-अप से सिस्टम भर देना
   d) यूएसबी ड्राइव से फैलना
4. **ट्रोजन हॉर्स के फैलने के लिए उपयोगकर्ता को क्या करना पड़ता है?**
   a) एक दुर्भावनापूर्ण फाइल खोलना
   b) RDP से कनेक्ट करना
   c) एंटीवायरस इंस्टॉल करना
   d) फ़ायरवॉल डिसेबल करना
5. **कौन-सा मैलवेयर बिना मानव क्रिया के स्वयं-प्रतिलिपि बना सकता है?**
   a) वायरस
   b) वर्म
   c) ट्रोजन
   d) स्पायवेयर
6. **कौन-सा मैलवेयर ऑपरेटिंग सिस्टम में गहराई में छिपकर डिटेक्शन से बचता है?**
   a) रूटकिट
   b) एडवेयर
   c) स्केयरवेयर
   d) वायरस
7. **संक्रमित और दूर से नियंत्रित मशीनों का समूह क्या कहलाता है?**
   a) वर्म नेटवर्क
   b) बॉटनेट
   c) ट्रोजन ग्रुप
   d) स्पाय क्लस्टर
8. **कंप्यूटर वायरस कब फैलता है?**
   a) जब उपयोगकर्ता कोई क्रिया करता है
   b) जब सिस्टम एन्क्रिप्टेड हो
   c) जब फ़ायरवॉल डिसेबल हो
   d) जब डेटा बैकअप हटाया जाए
9. **पेलोड डाउनलोड कब होता है?**
   a) जब उपयोगकर्ता लैपटॉप रिस्टार्ट करता है
   b) जब दुर्भावनापूर्ण फाइल रन होती है
   c) एंटीवायरस अपडेट के दौरान
   d) बैकअप पूरा होने के बाद
10. **प्रिविलेज एस्केलेशन हमलावरों को क्या करने में मदद करता है?**
    a) डॉक्युमेंट प्रिंट करना
    b) एडमिन-लेवल नियंत्रण प्राप्त करना
    c) इंटरनेट डिसकनेक्ट करना
    d) सिस्टम प्रदर्शन बेहतर करना
11. **रैनसमवेयर के किस चरण में फाइलें लॉक होती हैं?**
    a) संक्रमण (Infection)
    b) एन्क्रिप्शन

c) पेलोड ड्रॉप

d) रिकॉनिसेंस

12. **बैकअप को डिलीट क्यों किया जाता है?**

a) सिस्टम तेज़ बनाने के लिए

b) ताकि पीड़ित आसानी से डेटा रिकवर न कर सके

c) फाइल क्लाउड पर अपलोड करने के लिए

d) एंटीवायरस निष्क्रिय करने के लिए

13. **RDP समझौता (compromise) आमतौर पर किस कारण होता है?**

a) मजबूत पासवर्ड

b) डिफॉल्ट या कमजोर क्रेडेंशियल

c) टू-फैक्टर ऑथेंटिकेशन

d) फ़ायरवॉल मॉनिटरिंग

14. **हमलावर प्रारंभिक मैलवेयर डिलीवर करने के लिए सबसे अधिक किसका उपयोग करते हैं?**

a) कॉर्पोरेट इंट्रानेट

b) दुर्भावनापूर्ण ईमेल अटैचमेंट

c) गूगल सर्च रिजल्ट

d) प्रिंटर ड्राइवर

15. **रैनसमवेयर में फाइल एन्क्रिप्शन किससे होता है?**

a) रैंडम फॉर्मेटिंग

b) क्रिप्टोग्राफिक एल्गोरिदम

c) BIOS ओवरराइट

d) ब्राउज़र एक्सटेंशन

16. **रैनसमवेयर का पता चलते ही सबसे पहले क्या करना चाहिए?**

a) सिस्टम रिस्टार्ट करना

b) नेटवर्क से डिसकनेक्ट करना

c) सभी लॉग डिलीट करना

d) पहले फिरौती का भुगतान करना

17. **सिस्टम आइसोलेशन क्यों महत्वपूर्ण है?**

a) प्रदर्शन बढ़ाने के लिए

b) संक्रमण को फैलने से रोकने के लिए

c) हमलावर को पुनः कनेक्ट करने देने के लिए

d) पुराने बैकअप हटाने के लिए

18. **साक्ष्य संरक्षण (evidence preservation) में क्या शामिल है?**

a) हार्ड डिस्क पोंछना

b) लॉग और मेमोरी कैप्चर करना

c) संक्रमित फ़ोल्डर डिलीट करना

d) फ़ायरवॉल रीसेट करना

19. **सर्वोत्तम प्रथाओं के अनुसार घटना के दौरान किसे सूचित किया जाना चाहिए?**

a) पड़ोसियों को

b) संबंधित आंतरिक टीमों को

c) सोशल मीडिया फॉलोअर्स को

d) कैब ड्राइवर को

20. **रैनसमवेयर रिकवरी कब शुरू करनी चाहिए?**

a) जब हमलावर दोस्ताना संदेश भेजें

b) जब संक्रमण पूरी तरह नियंत्रित हो जाए

c) जब एंटीवायरस अनइंस्टॉल किया जाए

d) जब उपयोगकर्ता रैंडम स्क्रिप्ट चलाएँ

ANSWERS

Module 1

Cyber Crime and Cyber Hygiene

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

Module - 2

Social Media Threats & Cyberbullying

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	B
3	B	9	B	15	A		
4	C	10	A	16	B		
5	B	11	B	17	B		
6	A	12	B	18	B		

Module - 3

Identity Theft & Personal

Data Leaks

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

Module - 4

Online Financial Frauds & Digital Payments Security

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

Module – 5

Women & Child Online Safety

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

Module – 6

Dark Web, Cyber Terrorism & Illegal Activities

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

Module -7

Cyber Hygiene

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

Module - 8

Awareness Ransomware

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