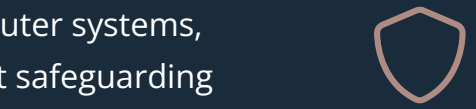
Cyber Security: Safeguarding the Digital Frontier

Presented by Shivanshu Tripathi
Computer Science and Engineering, PSIT, Kanpur

What is Cybersecurity & Its Importance?

Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks. It's about safeguarding your information and privacy in an increasingly connected world.

In our modern digital landscape, where **AI, IoT devices, mobile banking**, and **cloud services** are everywhere, cybersecurity is no longer optional—it's essential.



Protection

Defending against threats

Data Integrity

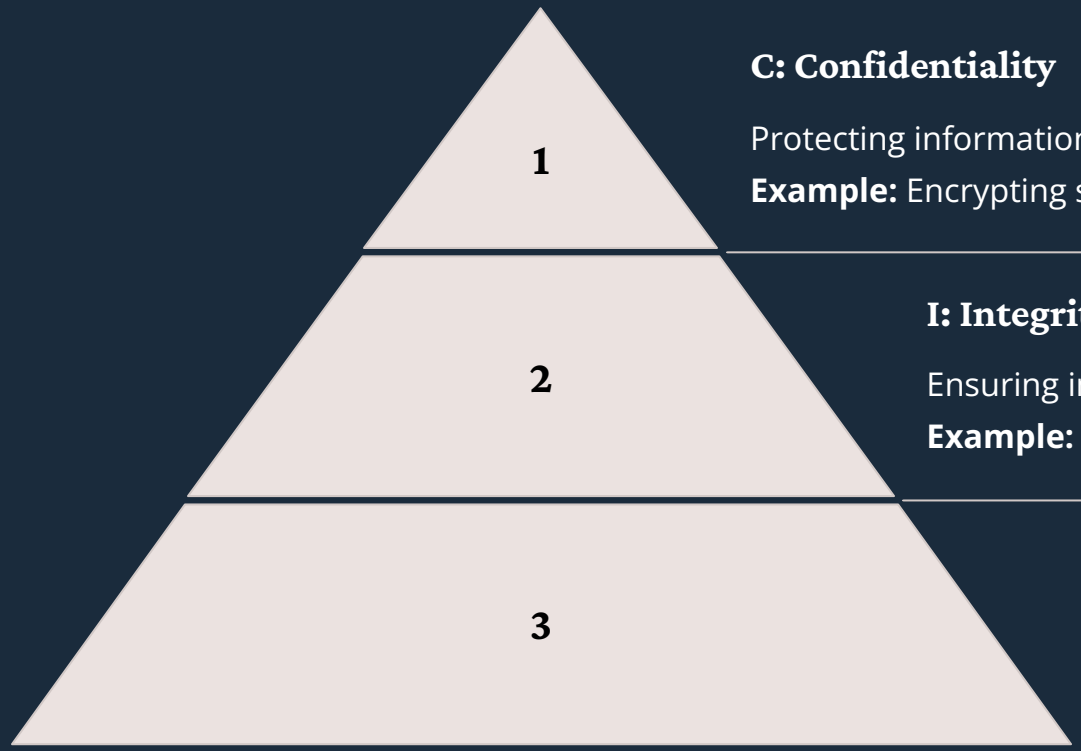
Ensuring data is accurate

Global Security

Securing interconnected systems

The CIA Triad: Core Principles of Cybersecurity

The CIA Triad is a fundamental model for security, guiding policies for information security within an organization.



C: Confidentiality

Protecting information from unauthorized access.
Example: Encrypting sensitive files or using strong passwords.

I: Integrity

Ensuring information is accurate and hasn't been tampered with.
Example: Digital signatures for documents or data backups.

A: Availability

Ensuring information and systems are accessible when needed.
Example: Redundant systems and disaster recovery plans.

Malware Unveiled: Virus, Worm, & Trojan Horse

Understanding different types of malware is crucial for defense. While often confused, they have distinct behaviors.

Type	How it Spreads	Behavior
Virus	Attaches to legitimate programs; requires user action to spread.	Infects files, corrupts data, can delete files. **Example:** USB virus infecting documents.
Worm	Self-replicating; spreads independently across networks.	Consumes bandwidth, can carry payloads. **Example:** Email worm sending itself to your contacts.
Trojan Horse	Disguises as legitimate software; tricks users into installing it.	Creates backdoors, steals data, takes control. **Example:** A fake software installer that looks genuine.

Phishing: Hooking Your Digital Identity

Phishing is a cybercrime where attackers trick individuals into revealing sensitive information, often through deceptive emails or websites.

The Fake Login Page

Attackers create websites that mimic legitimate ones (e.g., banking, social media) to steal your credentials. Always check the URL!

The Deceptive Job Offer

Beware of unsolicited job offers or urgent requests. They often contain malicious links designed to compromise your device or steal personal data.

Ethical Hacking vs. Malicious Hacking

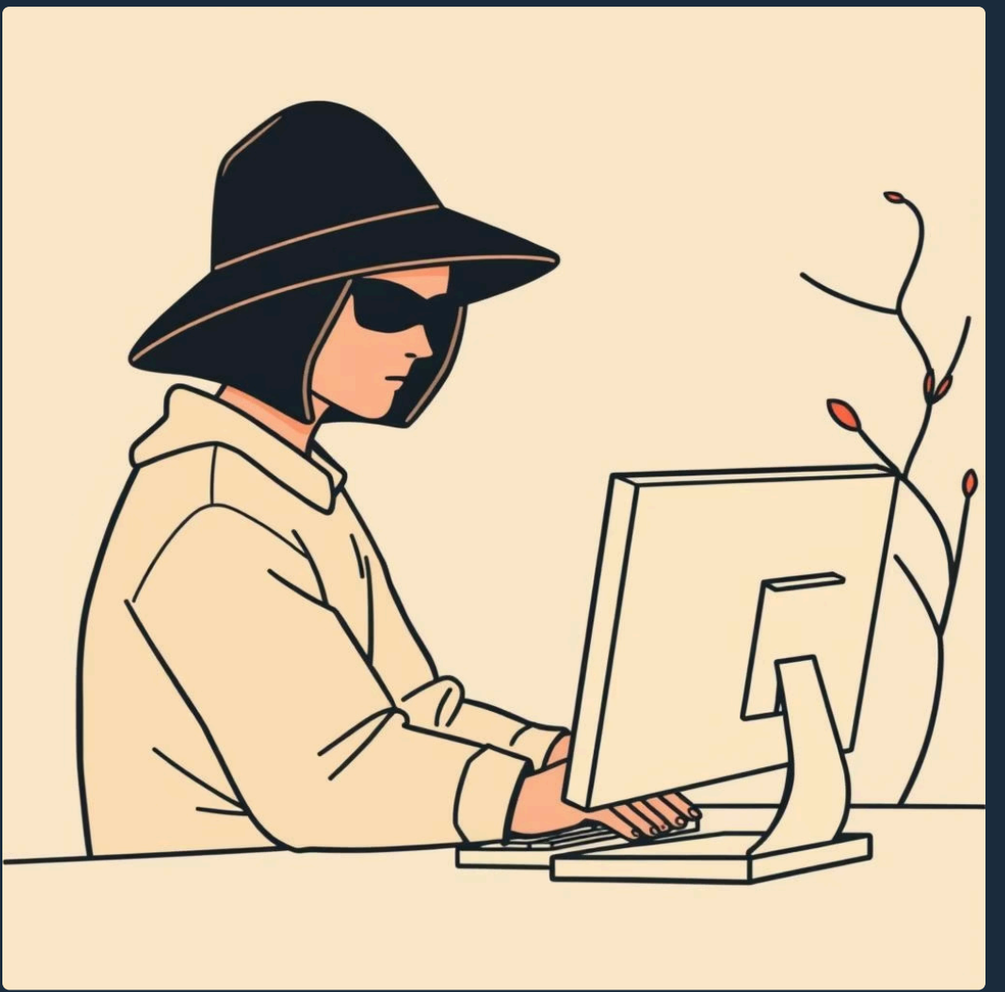
While both involve exploiting vulnerabilities, their intent and purpose are worlds apart.

Ethical Hacking (White Hat)

Definition: Legally breaking into systems with permission to find security vulnerabilities and fix them before malicious hackers can exploit them.

Purpose: Improve security, protect data, and maintain system integrity. They are security professionals.

Tools: Metasploit, Nmap, Wireshark are often used for penetration testing and vulnerability assessment.



Malicious Hacking (Black Hat)

Definition: Illegally breaking into systems without permission for personal gain, disruption, or malicious intent.

Purpose: Steal data, disrupt services, financial fraud, or cause damage. Their actions are criminal.

Consequences: Can lead to severe legal penalties, data breaches, and reputational damage for organizations.

5 Common Cyber-Attacks to Watch Out For

Cyber threats are diverse. Here are some of the most prevalent attack types.

1. **Ransomware**

   Encrypts data, demanding payment (ransom) for its release.

2. **DDoS (Distributed Denial-of-Service)**

   Overwhelms a server with traffic to make a service unavailable.

3. **SQL Injection**

   Injects malicious SQL queries into input fields to manipulate a database.

4. **Brute Force Attack**

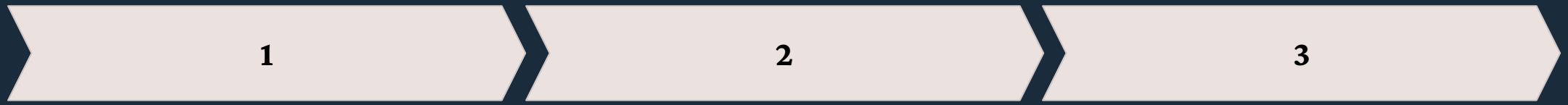
   Tries many combinations of usernames/passwords until access is gained.

5. **Man-in-the-Middle (MITM)**

   Attacker intercepts communication between two parties without their knowledge.

Enhancing Security with Two-Factor Authentication (2FA)

2FA adds an extra layer of security beyond just a password, making it much harder for unauthorized users to access your accounts.



Step 1: Something You Know

This is your password—the first factor of authentication.

Step 2: Something You Have/Are

A second verification, like an OTP sent to your phone, a biometric scan (fingerprint), or a hardware token.

Secure Access

Only after both factors are successfully verified is access granted. This significantly reduces the risk of account compromise.

Examples: Password + SMS OTP, Biometric + PIN, Password + Authenticator App Code. Always enable 2FA where available!

Case Study: AIIMS Delhi Ransomware Attack (2022)

What Happened?

In November 2022, the All India Institute of Medical Sciences (AIIMS) in Delhi suffered a massive ransomware attack, crippling its digital services.

Impact:

- Patient data compromised and encrypted.
- Online appointments, billing, and lab services disrupted.
- Manual operations for emergency services.

Consequences:

- Significant operational disruption for weeks.
- Loss of patient trust and privacy concerns.
- Highlighting vulnerabilities in critical infrastructure.

Your Personal Cybersecurity Guide & Firewalls

Do's for Students

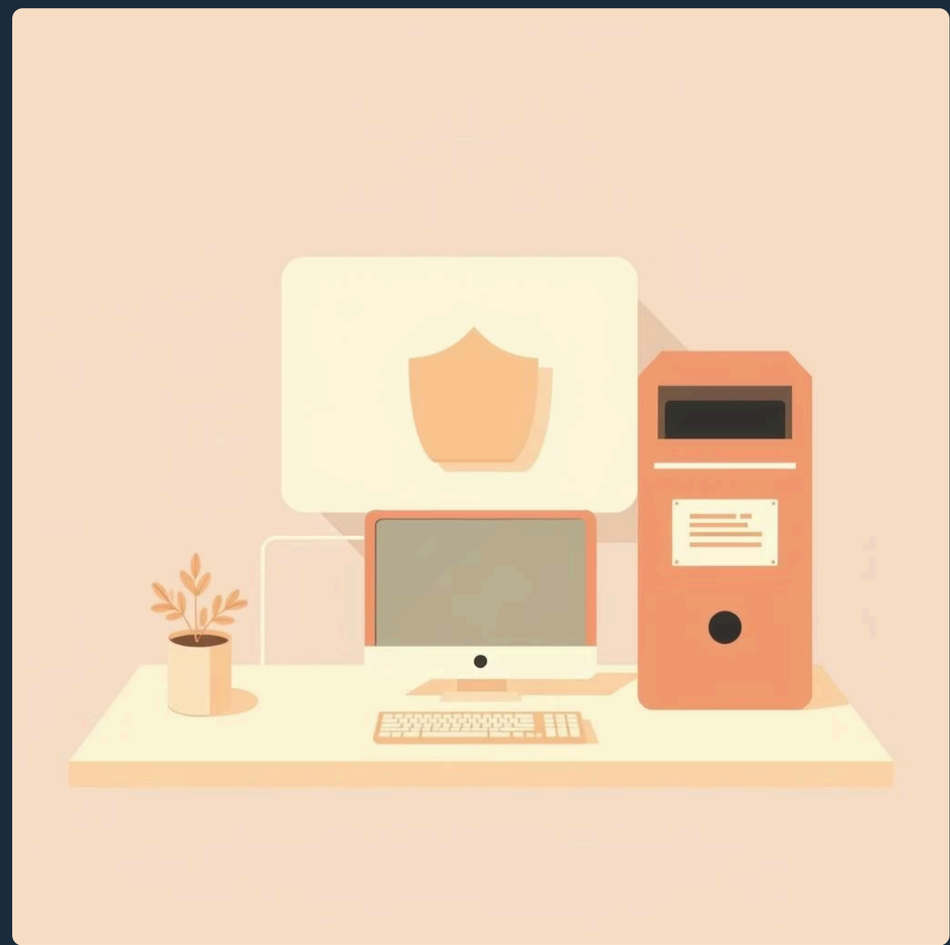
- Use strong, unique passwords for every account.
- Install reputable antivirus software.
- Enable Two-Factor Authentication (2FA).
- Keep your software and apps updated.

Don'ts for Students

- Click on unknown links or suspicious attachments.
- Share your passwords with anyone.
- Use public Wi-Fi for sensitive transactions without a VPN.

The Role of Firewalls

A firewall acts as a barrier, monitoring and controlling incoming and outgoing network traffic based on predefined security rules.



Components: Packet filters inspect data packets, proxies act as intermediaries, and Network Address Translation (NAT) masks internal IP addresses, all working to block unauthorized access.