Unit 4

Cyber Security Initiatives in India

---

1. Which agency is the nodal authority for cyber security in India?
a) IB
b) CBI
c) CERT-In
d) NITI Aayog
Answer: c) CERT-In

---

2. What does CERT-In stand for?
a) Central Emergency Response Team – India
b) Cyber Emergency Rescue Team – India
c) Computer Emergency Response Team – India
d) Cybercrime Emergency Rapid Team – India
Answer: c) Computer Emergency Response Team – India

---

3. Which Indian law governs cyber crimes and electronic commerce?
a) Cyber Law Act 2005
b) Information Technology Act, 2000
c) E-Commerce Act 1999
d) Digital India Act 2022
Answer: b) Information Technology Act, 2000

---

4. Which of the following is a flagship programme to promote digital infrastructure and services in India?
a) Start-up India
b) Digital India
c) Skill India
d) Make in India
Answer: b) Digital India

---

5. The National Cyber Security Policy was launched in:
a) 2000

b) 2005
c) 2013
d) 2020
Answer: c) 2013

---

6. The purpose of the National Cyber Security Policy, 2013 is to:
a) Ban social media
b) Promote antivirus products
c) Protect public and private IT infrastructure
d) Increase bandwidth
Answer: c) Protect public and private IT infrastructure

---

7. Which Indian ministry handles cyber laws and cyber security policies?
a) Ministry of Defence
b) Ministry of External Affairs
c) Ministry of Electronics and Information Technology (MeitY)
d) Ministry of Home Affairs
Answer: c) Ministry of Electronics and Information Technology (MeitY)

---

8. Which of the following is a cyber security awareness initiative by the Indian government?
a) CyberYatra
b) CyberSafe India
c) I4C
d) Cyber Swachhta Kendra
Answer: d) Cyber Swachhta Kendra

---

9. What is the function of Cyber Swachhta Kendra?
a) Promote yoga online
b) Block all internet traffic
c) Provide tools to clean malware-infected systems
d) Issue driving licenses
Answer: c) Provide tools to clean malware-infected systems

---

10. What is "I4C" in the context of Indian Cyber Security?
a) Indian Centre for Cyber Crimes Control

b) Indian Cyber Crime Coordination Centre
c) International Cyber Crime Council
d) Indian Committee for Cyber Safety
Answer: b) Indian Cyber Crime Coordination Centre

---

11. National Critical Information Infrastructure Protection Centre (NCIIPC) protects:
a) Wi-Fi networks
b) Social media apps
c) Strategic and critical sectors
d) Gaming data
Answer: c) Strategic and critical sectors

---

12. The "Cyber Surakshit Bharat" initiative is aimed at:
a) Giving digital loans
b) Promoting digital games
c) Training government officials in cyber security
d) Selling antivirus
Answer: c) Training government officials in cyber security

---

13. Which of the following apps is launched by the Indian government for cyber crime reporting?
a) CrimeWatch
b) CyberSafe
c) DigiCop
d) Cyber Crime Reporting Portal
Answer: d) Cyber Crime Reporting Portal

---

14. Which Indian organisation works on national-level cyber exercises and incident response?
a) ISRO
b) DRDO
c) CERT-In
d) UIDAI
Answer: c) CERT-In

---

15. What is the full form of NCIIPC?
a) National Cyber Info and Investigation Protection Cell
b) National Critical Information Infrastructure Protection Centre
c) National Cyber Institute for Internet Protection Cell
d) National Cyber Infrastructure and Protection Commission
Answer: b) National Critical Information Infrastructure Protection Centre

---

16. The Information Technology Act, 2000 was amended in:
a) 2002
b) 2005
c) 2008
d) 2011
Answer: c) 2008

---

17. Under IT Act 2000, who is the adjudicating officer for cyber offences?
a) District Magistrate
b) Chief Justice
c) Controller of Certifying Authorities
d) Designated IT Secretary
Answer: d) Designated IT Secretary

---

18. "National Cyber Coordination Centre (NCCC)" was set up for:
a) Social media tracking
b) Tracking viruses only
c) Threat intelligence and coordination
d) Selling cyber insurance
Answer: c) Threat intelligence and coordination

---

19. Who launched Cyber Surakshit Bharat initiative?
a) Ministry of Education
b) MeitY + NeGD
c) RBI
d) CBI
Answer: b) MeitY + NeGD

---

20. The Digital India Programme was launched in:
a) 2005
b) 2010
c) 2012
d) 2015
Answer: d) 2015

Cyber Security Incident Handling – MCQs

---

1. What is a security incident?
a) Scheduled system update
b) Any event that threatens data integrity, confidentiality, or availability
c) Installing antivirus
d) Changing user password
Answer: b) Any event that threatens data integrity, confidentiality, or availability

---

2. Which of the following is the first step in incident handling?
a) Eradication
b) Containment
c) Preparation
d) Recovery
Answer: c) Preparation

---

3. What is the main goal of incident handling?
a) Improve RAM performance
b) Build new software
c) Detect, respond, and recover from security incidents
d) Format hard drives
Answer: c) Detect, respond, and recover from security incidents

---

4. What comes after detection in the incident response process?
a) Eradication
b) Recovery
c) Containment
d) Preparation
Answer: c) Containment

---

5. The phase where normal operations are restored is:
a) Containment
b) Recovery
c) Eradication
d) Documentation
Answer: b) Recovery

---

6. Which team handles cyber security incidents in large organizations?
a) IT department
b) Cyber Crime Police
c) CSIRT (Computer Security Incident Response Team)
d) HR department
Answer: c) CSIRT (Computer Security Incident Response Team)

---

7. What is containment in incident response?
a) Deleting files
b) Isolating affected systems to prevent damage
c) Backing up data
d) Changing system design
Answer: b) Isolating affected systems to prevent damage

---

8. What is the last phase of the incident response process?
a) Recovery
b) Preparation
c) Lessons Learned
d) Scanning
Answer: c) Lessons Learned

---

9. Incident documentation is important for:
a) Marketing
b) Avoiding detection
c) Legal and learning purposes
d) Adding new users
Answer: c) Legal and learning purposes

---

10. What does 'eradication' mean in incident response?
a) Removing the threat or malware from the system
b) Updating user profile
c) Blocking all websites
d) Deleting antivirus
Answer: a) Removing the threat or malware from the system

Cyber Security Assurance

11. What is cyber security assurance?
a) Speed testing tool
b) Providing guarantees about system security
c) Social media login system
d) Antivirus scanning
Answer: b) Providing guarantees about system security

---

12. Which of the following is NOT part of cyber assurance?
a) Risk assessment
b) Policy enforcement
c) Random software coding
d) Compliance verification
Answer: c) Random software coding

---

13. Which standard is commonly used for information security assurance?
a) ISO 9001
b) ISO 27001
c) ISO 14001
d) ISO 5001
Answer: b) ISO 27001

---

14. Which of the following helps in providing cyber assurance?
a) Penetration Testing
b) Ignoring threats
c) Removing passwords
d) Gaming apps
Answer: a) Penetration Testing

---

15. Assurance ensures:
a) There will never be a cyber attack
b) That risks are understood and controls are in place
c) That systems run faster
d) That systems are always online
Answer: b) That risks are understood and controls are in place

---

16. A security audit is part of:
a) Encryption
b) Cyber assurance process
c) Password guessing
d) Software installation
Answer: b) Cyber assurance process

---

17. Assurance is necessary in systems that handle:
a) Only entertainment data
b) Confidential, financial, or government information
c) Wallpapers
d) Online advertisements
Answer: b) Confidential, financial, or government information

---

18. Which of the following increases trust in a system's security?
a) Assurance documentation
b) Pirated software
c) Social media integration
d) Internet download speed
Answer: a) Assurance documentation

---

19. Cyber assurance activities are mainly:
a) Legal actions
b) Preventive and proactive
c) Reactive only
d) Physical security
Answer: b) Preventive and proactive

---

20. What is the goal of cyber assurance testing?
a) Increase RAM
b) Make apps look better
c) Validate that security controls are effective
d) Disable updates
Answer: c) Validate that security controls are effective

---

21. What does compliance mean in cyber assurance?
a) Ignoring threats
b) Meeting security rules, standards, and regulations
c) Writing logs
d) Banning emails
Answer: b) Meeting security rules, standards, and regulations

---

22. Which organization in India promotes assurance in digital services?
a) TRAI
b) UIDAI
c) STQC (Standardisation Testing and Quality Certification)
d) NSDL
Answer: c) STQC (Standardisation Testing and Quality Certification)

---

23. Which cyber assurance process includes risk identification and mitigation?
a) Gaming module
b) Risk management
c) Software licensing
d) Video conferencing
Answer: b) Risk management

---

24. A well-assured system is:
a) Fast but unprotected
b) Reliable and secure
c) Without encryption
d) Without firewalls
Answer: b) Reliable and secure

---

25. A major benefit of cyber assurance is:
a) Better graphics
b) Greater user trust and system resilience
c) Low bandwidth
d) Ad-free websites
Answer: b) Greater user trust and system resilience

Information Technology (IT) Act, 2000

---

1. The Information Technology Act was enacted in India in the year:
a) 1999
b) 2000
c) 2002
d) 2005
Answer: b) 2000

---

2. The IT Act 2000 mainly deals with:
a) Banking laws
b) Property rights
c) Legal recognition of electronic transactions and cybercrime penalties
d) Labour law
Answer: c) Legal recognition of electronic transactions and cybercrime penalties

---

3. The IT Act came into force on:
a) January 1, 2000
b) October 17, 2000
c) August 15, 2000
d) December 31, 2000
Answer: b) October 17, 2000

---

4. The IT Act was amended in the year:
a) 2005
b) 2008
c) 2010
d) 2013
Answer: b) 2008

---

5. Which section of the IT Act deals with hacking and data theft?
a) Section 43
b) Section 66
c) Section 72
d) Section 4
Answer: b) Section 66

---

6. Section 43 of the IT Act provides penalties for:
a) Publishing obscene material
b) Unauthorized access and damage to computer systems
c) Phishing
d) Cyber terrorism
Answer: b) Unauthorized access and damage to computer systems

---

7. Which section of the IT Act deals with cyber terrorism?
a) Section 65
b) Section 67
c) Section 66F
d) Section 72
Answer: c) Section 66F

---

8. Section 67 of the IT Act deals with:
a) Online banking fraud
b) Publishing or transmitting obscene content in electronic form
c) Cyber bullying
d) Data theft
Answer: b) Publishing or transmitting obscene content in electronic form

---

9. Who is the adjudicating officer under the IT Act?
a) District Magistrate
b) Police Commissioner
c) Appointed IT Secretary (not below the rank of Director)
d) Cyber Cafe Owner
Answer: c) Appointed IT Secretary (not below the rank of Director)

---

10. The IT Act legally recognizes:
a) Print documents only
b) Voice messages only
c) Electronic records and digital signatures
d) SMS only
Answer: c) Electronic records and digital signatures

---

11. The IT Act applies to:
a) India only
b) Outside India only
c) India and abroad if the crime involves a computer in India
d) UN Members only
Answer: c) India and abroad if the crime involves a computer in India

---

12. Under which section is identity theft and cheating by personation using computer resource covered?
a) Section 66C and 66D
b) Section 43A
c) Section 70
d) Section 69
Answer: a) Section 66C and 66D

---

13. Which authority issues digital certificates in India?
a) UIDAI
b) SEBI
c) Controller of Certifying Authorities (CCA)
d) TRAI
Answer: c) Controller of Certifying Authorities (CCA)

---

14. What is the punishment for cyber terrorism under Section 66F?
a) 6 months imprisonment
b) Life imprisonment
c) Fine only
d) No punishment
Answer: b) Life imprisonment

---

15. Section 72 of the IT Act penalizes:
a) Online trolling
b) Breach of confidentiality and privacy
c) File sharing
d) SMS forwarding
Answer: b) Breach of confidentiality and privacy

---

16. Which act supports e-governance and electronic contracts legally?
a) RTI Act
b) IT Act 2000
c) Income Tax Act
d) Digital Security Act
Answer: b) IT Act 2000

---

17. The maximum penalty for damage to computer, system, or data under Section 43 is:
a) ₹1 lakh
b) ₹5 lakh
c) ₹10 lakh
d) ₹1 crore
Answer: d) ₹1 crore

---

18. Which of the following is NOT covered under IT Act?
a) Digital signatures
b) Cyber terrorism
c) Property disputes
d) Obscene content on the internet
Answer: c) Property disputes

---

19. Section 69 of the IT Act gives power to:
a) Register domain names
b) Intercept, monitor, or decrypt information for security reasons
c) Launch websites
d) Export software
Answer: b) Intercept, monitor, or decrypt information for security reasons

---

20. The primary purpose of IT Act is to:
a) Promote tourism
b) Control inflation
c) Provide legal framework for e-transactions and cybercrime laws
d) Improve entertainment industry
Answer: c) Provide legal framework for e-transactions and cybercrime laws

Hackers, Attackers & Countermeasures

Hackers & Attackers

1. Who is a hacker in cyber security?
a) Someone who plays online games
b) A person who illegally accesses computer systems
c) A software developer
d) A network engineer
Answer: b) A person who illegally accesses computer systems

---

2. Which type of hacker works with good intentions and helps improve security?
a) Black Hat Hacker
b) Grey Hat Hacker
c) White Hat Hacker
d) Red Hat Hacker
Answer: c) White Hat Hacker

---

3. Which type of hacker breaks into systems for malicious purposes?
a) White Hat
b) Black Hat
c) Red Hat
d) Blue Hat
Answer: b) Black Hat

---

4. A hacker who breaks into a system without malicious intent but without permission is a:
a) Red Hat
b) Grey Hat
c) White Hat
d) Cyber Cop
Answer: b) Grey Hat

---

5. Blue Hat Hackers are usually associated with:
a) Cyber warfare
b) Revenge-based hacking without deep technical knowledge
c) Ethical hacking exams
d) Network testing
Answer: b) Revenge-based hacking without deep technical knowledge

---

6. Red Hat Hackers are known for:
a) Passive defense
b) Fighting back against Black Hats
c) Teaching hacking
d) Writing malware
Answer: b) Fighting back against Black Hats

Common Cyber Attacks

7. Which of the following is a common form of cyber attack?
a) Data backup
b) Phishing
c) App download
d) Captcha solving
Answer: b) Phishing

---

8. A DoS (Denial of Service) attack aims to:
a) Secure a system
b) Backup data
c) Overwhelm a system to make it unavailable
d) Speed up software
Answer: c) Overwhelm a system to make it unavailable

---

9. What is a Trojan Horse?
a) A fake app that entertains
b) Malware disguised as legitimate software
c) Virus sent via USB
d) Software used for passwords
Answer: b) Malware disguised as legitimate software

---

10. SQL Injection targets which component?
a) Operating system
b) Database
c) Network
d) BIOS
Answer: b) Database

---

11. Keyloggers are used to:
a) Increase typing speed
b) Record user keystrokes secretly
c) Speed up RAM
d) Clean hard disks
Answer: b) Record user keystrokes secretly

---

12. What is sniffing in cyber security?
a) Cleaning hard drives
b) Capturing network traffic to steal data
c) Creating fake profiles
d) Compressing files
Answer: b) Capturing network traffic to steal data

Countermeasures & Prevention Techniques

13. What is the main goal of countermeasures in cybersecurity?
a) To attack hackers
b) To reduce the cost of hacking
c) To prevent or minimize the impact of cyber attacks
d) To delete all data
Answer: c) To prevent or minimize the impact of cyber attacks

---

14. Which of the following is NOT a cyber countermeasure?
a) Encryption
b) Installing malware
c) Firewall
d) Antivirus software
Answer: b) Installing malware

15. What is the best way to prevent phishing attacks?
a) Open all emails
b) Click on all links
c) Verify sender and avoid suspicious links
d) Forward emails to everyone
Answer: c) Verify sender and avoid suspicious links

---

16. Which technique helps protect data during transmission?
a) Formatting
b) Encryption
c) Copying
d) Rebooting
Answer: b) Encryption

---

17. What should you use to protect a network from unauthorized access?
a) Printer
b) Firewall
c) Scanner
d) Keyboard
Answer: b) Firewall

---

18. Which of these is a strong password example?
a) 12345
b) password
c) Qw!9#Xz$T7
d) name123
Answer: c) Qw!9#Xz$T7

---

19. Two-Factor Authentication (2FA) increases:
a) System speed
b) Internet bill
c) Account security
d) Website ads
Answer: c) Account security

---

20. Penetration testing is used to:
a) Enter social media accounts
b) Check vulnerabilities in systems
c) Create backups
d) Speed up computers
Answer: b) Check vulnerabilities in systems

Web Application Security

---

1. What is the purpose of Web Application Security?
a) To develop websites faster
b) To protect users from spam
c) To secure web applications from threats and vulnerabilities
d) To create attractive designs
Answer: c) To secure web applications from threats and vulnerabilities

---

2. Which of the following is a web application vulnerability?
a) SQL Injection
b) Disk formatting
c) Disk fragmentation
d) Internet sharing
Answer: a) SQL Injection

---

3. Which organization releases the OWASP Top 10 vulnerabilities list?
a) Google
b) Microsoft
c) OWASP Foundation
d) W3C
Answer: c) OWASP Foundation

---

4. What is the OWASP Top 10?
a) Top 10 websites
b) Top 10 cyber laws
c) Top 10 security risks in web applications
d) Top 10 Google tools
Answer: c) Top 10 security risks in web applications

---

5. A web application is vulnerable if:
a) It is mobile responsive
b) It stores user data securely
c) It doesn't validate user input
d) It uses modern UI
Answer: c) It doesn't validate user input

---

6. What is SQL Injection?
a) A database design method
b) Injecting JavaScript into web apps
c) Inserting malicious SQL queries into user input fields
d) A type of encryption
Answer: c) Inserting malicious SQL queries into user input fields

---

7. Cross-Site Scripting (XSS) is used to:
a) Hack emails
b) Inject malicious scripts into web pages
c) Scan for viruses
d) Increase website traffic
Answer: b) Inject malicious scripts into web pages

---

8. CSRF stands for:
a) Cyber Security Report File
b) Central Secure Response Force
c) Cross Site Request Forgery
d) Client Script Runtime Framework
Answer: c) Cross Site Request Forgery

---

9. Session Hijacking is:
a) Protecting user sessions
b) Tracking cookies
c) Stealing valid session IDs to impersonate users
d) Refreshing websites
Answer: c) Stealing valid session IDs to impersonate users

---

10. Which attack allows attackers to access unauthorized files via the URL?
a) SQL Injection
b) Broken Authentication
c) Directory Traversal
d) Phishing
Answer: c) Directory Traversal

---

11. What is Broken Authentication?
a) A website login page
b) Misuse or exposure of authentication credentials
c) Forgetting a password
d) Changing username
Answer: b) Misuse or exposure of authentication credentials

---

12. What is Security Misconfiguration?
a) Fast website setup
b) Improper setup of security headers, servers, or permissions
c) Installing firewalls
d) Missing images
Answer: b) Improper setup of security headers, servers, or permissions

---

13. Insecure Deserialization refers to:
a) Slow loading of websites
b) Converting data into images
c) Executing malicious code by tampering with serialized data
d) File transfer
Answer: c) Executing malicious code by tampering with serialized data

---

14. Which one is NOT a web application attack?
a) XSS
b) DoS
c) CSRF
d) Format Conversion
Answer: d) Format Conversion

Digital Infrastructure Security

---

1. What does digital infrastructure security aim to protect?
a) Roads and bridges
b) Software games
c) Network, data centers, servers, and cloud environments
d) Social events
Answer: c) Network, data centers, servers, and cloud environments

---

2. Which of the following is part of digital infrastructure?
a) Internet cables
b) Cloud storage
c) Data centers
d) All of the above
Answer: d) All of the above

---

3. What is a major threat to digital infrastructure?
a) Rainfall
b) Power surge
c) DDoS (Distributed Denial of Service) attack
d) Loud noise
Answer: c) DDoS (Distributed Denial of Service) attack

---

4. Which of the following protects digital infrastructure from unauthorized access?
a) Firewall
b) Mouse
c) Monitor
d) Keyboard
Answer: a) Firewall

---

5. A VPN (Virtual Private Network) helps by:
a) Watching videos faster
b) Encrypting internet connections
c) Increasing ad views
d) Deleting viruses
Answer: b) Encrypting internet connections

---

6. What does a Data Center primarily store?
a) Videos
b) Hardware components
c) Digital data and applications
d) Online tickets
Answer: c) Digital data and applications

---

7. Which government initiative supports digital infrastructure in India?
a) Make in India
b) Digital India
c) Skill India
d) Cyber India
Answer: b) Digital India

---

8. What is the purpose of Network Access Control (NAC)?
a) To format hard disks
b) To restrict device access to the network
c) To improve UI
d) To track file downloads
Answer: b) To restrict device access to the network

---

9. Cloud infrastructure is secured using:
a) Public WiFi
b) Shared passwords
c) Access control, encryption, and monitoring
d) Loud alarms
Answer: c) Access control, encryption, and monitoring

---

10. What is physical security in digital infrastructure?
a) Encrypting data
b) Installing anti-virus
c) Protecting hardware from theft and damage
d) Securing websites
Answer: c) Protecting hardware from theft and damage

Defensive Programming

---

11. What is Defensive Programming?
a) Writing stylish code
b) Writing code that avoids syntax errors
c) Writing secure code to anticipate and handle unexpected inputs or behavior
d) Compressing code
Answer: c) Writing secure code to anticipate and handle unexpected inputs or behavior

---

12. Defensive programming is mainly used to:
a) Increase performance only
b) Avoid compiler warnings
c) Improve code reliability and security
d) Hide errors
Answer: c) Improve code reliability and security

---

13. Which of the following is a key principle of defensive programming?
a) Trust all inputs
b) Ignore exceptions
c) Validate input data
d) Write code once
Answer: c) Validate input data

---

14. Input validation is essential because:
a) It saves memory
b) It prevents unauthorized or dangerous operations
c) It removes white spaces
d) It allows free access
Answer: b) It prevents unauthorized or dangerous operations

---

15. What should be used to handle unexpected input or program failure?
a) Alerts
b) Exception handling
c) Copy-paste code
d) Formatting
Answer: b) Exception handling

---

16. Which of the following practices enhances defensive programming?
a) Hardcoding passwords
b) Avoiding error messages
c) Using assertions
d) Skipping comments
Answer: c) Using assertions

---

17. Boundary checking helps in:
a) Shortening programs
b) Preventing buffer overflows
c) Reducing graphics
d) Enhancing colors
Answer: b) Preventing buffer overflows

---

18. Which language feature helps in handling errors gracefully?
a) Loops
b) Try-Catch blocks
c) Comments
d) Variables
Answer: b) Try-Catch blocks

---

19. A secure way to handle user credentials in code is:
a) Use plain text files
b) Use environment variables or secure vaults
c) Write them on screen
d) Store in Excel files
Answer: b) Use environment variables or secure vaults

---

20. Defensive programming improves:
a) Code readability
b) Code security and fault tolerance
c) Video quality
d) Output printing
Answer: b) Code security and fault tolerance

---

21. Why is "never trust user input" a common rule in defensive programming?
a) Users always type in caps
b) Input can be manipulated to exploit vulnerabilities
c) It helps design faster websites
d) Reduces storage
Answer: b) Input can be manipulated to exploit vulnerabilities

---

22. Logging errors during program execution is useful for:
a) Reducing code size
b) Watching logs
c) Debugging and auditing
d) Deleting old code
Answer: c) Debugging and auditing

---

23. Which of the following is NOT a defensive programming technique?
a) Input validation
b) Output encoding
c) Ignoring errors
d) Error logging
Answer: c) Ignoring errors

---

24. Which programming style is most secure?
a) Defensive
b) Aggressive
c) Lazy
d) Obfuscated
Answer: a) Defensive

---

25. Defensive programming is best described as:
a) Writing complex code
b) Coding with assumptions
c) Coding with care to protect against misuse
d) Coding without testing
Answer: c) Coding with care to protect against misuse

Information Destroying and Recovery Tools

---

1. What is the main goal of information destroying tools?
a) Recover deleted files
b) Compress files
c) Permanently delete data beyond recovery
d) Hide files in folders
Answer: c) Permanently delete data beyond recovery

---

2. Which of the following tools is used for secure file deletion?
a) WinRAR
b) CCleaner
c) Eraser
d) Notepad
Answer: c) Eraser

---

3. Which process is used by data destroying tools to ensure data cannot be recovered?
a) Formatting
b) Data masking
c) Data overwriting (wiping)
d) Compression
Answer: c) Data overwriting (wiping)

---

4. Which of these is a command-line tool used in Linux to destroy data?
a) rm
b) mv
c) shred
d) grep
Answer: c) shred

---

5. A disk wipe tool:
a) Makes backup copies
b) Destroys physical disk
c) Overwrites entire disk with random data
d) Resets passwords
Answer: c) Overwrites entire disk with random data

---

6. Formatting a hard disk:
a) Always deletes data permanently
b) Makes data unrecoverable
c) Can sometimes be recovered
d) Sends data to Recycle Bin
Answer: c) Can sometimes be recovered

---

7. Which method is considered safest for destroying confidential information?
a) Delete button
b) Shift+Delete
c) Overwriting with data wiping tools
d) Compress and move
Answer: c) Overwriting with data wiping tools

---

8. Physical destruction of storage devices includes:
a) Data encryption
b) Melting, shredding, or degaussing
c) Uploading to cloud
d) Disabling keyboard
Answer: b) Melting, shredding, or degaussing

Data Recovery Tools

9. Which of the following tools can be used to recover deleted files?
a) Eraser
b) Recuva
c) Disk Destroyer
d) Format Tool
Answer: b) Recuva

---

10. Data recovery is successful when:
a) File is in Recycle Bin only
b) Data is overwritten
c) Sectors are intact and not overwritten
d) Disk is physically destroyed
Answer: c) Sectors are intact and not overwritten

---

11. Which tool is known for deep scan file recovery?
a) CCleaner
b) VLC
c) EaseUS Data Recovery
d) Snipping Tool
Answer: c) EaseUS Data Recovery

---

12. Data recovery software works by:
a) Creating new files
b) Reading index of lost or deleted data sectors
c) Encrypting files
d) Locking disk
Answer: b) Reading index of lost or deleted data sectors

---

13. Which of these is a free file recovery tool?
a) Notepad++
b) Recuva
c) BitLocker
d) TeamViewer
Answer: b) Recuva

---

14. Which tool is best for recovering data from formatted drives?
a) Paint
b) MS Word
c) Stellar Data Recovery
d) Control Panel
Answer: c) Stellar Data Recovery

---

15. Recovery is NOT possible when:
a) File is renamed
b) Disk is formatted once
c) Disk has been wiped using secure erase tools
d) File is moved to another folder
Answer: c) Disk has been wiped using secure erase tools

Destroying Sensitive Information

---

1. What does destroying sensitive information mean in cyber security?
a) Archiving the data
b) Making data unreadable and unrecoverable
c) Sending data to cloud
d) Locking the folder
Answer: b) Making data unreadable and unrecoverable

---

2. Which of the following methods is most secure for destroying sensitive digital data?
a) Deleting the file
b) Moving to recycle bin
c) Overwriting using a data wiping tool
d) Renaming the file
Answer: c) Overwriting using a data wiping tool

---

3. Which command-line tool in Linux is used for securely deleting files?
a) ls
b) rm
c) shred
d) sudo
Answer: c) shred

---

4. What does data wiping involve?
a) Encrypting files
b) Replacing file names
c) Overwriting data with random bits multiple times
d) Formatting file extensions
Answer: c) Overwriting data with random bits multiple times

---

5. Which of the following tools is widely used for securely erasing data on Windows?
a) Notepad
b) Eraser
c) WinRAR
d) Paint
Answer: b) Eraser

---

6. Deleting files using Shift+Delete:
a) Permanently destroys files
b) Sends them to backup
c) Removes from Recycle Bin but recoverable
d) Encrypts the file
Answer: c) Removes from Recycle Bin but recoverable

---

7. What is the purpose of using disk wipe software?
a) Improve disk speed
b) Securely erase entire hard disk
c) Create new partitions
d) Recover deleted files
Answer: b) Securely erase entire hard disk

---

8. Which technique ensures sensitive data cannot be recovered from a storage device?
a) Formatting
b) Compression
c) Secure erasure
d) Defragmentation
Answer: c) Secure erasure

---

9. What is DBAN used for?
a) Backup software
b) Antivirus software
c) Boot and Nuke disk wiping
d) Password generator
Answer: c) Boot and Nuke disk wiping

---

10. What is degaussing?
a) Cooling hard drives
b) Magnetically erasing data from magnetic storage devices
c) Encrypting USB drives
d) Compressing SSDs
Answer: b) Magnetically erasing data from magnetic storage devices

---

11. Which of the following is not a secure method of destroying sensitive information?
a) Data overwriting
b) Physical destruction
c) Deleting files only
d) Degaussing
Answer: c) Deleting files only

---

12. What is physical destruction of sensitive data?
a) Deleting files
b) Formatting disk
c) Shredding or crushing storage devices
d) Backing up data
Answer: c) Shredding or crushing storage devices

---

13. Which of the following methods is suitable for destroying printed sensitive information?
a) Crumpling
b) Shredding
c) Filing
d) Folding
Answer: b) Shredding

---

14. Why is formatting not considered a fully secure way to destroy data?
a) It slows the computer
b) It doesn't affect the OS
c) The data can still be recovered with tools
d) It is expensive
Answer: c) The data can still be recovered with tools

---

15. For highly classified data, which combination is best for destruction?
a) Move to trash + rename
b) Delete + Reboot
c) Secure wipe + Physical destruction
d) Format + Print
Answer: c) Secure wipe + Physical destruction