Zed-King
GROUP OF INSTITUTIONS
ISO 9001 : 2015 Certified

EXPERT COMPUTER COURSE

CYBER SECURITY

Topics Covered:

1. 8.1 Introduction to Cyber Security
2. 8.2 Basic Concepts of Threats (Vulnerabilities, Controls, Risk, Cyber Crime)
3. 8.3 Cyber Security Goals - CIA Triad
4. 8.4 Security Policies
5. 8.5 Security Mechanisms
6. 8.6 Data Security & Safe Browsing
7. 8.7 Security Considerations - Viruses, Worms, Trojans, Spyware, Malware (ALL Types)
8. 8.8 Netiquettes
9. 8.9 Phishing Awareness
10. 8.10 Software Licensing - All Types
11. 8.11 IT Act 2000 - Important Sections

8.1 Introduction to Cyber Security

Cyber Security means protecting computers, networks, programs and data from digital attacks, damage or unauthorized access.

In simple words: Just like we lock our house to keep thieves out, we use Cyber Security to keep hackers and bad people away from our computers and information.

Why is Cyber Security Important?

- Our personal data (photos, bank info, passwords) is stored online
- Businesses store important customer data digitally
- Hackers and cybercriminals are always trying to steal or damage this data
- Without cyber security, anyone could access your private information

Example: Real Life
When you use online banking, Cyber Security keeps your money safe from hackers who try to steal your password.

Hindi Tip	**Cyber Security matlab - computer aur internet ko hackers aur bure logon se bachana, jaise ghar mein lock lagana.**

8.2 Basic Concepts of Threats

There are 4 important concepts you must understand:

1. Vulnerability

A vulnerability is a weakness or gap in a computer system that can be exploited (used) by attackers.

- It is like a crack in a wall - the crack itself does not hurt you, but someone can break through it
- Example: An old software that has not been updated is a vulnerability
- Example: Using a weak password like '123456' is a vulnerability

Example: Simple Example
A website that stores passwords without encryption (plain text) has a vulnerability. A hacker can easily read all passwords if they get in.

Hindi Tip	**Vulnerability matlab system ki kamzori - jaise purana lock jo asaani se toot jaye.**

2. Controls

Controls are the safety measures we put in place to reduce or remove vulnerabilities.

- Think of controls as the solutions to vulnerabilities
- There are 3 types of controls:
  - Preventive Controls - Stop attacks before they happen (e.g., antivirus software, strong passwords)
  - Detective Controls - Find out if an attack is happening (e.g., security alerts, logs)
  - Corrective Controls - Fix damage after an attack (e.g., restoring backup data)

Example: Example
Installing antivirus software is a Preventive Control. It stops viruses before they infect your computer.

Zedking Group Of Institutions

Hindi Tip	**Controls matlab wo upay jo hum system ko surakshit rakhne ke liye karte hain - jaise antivirus lagana ya strong password banana.**

3. Risk

Risk = the chance (probability) that a threat will use a vulnerability and cause harm.

- Risk cannot be completely removed, but it can be reduced
- Formula to remember: Risk = Threat x Vulnerability
- High risk = When there are many threats AND many weaknesses in the system
- Low risk = When controls are strong and weaknesses are fixed

Example: Example
If you use public WiFi (vulnerability) and a hacker is nearby trying to steal data (threat), there is HIGH RISK of your information being stolen.

Hindi Tip	**Risk matlab khataraa - agar aapka system kamzor hai aur hacker aa jaye, toh nuksaan hone ka darr hai, isi ko Risk kehte hain.**

4. Cyber Crime

Cyber Crime means any illegal activity done using a computer or the internet.

- Hacking someone's account without permission
- Stealing credit card information online
- Spreading viruses to destroy data
- Online fraud and cheating
- Cyberbullying - harassing someone online
- Identity theft - stealing someone's personal information to pretend to be them

Example: Example
A person sends you a fake email pretending to be your bank, asking for your password. When you give it, they steal your money. This is Cyber Crime (Phishing).

Hindi Tip	**Cyber Crime matlab computer ya internet ka use karke koi bhi galat kaam karna - jaise kisi ka account hack karna ya online dhokha dena.**

8.3 Cyber Security Goals (CIA Triad)

There are 3 main goals of Cyber Security, known as the CIA Triad:

GOAL	MEANING	EXAMPLE
C - Confidentiality	Only authorized people can access the data. Your private info stays private.	Your email password - only you should know it, not your friend.
I - Integrity	Data should not be changed or tampered by unauthorized people. Data must remain accurate.	A bank transfer of Rs. 1000 should arrive as Rs. 1000, not changed to Rs. 100 by a hacker.
A - Availability	Data and systems should be available (working) when authorized users need them.	A hospital's patient records must always be available to doctors - system should not crash.

Hindi Tip	**CIA Triad = C (Data sirf sahi insaan dekhe), I (Data badla na jaye), A (System hamesha kaam karta rahe) - yahi teen kaam karta hai Cyber Security.**

8.4 Security Policies

A Security Policy is a set of rules and guidelines that define how an organization protects its computer systems and data.

Think of it as: A set of rules everyone must follow to keep the office/school computers safe.

What does a Security Policy include?

- Who can access which data (Access Control rules)
- Password rules - how long, how complex passwords should be
- Rules about using internet at workplace
- What to do if there is a security breach (attack)
- Rules about installing software
- Data backup rules - how often to take backup

Example: Example
A company policy says: All employees must change their password every 30 days and must not share passwords with anyone. This is a Security Policy.

Hindi Tip	**Security Policy matlab wo niyam jo kisi office ya school mein computer use karne ke liye banaye jaate hain - jaise password baar baar badalna compulsory ho.**

8.5 Security Mechanisms

Security Mechanisms are the actual tools and techniques used to enforce security policies.

1. Encryption

Converting data into a secret code so that only authorized people can read it.

> **Example: Example**
> When you send a WhatsApp message, it is encrypted. Even WhatsApp itself cannot read your messages - only you and the receiver can.

2. Authentication

Verifying the identity of a user before giving access.

- Password-based authentication - enter correct password
- OTP (One Time Password) - code sent to your phone
- Biometric - fingerprint or face recognition
- Two-Factor Authentication (2FA) - password + OTP together

3. Firewall

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on rules.

> **Example: Example**
> A firewall is like a security guard at the gate - it checks who is coming in and only lets authorized people through.

4. Antivirus Software

Software that detects and removes viruses, malware, and other threats from your computer.

- Examples: Quick Heal, Norton, McAfee, Kaspersky, Windows Defender

5. Digital Signature

A digital signature verifies that a document or message came from a specific person and was not changed.

> **Example: Example**

Zedking Group Of Institutions

Just like you sign a cheque to prove it is from you, a Digital Signature proves that an online document is genuine.

Hindi Tip	**Security Mechanisms matlab wo asli tools aur tarike jo system ki suraksha karte hain - jaise antivirus, firewall, aur password.**

8.6 Data Security

Data Security means protecting digital data from unauthorized access, corruption, or theft throughout its entire life.

8.6.1 Creating Strong Passwords

A strong password is your first line of defense against hackers.

Rules for a Strong Password:

- Minimum 8 characters long (12 or more is better)
- Use UPPERCASE letters (A-Z)
- Use lowercase letters (a-z)
- Use Numbers (0-9)
- Use Special characters (!@#$%^&*)
- Do NOT use your name, birthday, or simple words
- Use different passwords for different accounts
- Change passwords regularly

WEAK Password (AVOID)	STRONG Password (USE)
123456 password Rahul1990 iloveyou	R@hul#9820! Tr$ee7&Sky! P@ssw0rd#99 C0mputer@2024!

Hindi Tip	**Strong password matlab aisa password jo guess karna mushkil ho - chota nam, janmadin ya simple number mat rakhna, hamesha mix karo letters, numbers aur special characters.**

8.6.2 How to Stay Safe When Surfing the Internet

The internet can be dangerous if we are not careful. Here are ways to stay safe:

8.6.2.1 In Private Browsing (Incognito Mode)

Private/Incognito mode is a browser feature that does not save your browsing history, cookies, or form data on your computer.

- Your history is automatically deleted when you close the window
- Other people using the same computer cannot see what you browsed
- How to open: Chrome - Ctrl + Shift + N | Firefox - Ctrl + Shift + P

IMPORTANT NOTE	Incognito mode does NOT make you completely invisible on the internet. Your Internet Service Provider (ISP) and the websites you visit can still see your activity. It only hides from other people on the same device.

Hindi Tip	**Incognito mode matlab browsing history save nahi hogi us computer mein - lekin ISP aur website ko pata chal sakta hai, sirf same device wale nahi dekh sakte.**

8.6.2.2 Identify Secure Websites

Before entering any personal information on a website, check if it is secure.

Signs of a SECURE website:

- URL starts with HTTPS (not just HTTP) - the 'S' stands for Secure
- A padlock icon appears in the address bar
- The website has a valid SSL Certificate

Signs of an UNSAFE website:

- URL starts with only HTTP (no S)
- No padlock icon
- Browser shows a warning like 'Not Secure' or 'Your connection is not private'

Example: Example
https://www.sbi.co.in is secure (HTTPS + padlock). Never do banking on a website with only HTTP.

Hindi Tip	**Safe website ki pehchaan: URL mein HTTPS ho aur address bar mein tala (padlock) ka nishan ho - agar sirf HTTP hai toh us site par koi personal info mat do.**

8.6.2.3 Clear Cookies and Cache

Cookies are small files that websites store on your computer to remember your information (like login details, preferences).

Cache is temporary storage of website data on your computer to make pages load faster.

Why should you clear them?

- Cookies can be stolen by hackers to fake your login (called session hijacking)
- Old cached data can cause websites to not load properly
- Clearing cookies removes saved passwords and auto-fill data - keeps you safer

How to clear in Chrome:

- Press Ctrl + Shift + Delete
- Select time range (All time for complete clear)
- Check Cookies and Cache boxes
- Click Clear Data

Hindi Tip	**Cookies aur Cache clear karna matlab browser ki purani yaadaasht saaf karna - isse hackers aapki save info nahi chura sakte.**

8.7 Security Considerations

This section covers the different types of threats and dangers that can harm your computer.

8.7.1 Computer Security

Computer Security means protecting computer systems from theft, damage, and unauthorized access.

Types of Computer Security:

- Physical Security - Protecting the actual hardware (locks, CCTV cameras)
- Network Security - Protecting data traveling over networks (firewalls, encryption)
- Software Security - Protecting programs from bugs and attacks (antivirus, updates)
- Data Security - Protecting stored data from loss or theft (passwords, backups)

Hindi Tip	**Computer Security matlab sirf antivirus nahi - hardware, network, software aur data sabko alag alag tarike se surakshit rakhna padta hai.**

8.7.2 Viruses (Types of Virus)

A computer virus is a malicious program that copies itself and spreads from one computer to another, damaging files and the system.

Zedking Group Of Institutions

Just like a biological virus infects humans, a computer virus infects computers and spreads!

How viruses spread:

- Through infected USB drives / pen drives
- Downloading files from unknown websites
- Opening suspicious email attachments
- Visiting malicious websites

ALL Types of Computer Viruses:

Virus Type	What it does	Example
Boot Sector Virus	Attacks the boot sector (starting part) of a hard disk. It runs automatically when the computer starts. Very dangerous as it loads before OS.	*Stoned, Michelangelo, Disk Killer*
File Infector Virus	Attaches itself to executable program files (.exe, .com, .bat). Spreads whenever the infected file is run.	*Jerusalem, Cascade, Vienna*
Macro Virus	Hides inside document files like MS Word or Excel files. Activates when document is opened. Very common in offices.	*Melissa, Concept, DMV*
Polymorphic Virus	Changes its own code/signature every time it copies itself, making it very hard for antivirus to detect.	*Storm Worm, Virut, Marburg*
Stealth Virus	Hides itself from the operating system and antivirus programs. It tricks the OS into showing clean files.	*Brain, Frodo, Number of the Beast*
Resident Virus	Permanently installs itself in the computer's RAM (memory). Infects all files and programs that are run or opened.	*CMJ, Meve, MrKlunky*
Non-Resident Virus	Does NOT stay in memory. It searches for host files, infects them, and moves on. Harder to detect.	*Vienna, Cascade*
Multipartite Virus	Attacks both the boot sector AND program files at the same time. Spreads very fast and is difficult to remove.	*Invader, Flip, Tequila*
Web Scripting Virus	Spreads through malicious websites and web scripts (JavaScript, HTML). Activates when you visit an infected website.	*JS/Redirector, Ramnit*
Network Virus	Spreads rapidly through computer networks (LAN, internet). Targets network shares and connected devices.	*Nimda, SQLSlammer*

Overwrite Virus	Deletes or overwrites the original content of infected files completely. The original file data is permanently lost.	*Way, Trj.Reboot, Trivial.88.D*
Sparse Infector Virus	Infects files only occasionally (e.g., every 10th file) to avoid detection by antivirus programs.	*Various sparse variants*
Spacefiller / Cavity Virus	Fills in the empty (unused) spaces inside program files without increasing the file size, making detection very hard.	*Lehigh virus*
FAT Virus	Attacks the File Allocation Table (FAT) - the part of disk that stores information about where files are saved. Can make files inaccessible.	*Link virus*
Directory Virus	Changes directory paths of files so they point to the virus code instead of the actual file.	*Dir-2 virus*

How to protect yourself from Viruses:

- Install and update antivirus software regularly
- Do not open suspicious emails or attachments
- Scan USB drives before opening
- Keep your operating system updated
- Download software only from official websites

Hindi Tip	**Computer Virus matlab ek chhupa hua nuksandeh program jo ek file se doosri file mein failta rehta hai - antivirus lagao, USB scan karo, aur anjaan files mat kholo.**

8.7.3 Computer Worm

A Computer Worm is a type of malware that copies itself and spreads across networks WITHOUT needing to attach to a file or program.

KEY DIFFERENCE	Virus needs a host file to spread. Worm spreads on its own through networks - no host needed!

How Worms are Dangerous:

- They consume network bandwidth and slow down the internet
- They can delete files or install other malware
- They can spread to thousands of computers very quickly
- They can open backdoors for hackers to enter your system

Example: Famous Example
ILOVEYOU Worm (2000) - Spread through email with subject 'I Love You'. When opened, it deleted files and sent itself to all contacts. It infected 50 million computers worldwide!

Example: Another Example
WannaCry Worm (2017) - A ransomware worm that spread across networks and locked files, demanding money to unlock them. It affected hospitals and banks in many countries.

Hindi Tip	**Worm ek aisa virus jaisa khatara hai jo khud hi network mein failta rehta hai bina kisi file ka sahara liye - internet se aapke pure system mein ghus sakta hai.**

8.7.4 Trojan Horses

A Trojan Horse (or Trojan) is malware that disguises itself as a legitimate, useful program but actually performs harmful actions.

The name comes from the ancient Greek story of the Trojan Horse - Greek soldiers hid inside a giant wooden horse gifted to Troy, then came out at night to attack.

How a Trojan Works:

- Step 1: You download what looks like a useful free app or game
- Step 2: The app installs and works normally (so you don't suspect anything)
- Step 3: Secretly, the Trojan runs in the background doing harmful things
- Step 4: It can steal data, give hackers remote access, or damage files

Types of Trojans:

- Remote Access Trojan (RAT) - Gives hacker complete control of your computer
- Banking Trojan - Steals your online banking credentials
- Downloader Trojan - Downloads other malware onto your system
- Spy Trojan - Records your keystrokes and sends to hacker

Example: Example
You download a free game from an unknown website. The game works fine, but secretly a Trojan inside it records your passwords and sends them to a hacker. This is a Trojan Horse attack!

KEY DIFFERENCE	Unlike viruses and worms, Trojans do NOT copy themselves. They need YOU to download and install them by tricking you.

Hindi Tip	**Trojan matlab dhoka - ek useful app ya game ki tarah dikhta hai lekin andar se chor hota hai jo aapka data chura leta hai.**

8.7.5 Spyware

Spyware is software that secretly monitors your computer activity and collects personal information without your knowledge or consent.

What Spyware does:

- Tracks which websites you visit
- Records your keystrokes (called Keylogging) - captures passwords you type
- Takes screenshots of your screen
- Steals credit card numbers and banking info
- Sends all collected information to the hacker

How Spyware gets into your computer:

- Bundled with free software downloads
- Through malicious email attachments
- By visiting infected websites
- Through fake software updates

Example: Example
You install a free PDF converter from an unknown site. Along with it, spyware is installed that records every password you type and sends it to a criminal. You never know it is happening!

How to protect yourself from Spyware:

- Use reputable antivirus/anti-spyware software
- Only download software from official websites
- Keep your browser and OS updated
- Be careful about what permissions you give to apps

Hindi Tip	**Spyware matlab jasoosi software - aapki jaankari ke bina aapki sab activity dekhta rehta hai aur passwords chura leta hai, bilkul chhupe jasoos ki tarah.**

8.7.6 Malware and Malware Types

Malware = Malicious Software. It is an umbrella term for any software designed to harm, disrupt, or gain unauthorized access to computer systems.

Viruses, Worms, Trojans, and Spyware are ALL types of Malware.

Complete List of Malware Types:

Malware Type	Description	Real Example

Virus	Attaches to files, copies itself, spreads when infected file runs	Melissa, CIH virus
Worm	Spreads through networks on its own without a host file	WannaCry, ILOVEYOU
Trojan	Disguises as useful software but is harmful	Zeus, Emotet
Spyware	Secretly monitors and steals your information	FinFisher, DarkHotel
Ransomware	Locks/encrypts your files and demands money to unlock them	WannaCry, Petya
Adware	Shows unwanted ads and can redirect your browser	Superfish, Fireball
Rootkit	Hides deep in the OS giving hackers admin-level access	TDSS, ZeroAccess
Keylogger	Records every key you press (captures passwords)	Ardamax, Refog
Botnet	Takes control of many computers to launch attacks together	Mirai, Zeus Botnet

Hindi Tip	**Malware ek bada group hai jisme virus, worm, trojan, spyware sab aate hain - ye sab alag alag tarike se computer ko nuksaan pohunchate hain.**

8.8 Netiquettes

Netiquette = Network + Etiquette. It means the code of polite behavior and good manners while using the internet.

Just like we have manners in real life (saying please/thank you), we must have good manners online too!

Important Netiquettes to Follow:

- **Do NOT write in ALL CAPS - It means shouting online and is considered rude**
- Be respectful and polite in emails, chats, and comments
- Do not share private information of others without permission
- Do not spread rumors or fake news online
- Give credit when you use someone else's work (images, articles, etc.)
- Do not use rude or abusive language in online discussions
- Reply to emails and messages in a reasonable time
- Do not send spam (unwanted bulk messages)

- Keep emails short and to the point
- Proofread before sending - check for spelling and grammar errors
- Do not cyberbully - bullying someone online is harmful and illegal
- Respect others' privacy - do not share their personal details

Example: Example of Good Netiquette
When someone asks a question in an online group, answer politely. Don't make fun of them for not knowing something. Remember: online behavior affects real people with real feelings.

Hindi Tip	**Netiquette matlab internet par bhi tameez se rehna - jaise real life mein seedha bolna zaroori hai waise hi online bhi seedha, izzatdar aur saaf baat karo.**

8.9 Security Considerations - Phishing

Be aware of the possibility of receiving fraudulent and unsolicited emails!

8.9.1 Phishing

Phishing is a type of cyber attack where criminals send fake emails or messages pretending to be from trusted sources (banks, companies, government) to trick you into giving your personal information.

The word comes from 'fishing' - just like a fisherman uses bait to catch fish, hackers use fake messages as bait to catch victims.

What hackers want from you in Phishing:

- Bank account details and passwords
- Credit/Debit card numbers and CVV
- OTP (One Time Password)
- Social media login credentials
- Personal ID information (Aadhar, PAN)

Example: Classic Phishing Example
You receive an email: 'Dear Customer, Your SBI account has been suspended. Click here to verify your details immediately: www.sbi-secure-login.com' - This is PHISHING! SBI's real website is sbi.co.in. The fake link tricks you into entering your password.

Zedking Group Of Institutions

Hindi Tip	**Phishing matlab koi aapko bank ya company banakar email karta hai aur password maangta hai - yaad rakho koi bhi asli bank kabhi password ya OTP nahi maangta!**

8.9.2 How to Recognize Phishing Attempts

How to spot a Phishing email or message:

- **The email comes from a suspicious address (e.g., sbi.support@gmail.com instead of @sbi.co.in)**
- Creates urgency - 'Act immediately!' or 'Your account will be blocked in 24 hours!'
- Contains spelling mistakes and grammatical errors
- Asks for sensitive info like password, OTP, CVV via email
- Contains suspicious links - hover over link to see the real URL before clicking
- Generic greeting like 'Dear Customer' instead of your name
- Attachments you did not expect

Golden Rules to Avoid Phishing:

- **NEVER share OTP, password, or CVV with anyone - banks never ask for these!**
- Always verify the sender's email address carefully
- Type the URL directly in browser instead of clicking email links
- When in doubt, call the organization directly on their official number
- Use email filters to block phishing emails

REMEMBER THIS	No bank, government office, or legitimate company will EVER ask for your password or OTP through email, call, or message!

Hindi Tip	**Phishing email ko pehchano: galat spelling, urgent tone, aur password/OTP maangna - agar koi bhi aisa maange toh turant ignore karo aur report karo.**

8.10 Basics of Software Licensing

Software License = A legal agreement that defines how you can use a software program.

When you buy or download software, you don't actually own the software - you buy a LICENSE to use it under certain conditions.

Types of Software Licenses:

Zedking Group of Institutions

1. Proprietary/Commercial License

You must pay to use it. You cannot copy, modify, or share it freely.

- Examples: Microsoft Office, Adobe Photoshop, Windows OS
- Using it without buying is illegal (called piracy)

2. Freeware

Free to download and use, but you cannot modify the source code.

- Examples: Adobe Acrobat Reader, Google Chrome, VLC Media Player
- Free for use but not open source

3. Shareware

Software given for a trial period. After trial, you must pay to continue using.

- You can try before buying
- Examples: WinRAR (keeps asking you to buy after trial), many games

4. Open Source License

Source code is freely available. Anyone can use, modify, and distribute it.

- Examples: Linux, Mozilla Firefox, LibreOffice, VLC, Android (AOSP)
- Usually free to use

5. Free Software (GNU/GPL)

Software that gives users the freedom to run, copy, distribute, study, change, and improve it.

- GNU GPL (General Public License) is the most common
- Examples: Linux kernel, WordPress, MySQL

6. Site License

One license that allows installation on multiple computers in one location (like a school or office).

- Cost-effective for organizations
- Example: A school buys one MS Office Site License for all 100 computers

7. OEM License

Software that comes pre-installed with a new device. It is tied to that specific device.

- Example: Windows that comes pre-installed when you buy a new laptop

Zedking Group Of Institutions

- You cannot transfer this license to another computer

Hindi Tip	**Software License matlab software use karne ka kanuni adhikar - paid software ki copy karna piracy hai aur illegal hai, jabki open source free mein sabka hota hai.**

8.11 IT Act 2000

The Information Technology Act 2000 (IT Act) is a law passed by the Government of India to handle cyber crimes and provide legal recognition to electronic transactions.

Why was it made?

- To legally recognize e-commerce and digital transactions
- To prevent and punish cyber crimes
- To give legal status to digital signatures
- To protect sensitive personal data online

Key Provisions (Important Sections):

Section	What it covers	Punishment
Section 43	Unauthorized access or damage to computer/network	Compensation up to Rs. 1 Crore
Section 65	Tampering with computer source code	Up to 3 years jail or fine up to Rs. 2 Lakh
Section 66	Hacking - unauthorized access to computer system	Up to 3 years jail or fine up to Rs. 5 Lakh
Section 66C	Identity theft - using someone else's password or ID	Up to 3 years jail and fine up to Rs. 1 Lakh
Section 66D	Cheating using computer/internet	Up to 3 years jail and fine up to Rs. 1 Lakh
Section 66E	Violation of privacy - publishing private images	Up to 3 years jail or fine up to Rs. 2 Lakh
Section 67	Publishing obscene material online	Up to 5 years jail and fine up to Rs. 10 Lakh
Section 69	Govt can intercept/monitor info for national security	Non-compliance: up to 7 years jail

IT Act 2000 was later amended (updated) in 2008 to include more cyber crimes like phishing, cyber terrorism, and data theft.

Hindi Tip	IT Act 2000 matlab India ka cyber law - agar internet ya computer se koi bhi galat kaam karo toh jail aur juraane ka provision hai, isliye online sahi kaam karo.

QUICK REVISION - Most Important Points

EXAM READY: KEY DEFINITIONS TO REMEMBER
Cyber Security: Protection of computers, networks, and data from digital attacks
Vulnerability: A weakness in a system that can be exploited
Risk: Probability that a threat will exploit a vulnerability and cause harm
Virus: Malware that attaches to files and spreads when files are run
Worm: Malware that spreads on its own through networks without a host file
Trojan: Malware disguised as useful software to trick users
Spyware: Software that secretly monitors and steals your information
Ransomware: Malware that locks files and demands money to unlock them
Phishing: Fake emails/messages to trick you into giving personal info
Firewall: Security system that monitors and controls network traffic
Encryption: Converting data into a secret code for security
CIA Triad: Confidentiality + Integrity + Availability - 3 goals of Cyber Security
Netiquette: Code of polite behavior while using the internet
IT Act 2000: Indian law to handle cyber crimes and recognize digital transactions
Freeware: Free software but cannot modify source code (e.g., Chrome)
Open Source: Free software with modifiable source code (e.g., Linux)

KEY DIFFERENCES (Exam Favorite!)

Feature	Virus	Worm	Trojan
Self-replicating?	Yes	Yes	No

Needs host file?	Yes	No	No
Spreads via network?	Sometimes	Yes (main way)	No
Disguises itself?	No	No	Yes
User interaction needed?	Yes (run file)	No	Yes (install it)
Harms system?	Yes	Slows/damages	Yes (backdoor)

Best of Luck for Your Exam!

Zed King Institute, Kaithal | Networking & Troubleshooting

Zedking Group Of Institutions