Zed-King
GROUP OF INSTITUTIONS
ISO 9001: 2015 Certified

COURSE ON COMPUTER CONCEPTS

OVERVIEW OF CYBER SECURITY

Topics Covered:

#	Topic	#	Topic
9.0	Cyber Security	9.0.4	Securing Email and Social Media Accounts (Facebook, Instagram, WhatsApp)
9.0.1	Need and Goal of Cyber Security	9.0.5	Securing Smart Phone
9.0.2	Securing PC	9.1	Summary
9.0.3	Securing Browser	9.2	Model Questions and Answers

Zedking Group Of Institutions

SECTION 1: CYBER SECURITY — NEED AND GOALS

9.0 Cyber Security

> *Cyber security is the practice of protecting computers, mobile phones, networks, programs, accounts and data from digital attacks, theft, damage and unauthorized access. It is also called **information security** or **IT security**.*

We use the Internet for banking, shopping, studying, social media and government services, so our personal data and money are online. **Cyber crime** means any crime done using a computer, mobile or the Internet — for example online fraud, hacking, identity theft, data theft, cyberbullying and spreading fake or obscene content. Cyber security protects us from these crimes. Remember: **security is a shared responsibility** — technology helps, but safe habits of the user are equally important.

Important terms

Term	Meaning
Threat	Anything that can cause harm to a system or data (virus, hacker, phishing)
Vulnerability	A weakness (old software, weak password) that an attacker can use
Attack	An attempt to damage, steal or get unauthorized access to a system
Hacker	Person who gains access to computer systems. White hat = ethical (permitted), Black hat = criminal, Grey hat = in between
Authentication	Proving identity — password, OTP, fingerprint, face
Authorization	Deciding what an authenticated user may do (access rights)
Encryption	Converting data into a secret code so that only the right person can read it
Firewall	Hardware/software that filters network traffic and blocks unauthorized access
Patch / Update	Software fix that removes security weaknesses
Backup	Extra copy of data for recovery after loss or ransomware

9.0.1 Need and Goal of Cyber Security

A. Need of Cyber Security

- **Protect personal and financial data** — Aadhaar, PAN, bank, card and UPI details, photos, passwords.
- **Prevent financial loss** from online frauds, phishing, fake apps and fake calls.
- **Protect privacy and identity** — stop identity theft and misuse of personal information.
- **Protect computers and phones** from viruses, ransomware and data loss.
- **Protect business and government** — customer data, trade secrets, critical services such as banking, power, railways, hospitals and defence.
- **Safe growth of Digital India** — digital payments, e-governance and e-commerce need trust.
- **Protect children and society** from cyberbullying, harassment, fake news and harmful content.
- **Legal requirement** — organizations must protect personal data under laws such as the IT Act and the Digital Personal Data Protection Act, 2023.

B. Goals of Cyber Security — the CIA Triad

Goal	Meaning	Example
Confidentiality	Only authorized persons can see the information	Password, encryption, OTP, access control
Integrity	Information remains correct and is not changed by unauthorized persons	Backup, checksums, digital signature
Availability	Information and services are available to authorized users whenever needed	Backup, power backup, protection against DDoS

- Other goals: **Authentication** (who is the user?), **Non-repudiation** (a sender cannot deny sending a message — digital signature), **Accountability** (actions can be traced to a user).

Zedking Group Of Institutions

C. Common Cyber Threats and Attacks

Threat	Description	Protection
Virus	Program that attaches to files, spreads when the file is run and damages data	Antivirus, no pirated software
Worm	Spreads by itself through networks without user action	Updates, firewall
Trojan horse	Looks like useful software but carries harmful code / opens a backdoor	Download only from official sources
Ransomware	Encrypts files and demands money (ransom) to unlock them	Backup, updates, caution with attachments
Spyware / Keylogger	Secretly records activity, keystrokes and passwords	Antivirus, scan pen drives
Adware	Shows unwanted advertisements and pop-ups	Avoid free dubious software, ad-blocker
Phishing / Smishing / Vishing	Fake e-mail / SMS / phone call pretending to be a bank or company to steal data	Never click unknown links; never share OTP/PIN
Social engineering	Manipulating people to reveal secrets or give access	Awareness; verify the person
Brute force / Password attack	Trying many passwords to break an account	Long passwords, 2FA
DoS / DDoS	Floods a server with requests so that real users cannot use it	Firewall, traffic filtering
Man-in-the-Middle	Attacker secretly listens/alters communication, often on public Wi-Fi	HTTPS, VPN, avoid open Wi-Fi
Identity theft	Using someone's personal data to cheat or open accounts	Protect Aadhaar/PAN, monitor accounts
Data breach	Leak of data from a company's server	Strong passwords, change passwords after breach
Online / UPI frauds	Fake KYC, lottery, job, courier, QR-scan, remote-access app and "customer care" scams	Verify; never share OTP; use 1930
Cyberbullying / Stalking	Harassing or threatening a person online	Block, report, keep evidence

Cyber Laws and Reporting in India

Item	Details
IT Act, 2000 (amended 2008)	Main cyber law. Covers hacking, data theft, identity theft (Sec. 66C), cheating by personation (Sec. 66D), violation of privacy (Sec. 66E), publishing obscene material (Sec. 67), cyber terrorism etc.
Digital Personal Data Protection Act, 2023	Protects personal data of citizens and sets duties for organizations handling it
CERT-In	Indian Computer Emergency Response Team — national agency for responding to cyber security incidents
National Cyber Crime Reporting Portal	**cybercrime.gov.in** — report any cyber crime online; special facility for crimes against women and children
Helpline 1930	National helpline for reporting financial cyber fraud — report immediately so that the money can be frozen
Local police / Cyber Cell	File a complaint (FIR) and give evidence — screenshots, transaction ID, phone numbers

> **Important:** If money is lost in an online fraud: call **1930** at once, inform your bank to block the card/account, and report at **cybercrime.gov.in**. The sooner it is reported, the better the chance of recovery.

Zedking Group Of Institutions

SECTION 2: SECURING PC AND BROWSER

9.0.2 Securing PC

> *Securing a PC means taking steps to protect the computer, its programs and the data stored in it from viruses, hackers, theft and accidental loss. The steps below are for Windows 10/11.*

Security Step	How to do it
1. Keep Windows and programs updated	Settings → **Windows Update** → Check for updates → Install; turn on automatic updates. Update browsers, Office and other programs too
2. Use antivirus / Windows Security	Settings → Privacy & security → **Windows Security** → Virus & threat protection → keep **Real-time protection ON** → run **Quick scan / Full scan**. Use only one good antivirus and keep it updated
3. Keep the Firewall ON	Windows Security → **Firewall & network protection** → make sure it is ON for all networks
4. Use strong passwords and screen lock	Set a password/PIN for every user account; lock the PC with **Win + L** when leaving; set auto-lock in Settings → Accounts → Sign-in options
5. Use a Standard account for daily work	Use an Administrator account only for installing software; create a separate standard account for daily use or for children (Settings → Accounts → Other users)
6. Install software carefully	Install only genuine software from official websites/stores; avoid pirated/cracked software; click Yes on User Account Control (UAC) only when you started the installation
7. Scan USB drives and downloads	Scan pen drives with antivirus before opening files; turn off AutoPlay; do not open e-mail attachments from unknown senders
8. Take regular backup	Follow the **3-2-1 rule**: 3 copies, 2 types of media (PC + external drive), 1 off-site (cloud). Use File History / OneDrive / external hard disk
9. Encrypt the drive	Turn on **BitLocker / Device encryption** (Settings → Privacy & security → Device encryption) so that data is safe if the PC is stolen
10. Secure the network	Use a strong Wi-Fi password (WPA2/WPA3), change the default router password, switch off Remote Desktop and file sharing if not needed
11. Physical security	Do not leave the PC unattended; use a BIOS/UEFI password; keep the laptop in a safe place; use a cable lock in public places
12. Safe disposal	Before selling/giving away a PC, back up data and reset it (Settings → System → Recovery → Reset this PC → Remove everything / clean the drive)

Signs that your PC may be infected

- The computer has become very slow, hangs or restarts on its own.
- Unknown programs, toolbars or pop-up ads appear; browser home page changes.
- Files are missing/locked, or a message demands money; antivirus is switched off by itself.
- High disk/Internet use without any reason; friends receive strange messages from your account.

What to do: disconnect from the Internet, run a full antivirus scan (Windows Security → Scan options → Full scan or Microsoft Defender Offline scan), remove the suspicious programs (Settings → Apps), change the important passwords from a clean device and restore data from backup if needed.

9.0.3 Securing Browser

> *The browser is the main gateway to the Internet, so it is the target of many attacks such as fake websites, malicious downloads, tracking and password theft. A secure browser setting protects the user's privacy and data.*

Security Step	How to do it
1. Update the browser	Chrome: ⋮ menu → Help → About Google Chrome (updates automatically); Edge: ··· → Help and feedback → About Microsoft Edge; restart after the update
2. Look for https:// and the padlock	Enter passwords, OTP and card details only on **https** sites. Check the spelling of the web address (www.sbi.co.in vs www.sbi-login.xyz). Type the address yourself or use bookmarks for banks

Zedking Group of Institutions

Security Step	How to do it
3. Turn on Safe Browsing	Chrome: Settings → **Privacy and security** → **Security** → **Safe Browsing** (Standard or Enhanced protection). Edge: Settings → Privacy, search and services → **Microsoft Defender SmartScreen** ON
4. Block pop-ups and risky permissions	Settings → Privacy and security → **Site settings** → block Pop-ups and redirects; review Location, Camera, Microphone and Notifications permissions; never allow notifications from unknown sites
5. Control cookies and tracking	Site settings → Third-party cookies → **Block third-party cookies**; send "Do Not Track" request; clear cookies periodically
6. Clear browsing data	**Ctrl + Shift + Delete** → select History, Cookies, Cached images, Passwords/Autofill (if needed) → Clear data; do this on shared/public computers
7. Handle saved passwords carefully	Do not save passwords/card details on a shared PC. Use a trusted password manager or the browser's password manager protected by the device lock
8. Install only trusted extensions	Add extensions only from the official store with good reviews and few permissions; remove those you do not use
9. Use Incognito / Private window on shared PCs	It does not store history, cookies or form data **on that device**, but websites, employer, school and the ISP can still see your activity — it is not full anonymity
10. Download safely	Download from official sites only; check the file type (.exe, .zip, .apk); scan the download; do not open files from pop-ups
11. Be careful on public Wi-Fi	Avoid logging in to banking on open Wi-Fi; use mobile data or a trusted VPN; turn off auto-connect to open networks
12. Sign out of accounts	Sign out of the browser profile and sites after use on someone else's device

How to recognize a fake (phishing) website

- The address has spelling mistakes, extra words or odd domain endings (.xyz, .top); the site is not https or shows a browser warning.
- The page asks for **OTP, PIN, CVV or full card/Aadhaar details** without a proper reason; offers huge prizes/discounts; shows urgent messages like "account will be blocked".
- The link came from an unknown SMS, WhatsApp message, e-mail or advertisement. If in doubt, type the official address yourself or use the official app.

Zedking Group Of Institutions

SECTION 3: SECURING E-MAIL, SOCIAL MEDIA AND SMART PHONE

9.0.4 Securing Email and Social Media Accounts (Facebook, Instagram, WhatsApp)

A. Common Account Safety Rules

Rule	Explanation
Strong and unique password	At least 12 characters, a mix of letters, numbers and symbols, or a passphrase of 3–4 random words. Use a **different password for every account**; never use name, mobile number, date of birth or 123456
Two-factor authentication (2FA / 2-Step Verification)	Turn it ON everywhere — an OTP/authenticator app/security key is needed in addition to the password
Recovery information	Keep the recovery mobile number and recovery e-mail updated so that the account can be recovered
Beware of phishing	Do not click links or open attachments in unexpected messages; check the sender's address; companies never ask for passwords or OTP
Log out and check devices	Log out on shared devices; review the list of logged-in devices and remove the unknown ones
Review third-party app access	Remove apps/websites that you no longer use or do not trust (they may have access to your account)
Limit personal information	Do not post phone number, address, Aadhaar/PAN, tickets, boarding passes, or travel plans publicly
Think before you post or share	Posts, photos and comments can stay forever; do not share fake news, rumours or private photos
Accept friends carefully	Accept requests only from people you know; beware of fake profiles and strangers asking for money or personal photos
Report and block	Use Report and Block for abusive, fake or suspicious accounts; keep screenshots as evidence

B. Securing E-mail Account (Gmail example)

- Create a strong password; do not use it anywhere else. Change it if you suspect a leak (Manage your Google Account → Security → Password).
- Turn on **2-Step Verification**: Google Account → **Security** → **2-Step Verification** → Get started → verify using phone prompt/SMS/authenticator app. Save the backup codes.
- Run **Security Checkup** (Google Account → Security) to review devices, recent activity, third-party access and recovery options.
- Do not open unknown attachments (.exe, .zip, .docm); hover on a link to see the real address; use **Report spam / Report phishing** in the mail options.
- Check **Last account activity** (Details at the bottom of the Inbox) and sign out of other sessions if needed.
- Do not use public Wi-Fi/computers to log in; never share the OTP received on mail or phone.

C. Securing Facebook

- Open **Settings & privacy** → **Settings** → **Accounts Center** → **Password and security** → **Two-factor authentication** → choose the Facebook account → select Authentication app / SMS → follow the steps.
- Turn on **Login alerts** (Password and security → Where you're logged in / Login alerts) and log out of unknown devices.
- Use **Privacy Checkup** (Settings & privacy → Privacy Checkup): choose who can see your posts (Friends instead of Public), who can send friend requests, who can find you by phone/e-mail, and limit old posts.
- Review **Apps and websites** connected to the account and remove unused ones; turn on profile locking (where available) to protect the profile picture and posts.
- Do not accept unknown friend requests; **report** fake profiles and abusive content; avoid "quizzes", "who viewed my profile" and lottery links.

D. Securing Instagram

- Open **Profile** → ☰**Menu** → **Accounts Center** → **Password and security** → **Two-factor authentication** → select the account → use an authentication app or SMS.
- Make the account **Private**: Settings and privacy → **Account privacy** → Private account ON; check who can message, tag and mention you.

Zedking Group Of Institutions

- Use **Close Friends** for personal stories; turn off activity status/location tagging if not needed; control comments with **Hidden Words** and Restrict/Block.
- Check **Login activity** (Accounts Center → Password and security → Where you're logged in) and remove unknown devices.
- Beware of fake "verification badge", "copyright violation" and "free followers" messages — never enter the Instagram password on any link; Instagram does not ask for it in DMs.

E. Securing WhatsApp

- **Never share the 6-digit SMS verification code** with anyone — fraudsters use it to take over your account.
- Turn on **Two-step verification**: WhatsApp → Settings → **Account** → **Two-step verification** → **Turn on** → set a 6-digit PIN and add an e-mail address for recovery. Do not share this PIN.
- **Privacy settings** (Settings → Privacy): set Last seen, Profile photo, About and Status to "My contacts"; set **Groups** to "My contacts" so that strangers cannot add you to groups; turn on **Read receipts** as needed; use **Privacy Checkup**.
- Use **App lock / Chat lock** (fingerprint/face) and **Disappearing messages** for sensitive chats.
- Check **Linked devices** (Settings → Linked devices) and log out unknown WhatsApp Web sessions.
- Messages are **end-to-end encrypted**, but fraud still happens by tricking users. Do not click links of unknown senders, do not scan unknown QR codes, never send money to "relatives/officers" asking urgently, verify by a phone call.
- Install WhatsApp only from the official store; avoid modified apps (such as "GB WhatsApp"); beware of fake "WhatsApp Gold", wedding-invitation APK, parcel/KYC and job-offer scams; report and block unknown numbers.

> **What to do:** Account hacked? Immediately (1) change the password from a safe device, (2) log out of all devices, (3) check 2FA/recovery details, (4) tell friends not to trust messages from your account, and (5) use the platform's "hacked account" recovery page and report to cybercrime.gov.in if money is involved.

Zedking Group Of Institutions

9.0.5 Securing Smart Phone

> *A smartphone holds our contacts, photos, messages, bank apps, UPI and documents, so it needs security like a computer. Phones can be attacked through fake apps, fake links, public Wi-Fi/charging points, SIM swap and theft.*

Security Step	How to do it
1. Screen lock	Set a PIN/pattern/password (6 digits or more) plus fingerprint/face unlock; auto-lock in 30 seconds–1 minute. Android: Settings → Security (or Lock screen); iPhone: Settings → Face ID & Passcode
2. Update the phone and apps	Android: Settings → System → **Software update**; iPhone: Settings → General → **Software Update**; keep automatic updates ON for apps (Play Store / App Store)
3. Install apps from official stores only	Google Play Store / Apple App Store; avoid APK files from WhatsApp, Telegram or unknown websites; check developer name, reviews and downloads; keep **Google Play Protect** ON (Play Store → profile → Play Protect)
4. Check app permissions	Android: Settings → Apps → **Permission manager** (iPhone: Settings → Privacy & Security); allow camera, microphone, location, contacts and SMS only when really needed; remove unused apps
5. Never install remote-access apps for strangers	Apps like AnyDesk, TeamViewer or QuickSupport give full control of your phone; fraudsters ask you to install them in "customer care" or "refund" scams
6. Secure SIM and mobile number	Set a **SIM PIN**; if the network suddenly disappears on your phone, contact the operator (SIM-swap fraud); keep the bank-linked number safe
7. Use locator and remote-wipe	Turn on **Find My Device / Find Hub** (Android) or **Find My iPhone** (iPhone) to locate, ring, lock or erase a lost phone
8. Take backup and encrypt	Back up photos/contacts to Google/iCloud; modern phones encrypt storage when a screen lock is set
9. Be careful with Wi-Fi, Bluetooth and charging	Turn off Wi-Fi/Bluetooth/NFC when not in use; avoid open Wi-Fi for banking; do not use public USB charging stations ("juice jacking") — use your own charger/power bank
10. Secure payment apps	Keep UPI PIN secret; use app lock for UPI/banking apps; never scan QR or approve a "collect request" to receive money; check the payee name
11. Avoid rooting / jailbreaking	It removes built-in protections and makes the phone easier to attack
12. Beware of fake calls, SMS and links	Do not click links in SMS/WhatsApp from unknown numbers; banks never ask for OTP/PIN/CVV on call; report suspicious numbers

If the phone is lost or stolen

- Use **Find My Device / Find My iPhone** to locate, lock or erase the phone.
- Call the mobile operator to **block the SIM**; get a duplicate SIM. Change passwords of Google/Apple, e-mail, social media and banking accounts; block UPI/net banking and cards through the bank.
- File an **FIR / complaint** with the police; note the **IMEI number** (printed on the box or by dialling *#06# earlier). Use the Government's **Sanchar Saathi** portal (sancharsaathi.gov.in) to block a lost/stolen phone through the CEIR system and to trace it.

Quick Do's and Don'ts

Do's	Don'ts
Use strong, different passwords and 2FA	Do not share OTP, PIN, CVV, passwords
Update software, apps and the OS regularly	Do not click on unknown links, SMS, or attachments
Install apps/software from official sources	Do not install cracked software or unknown APKs
Take regular backups	Do not use public Wi-Fi/computers for banking
Check the website/app name and https	Do not give remote access of your device to strangers
Report fraud quickly — 1930, cybercrime.gov.in	Do not post personal details or private photos publicly

Zedking Group of Institutions

SECTION 4: SUMMARY

9.1 Summary

Cyber Security — Need and Goals

- Cyber security protects computers, networks, accounts and data from cyber attacks. Need: protect personal/financial data, privacy, money, business and Digital India services.
- Goals — CIA triad: **Confidentiality** (secrecy), **Integrity** (accuracy), **Availability** (access when needed).
- Threats: virus, worm, trojan, ransomware, spyware, adware, phishing/smishing/vishing, social engineering, DoS/DDoS, man-in-the-middle, identity theft, online frauds, cyberbullying.
- Laws and reporting: IT Act 2000, DPDP Act 2023, CERT-In, cybercrime.gov.in, helpline 1930.

Securing PC and Browser

- PC: update Windows and software, keep Windows Security (antivirus) and firewall ON, use strong passwords and Win + L, standard user account, genuine software, scan USB drives, backup (3-2-1), BitLocker, secure Wi-Fi.
- Browser: update, use https/padlock, Safe Browsing, block pop-ups/third-party cookies, clear browsing data (Ctrl + Shift + Delete), do not save passwords on shared PCs, trusted extensions only, beware of fake websites and public Wi-Fi.

Securing Accounts and Smartphone

- Accounts: strong unique password, 2-step verification, recovery details, login alerts, privacy checkup, review linked devices/apps, beware phishing, report and block.
- WhatsApp: never share the 6-digit code; turn on two-step verification PIN; set privacy; Instagram: private account; Facebook: Privacy Checkup and login alerts.
- Smartphone: screen lock, updates, official app stores, app permissions, Play Protect, Find My Device, SIM PIN, no remote-access apps for strangers, avoid public Wi-Fi/USB charging, block lost phone through Sanchar Saathi.

Zedking Group Of Institutions

SECTION 5: MODEL QUESTIONS AND ANSWERS

9.2 Model Questions and Answers

> *These questions are commonly asked in exams. Correct answers are marked with ✓and an explanation is provided.*

Part A: Multiple Choice Questions (MCQs)

Q1. Cyber security means:

(a) Protecting computers, networks, data and users from cyber attacks ✓
(b) Selling computers
(c) Repairing printers
(d) Designing websites

Explanation: *Cyber security is the practice of protecting systems, networks, programs and data from digital attacks and misuse.*

Q2. CIA triad in cyber security stands for:

(a) Confidentiality, Integrity, Availability ✓
(b) Computer, Internet, Application
(c) Control, Insurance, Access
(d) Code, Information, Audit

Explanation: *Confidentiality (secret), Integrity (correct/unchanged) and Availability (accessible when needed) are the three goals.*

Q3. Keeping information secret from unauthorized persons is called:

(a) Confidentiality ✓
(b) Integrity
(c) Availability
(d) Redundancy

Explanation: *Confidentiality means only authorized people can access the information.*

Q4. Making sure that data is not changed or damaged by unauthorized persons is:

(a) Integrity ✓
(b) Confidentiality
(c) Availability
(d) Encryption only

Explanation: *Integrity keeps the data accurate and unaltered.*

Q5. Malware stands for:

(a) Malicious software ✓
(b) Mail software
(c) Main hardware
(d) Manual ware

Explanation: *Malware is harmful software such as viruses, worms, trojans, ransomware and spyware.*

Q6. Which malware locks the files and demands money to unlock them?

(a) Ransomware ✓
(b) Adware
(c) Spyware
(d) Firewall

Explanation: *Ransomware encrypts files and demands a ransom payment.*

Q7. Which malware secretly records the activities of the user?

(a) Spyware ✓
(b) Antivirus
(c) Firewall
(d) Patch

Explanation: *Spyware (keyloggers) secretly collects information such as passwords.*

Q8. A program that looks useful but secretly carries harmful code is called a:

(a) Trojan horse ✓
(b) Worm
(c) Firewall
(d) Patch

Explanation: *A Trojan pretends to be genuine software but performs harmful actions.*

Zedking Group Of Institutions

Q9. Fake e-mails/messages/websites that trick users into giving passwords or bank details are called:

(a) Phishing ✓
(b) Streaming
(c) Tethering
(d) Booting

Explanation: *Phishing is a fraud technique using fake communication that looks genuine.*

Q10. Fraud through phone calls is called:

(a) Vishing ✓
(b) Smishing
(c) Hashing
(d) Pharming only

Explanation: *Vishing = voice phishing; smishing = SMS phishing.*

Q11. Tricking people psychologically into revealing secrets is:

(a) Social engineering ✓
(b) Data mining
(c) Compiling
(d) Tethering

Explanation: *Social engineering manipulates the human, not the computer.*

Q12. DoS / DDoS attack:

(a) Floods a server so that it cannot serve genuine users ✓
(b) Encrypts files
(c) Steals Aadhaar
(d) Deletes cookies

Explanation: *A Denial of Service attack overloads a website/server and makes it unavailable.*

Q13. A person who hacks with permission to find and fix weaknesses is called a:

(a) White hat hacker ✓
(b) Black hat hacker
(c) Cracker only
(d) Spammer

Explanation: *Ethical (white hat) hackers help organizations improve security.*

Q14. Which Indian law deals with cyber crimes and e-commerce?

(a) Information Technology Act, 2000 ✓
(b) Companies Act
(c) Motor Vehicles Act
(d) Consumer Credit Act

Explanation: *The IT Act, 2000 (amended in 2008) is India's main cyber law.*

Q15. The national helpline for reporting financial cyber fraud in India is:

(a) 1930 ✓
(b) 100 only
(c) 108 only
(d) 1800-0000 only

Explanation: *Dial 1930 and report at cybercrime.gov.in as early as possible.*

Q16. The official portal to report cyber crime in India is:

(a) cybercrime.gov.in ✓
(b) irctc.co.in
(c) passportindia.gov.in
(d) ors.gov.in

Explanation: *National Cyber Crime Reporting Portal: cybercrime.gov.in.*

Q17. Which is a strong password?

(a) T@ke#Care!2026Pen ✓
(b) 123456
(c) password
(d) ajay1234

Explanation: *A long mix of letters, numbers and symbols that is not related to personal details is strong.*

Q18. A good password should be:

(a) Long, unique and hard to guess ✓
(b) Your name
(c) Your date of birth
(d) Same for all accounts

Explanation: *Use long passwords/passphrases and a different one for every account.*

Zedking Group Of Institutions

Q19. 2-Step Verification (2FA) means:

(a) Password plus a second proof such as an OTP ✓
(b) Two passwords of the same type
(c) Logging in twice
(d) Two antivirus programs

Explanation: *Two-factor authentication asks for something you know (password) and something you have (OTP/app/phone).*

Q20. Which of the following is a firewall?

(a) A system that monitors and blocks unauthorized network traffic ✓
(b) A heating device
(c) A type of virus
(d) A cable

Explanation: *A firewall filters incoming and outgoing traffic according to security rules.*

Q21. The best way to protect against known software weaknesses is to:

(a) Install updates (patches) regularly ✓
(b) Never switch off the PC
(c) Use pirated software
(d) Disable the antivirus

Explanation: *Updates fix security holes that attackers exploit.*

Q22. Which Windows tool provides built-in antivirus protection?

(a) Windows Security (Microsoft Defender) ✓
(b) Paint
(c) Notepad
(d) Calculator

Explanation: *Windows Security with Microsoft Defender Antivirus is built into Windows 10/11.*

Q23. Which key combination locks a Windows PC quickly?

(a) Windows + L ✓
(b) Windows + D
(c) Alt + F4
(d) Ctrl + P

Explanation: *Win + L locks the screen so that nobody can use the PC without a password.*

Q24. BitLocker is used to:

(a) Encrypt the drive ✓
(b) Print documents
(c) Edit photos
(d) Browse the web

Explanation: *BitLocker/Device Encryption protects data on the drive if the PC is lost or stolen.*

Q25. The 3-2-1 backup rule means:

(a) 3 copies, on 2 types of media, 1 stored off-site ✓
(b) 3 passwords, 2 PINs, 1 OTP
(c) 3 antivirus, 2 firewalls, 1 router
(d) 3 users, 2 PCs, 1 printer

Explanation: *Keep three copies of data, on two different media, with one copy at another place (e.g., cloud).*

Q26. The padlock symbol and https:// in the browser address bar show that:

(a) The connection to the site is encrypted ✓
(b) The site is always genuine and safe
(c) The site is free
(d) The site has no ads

Explanation: *HTTPS encrypts data in transit, but even fake websites can use HTTPS, so also check the site name.*

Q27. Which of these is a sign of a phishing e-mail?

(a) Urgent threat, spelling mistakes and a suspicious link ✓
(b) Message from a known friend about a meeting
(c) Newsletter you subscribed to
(d) Message with your name only

Explanation: *Phishing mails create fear/urgency, ask for personal data and contain suspicious links/attachments.*

Zed King Group Of Institutions

Q28. A browser's Incognito/Private mode:

(a) Does not save history on that device but does not make you invisible on the Internet ✓
(b) Makes you completely anonymous
(c) Blocks all viruses
(d) Speeds up the Internet
Explanation: *Private mode only prevents local storage of history/cookies; websites and the ISP can still see activity.*

Q29. To prevent tracking, a user can:

(a) Block third-party cookies and review site permissions ✓
(b) Share passwords
(c) Disable updates
(d) Click all pop-ups
Explanation: *Cookie and permission settings in the browser help control tracking and data sharing.*

Q30. What should you do on a public computer after using e-mail?

(a) Log out and clear the browsing data ✓
(b) Just close the tab
(c) Save the password
(d) Leave it logged in
Explanation: *Always sign out and do not save passwords on shared computers.*

Q31. The 6-digit code that WhatsApp sends by SMS during registration should be:

(a) Never shared with anyone ✓
(b) Shared with friends
(c) Posted in status
(d) Given to customer care callers
Explanation: *Sharing the code lets a fraudster take over your WhatsApp account.*

Q32. WhatsApp's Two-step verification asks you to set a:

(a) 6-digit PIN ✓
(b) 10-digit PIN
(c) Bank PIN
(d) SIM PIN
Explanation: *The PIN protects your account when it is registered on a new phone.*

Q33. To make an Instagram account visible only to approved followers, set the account to:

(a) Private ✓
(b) Public
(c) Business
(d) Verified
Explanation: *A private account allows only approved followers to see posts.*

Q34. Which of the following improves smartphone security?

(a) Screen lock, updates and apps only from the official store ✓
(b) Installing APK files from unknown links
(c) Rooting the phone
(d) Sharing the PIN
Explanation: *Locks, updates, official stores and careful app permissions keep the phone safe.*

Q35. A lost phone can be located and locked using:

(a) Find My Device (Android) / Find My (iPhone) ✓
(b) Calculator app
(c) Gallery
(d) Clock app
Explanation: *These services can locate, ring, lock or erase a lost phone remotely.*

Q36. Which is a risk of using free public Wi-Fi?

(a) Data can be intercepted ✓
(b) Faster Internet always
(c) No risk at all
(d) Automatic virus removal
Explanation: *Open public Wi-Fi can be monitored by attackers, so avoid banking/passwords there or use a VPN.*

Part B: True or False

#	Statement	Answer
1	Confidentiality, Integrity and Availability are the three goals of cyber security.	True

Zedking Group Of Institutions

#	Statement	Answer
2	A firewall is used to cook food in a computer lab.	False — it filters network traffic and blocks unauthorized access.
3	Antivirus software need not be updated once installed.	False — it must be updated regularly to detect new threats.
4	Using the same password for all accounts is safe.	False — if one account leaks, all accounts are at risk.
5	Banks and companies never ask for your OTP or PIN on phone calls.	True
6	The padlock symbol in the browser guarantees that a website is genuine.	False — it only shows the connection is encrypted; fake sites can also use https.
7	Incognito mode makes a user completely anonymous.	False — it only stops saving history on that device.
8	Two-factor authentication gives extra protection to an account.	True
9	Apps should be installed from official stores only.	True
10	A WhatsApp 6-digit SMS code can be shared with a friend who asks for it.	False — sharing it can let someone take over your account.

Part C: Short Answer Questions

Q1. What is cyber security? Why is it needed?

Ans: Cyber security is protecting computers, networks, data and accounts from cyber attacks. It is needed to protect personal and financial data, privacy, money, businesses and digital services.

Q2. Explain the goals of cyber security (CIA triad).

Ans: Confidentiality — only authorized people can see data; Integrity — data stays accurate and unchanged; Availability — data and services are accessible when needed.

Q3. What is malware? Name its types.

Ans: Malware is malicious software designed to harm a system. Types: virus, worm, trojan horse, ransomware, spyware, adware.

Q4. What is phishing? How can it be avoided?

Ans: Phishing is a fraud using fake e-mails, SMS or websites to steal passwords or bank details. Avoid by not clicking unknown links, checking the sender and website address, and never sharing OTP/PIN.

Q5. Differentiate between a virus and a worm.

Ans: A virus attaches to a file and spreads when the file is run; a worm spreads on its own through networks without user action.

Q6. What is ransomware?

Ans: Ransomware is malware that locks or encrypts the user's files and demands money to unlock them. Regular backup is the best protection.

Q7. What is a firewall? What is its use?

Ans: A firewall is hardware or software that monitors network traffic and blocks unauthorized access according to security rules.

Q8. What is two-factor authentication? Why is it important?

Ans: 2FA asks for a second proof (OTP, authenticator app, fingerprint) along with the password. It protects the account even if the password is stolen.

Q9. Write any five steps to secure a PC.

Ans: Update Windows and software; keep antivirus and firewall ON; use strong passwords and lock the screen; install only genuine software and scan pen drives; take regular backups; use BitLocker.

Q10. What is a strong password? Give rules.

Ans: A strong password is long (12+ characters), has letters, numbers and symbols, is not related to personal information and is different for each account.

Q11. What is the 3-2-1 backup rule?

Ans: Keep 3 copies of data, on 2 different types of storage media, with 1 copy stored at another place such as the cloud.

Zedking Group Of Institutions

Q12. Write the steps to run a virus scan in Windows.

Ans: Settings → Privacy & security → Windows Security → Virus & threat protection → Quick scan (or Scan options → Full scan).

Q13. How can a browser be secured? Write any five steps.

Ans: Update the browser; check https/padlock; enable Safe Browsing; block pop-ups and third-party cookies; clear browsing data; avoid saving passwords on shared PCs; use trusted extensions only.

Q14. What is Incognito (Private) mode? What are its limits?

Ans: It opens a window that does not save history, cookies or form data on that device. It does not hide activity from websites, employer or ISP, nor protect from viruses.

Q15. How to recognize a fake website?

Ans: Spelling mistakes in the address, no https or browser warnings, strange domain endings, requests for OTP/PIN/card details, too-good-to-be-true offers and urgent threats.

Q16. How can an e-mail account be secured?

Ans: Use a strong unique password, turn on 2-step verification, keep recovery details updated, avoid unknown links and attachments, check account activity and log out on shared devices.

Q17. Write the steps to secure a WhatsApp account.

Ans: Never share the 6-digit code; turn on Two-step verification PIN (Settings → Account); set privacy for profile and groups; check Linked devices; use chat lock; avoid unknown links and modified apps.

Q18. How can Facebook and Instagram accounts be made safe?

Ans: Turn on two-factor authentication in Accounts Center, use login alerts, run Privacy Checkup, make Instagram account Private, review logged-in devices and linked apps, and accept only known friends.

Q19. Write any five ways to secure a smartphone.

Ans: Set screen lock; update OS and apps; install apps only from official stores; check app permissions; enable Find My Device; avoid public Wi-Fi/USB charging; don't install remote-access apps.

Q20. What should be done if a smartphone is lost? / Where to report a cyber fraud?

Ans: Locate/lock/erase with Find My Device, block SIM and bank accounts, change passwords, file a police complaint and block the phone through Sanchar Saathi. Report cyber fraud on 1930 and cybercrime.gov.in.

Part D: Long Answer Questions (Practice)

- What is cyber security? Explain its need and goals with the CIA triad.
- Explain the common cyber threats and attacks. What are the cyber laws and reporting methods in India?
- Explain the steps to secure a PC.
- Explain how to secure a web browser and how to recognize a fake website.
- Explain how to secure e-mail and social media accounts such as Facebook, Instagram and WhatsApp.
- Explain the steps to secure a smartphone and what to do if it is lost or stolen.
- Write the do's and don'ts of safe digital behaviour.

Best of Luck for Your Exam!

Zed King Institute, Kaithal | Overview of Cyber Security

Zedking Group Of Institutions