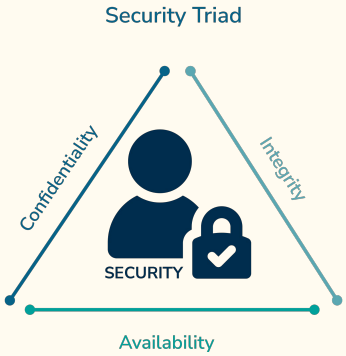
PBEL - IBM
Cyber Security Assignment

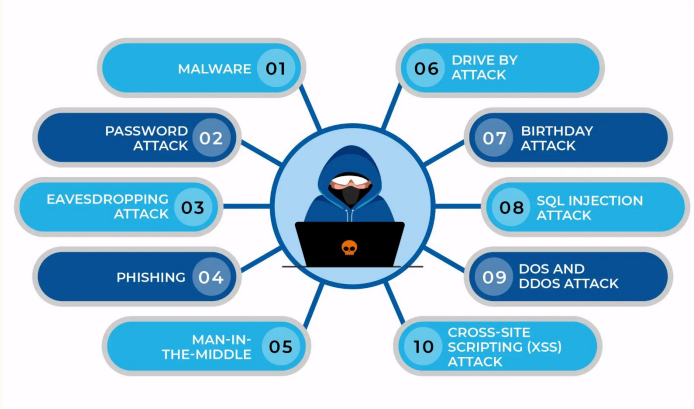
by SHIVANSH SINGH
shivanshsinghvishen18@gmail.com

1)What is cybersecurity? Why is it important in today's digital world?

Cybersecurity refers to the set of practices, technologies, and processes used to protect systems, networks, programs, and data from unauthorized access, attacks, damage, or theft. Its primary goal is to ensure **Confidentiality, Integrity, and Availability**—collectively known as the **CIA Triad**. These principles ensure that only authorized individuals access data (Confidentiality), that data remains accurate and unaltered (Integrity), and that services and information are reliably accessible (Availability).

In the modern world, where everything from banking, healthcare, education, and government functions relies heavily on digital infrastructure, cybersecurity has become critical. Daily threats such as **malware**, **phishing**, **ransomware**, and **advanced persistent threats (APTs)** can result in **data breaches**, **financial loss**, **identity theft**, and **reputational damage**.





Importance of Cybersecurity in the Digital Era:

- **Protection of Sensitive Data:** Personal information, trade secrets, and financial data must be shielded from hackers and unauthorized users.
- **Defending against Cyber Threats:** Incidents like the *WannaCry ransomware attack (2017)* and the *Yahoo data breach (2013-14)* show how devastating cyber attacks can be for individuals and large corporations alike.
- **Preserving National Security:** Nation-state-sponsored cyber attacks on infrastructure can compromise a country's security and stability.
- **Maintaining Trust:** Organizations need to ensure user data is safe to preserve trust and comply with laws such as the **IT Act, 2000 (India)** or **GDPR (Europe)**.

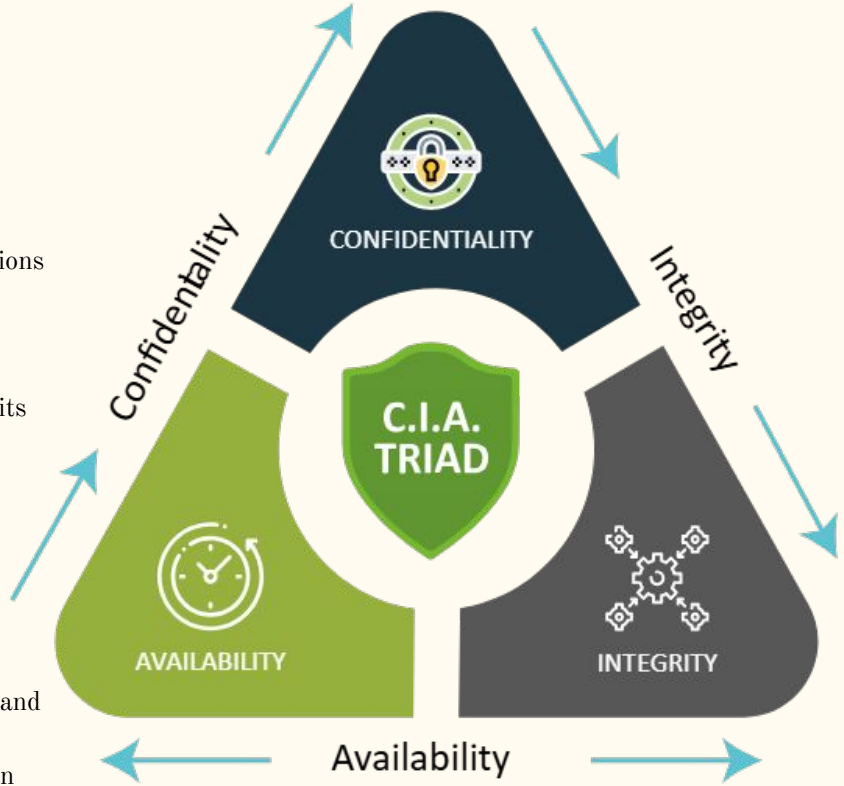
2) Define the CIA Triad in cybersecurity.

The **CIA Triad** is a foundational concept in cybersecurity, representing the three core principles that guide the protection of digital data and systems:

- 🔐 **C – Confidentiality**
  Confidentiality ensures that sensitive information is **only accessible to authorized users** and protected from unauthorized access or disclosure.
  Example: Using passwords, encryption, and access control lists (ACLs) to restrict data access.
  Real-World Case: In the *Yahoo data breach*, the loss of confidentiality exposed billions of user accounts.

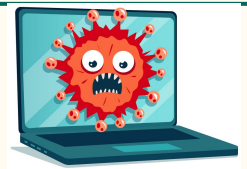
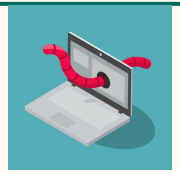
- ✅ **I – Integrity**
  Integrity guarantees that information is **accurate, consistent, and unaltered** from its original state unless modified by authorized sources.
  Example: Using checksums, digital signatures, and version control to detect and prevent unauthorized data tampering.
  Importance: Prevents scenarios like financial fraud, misinformation, or corrupt software updates.

- 📶 **A – Availability**
  Availability ensures that **authorized users have timely and reliable access** to data and systems when needed.
  Example: Redundant systems, regular backups, and DDoS protection help maintain uptime.
  Case Example: *WannaCry ransomware* attack severely impacted availability by locking critical files on infected systems.



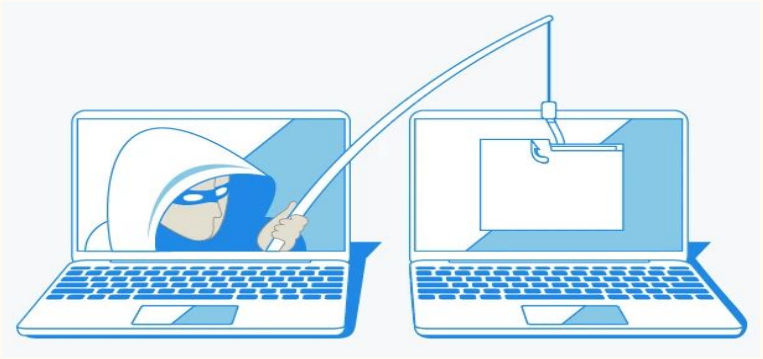
3) What is the difference between a virus, a worm, and a trojan horse?

Difference Between Virus, Worm, and Trojan Horse:

Aspect	Virus	Worm	Trojan Horse
Definition	Malicious code that attaches to legitimate files/programs	Self-replicating malware that spreads across networks	Malicious software disguised as legitimate or useful software
Replication	Needs user action to execute and spread	Spreads automatically without user intervention	Does not replicate itself
Spread Method	Infected files, email attachments	Network vulnerabilities, shared drives	Tricked download/install by the user
User Interaction	Required to execute infected file	Not required	Required (user believes it's safe and installs it)
Damage Caused	Corrupts or modifies files, slows system	Network congestion, system slowdown	Opens backdoors, steals data, installs other malware
Example	Melissa Virus	ILOVEYOU Worm	Fake antivirus programs
			

4) Explain the term phishing with an example.

Phishing is a type of **social engineering attack** where attackers deceive individuals into revealing sensitive information—such as login credentials, credit card numbers, or personal data—by pretending to be a trustworthy source, usually via email, message, or website.



🔑 **Key Characteristics:**

- Often mimics legitimate organizations (banks, government, social media).
- Creates a sense of urgency (e.g., “Your account will be locked!”).
- Redirects users to fake websites that look real.
- May include malicious attachments or links.

🎯 **Example:**

A user receives an email claiming to be from their bank saying:

"Dear Customer, we have detected suspicious activity in your account. Please verify your identity by clicking the link below."

The link leads to a **fake banking website**. When the user enters their username and password, the attackers capture this information and use it for **unauthorized access or financial theft**.

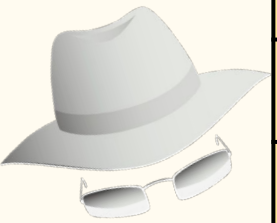
🧠 **Real-World Case:** In **2016**, phishing emails played a major role in the *Democratic National Committee (DNC) hack*, where attackers tricked staff into revealing login credentials.

🔐 **Protection Tips:**

- Always verify email senders.
- Hover over links to preview the URL.
- Enable two-factor authentication (2FA).
- Never share credentials via email or text.

5) Explain the term phishing with an example.

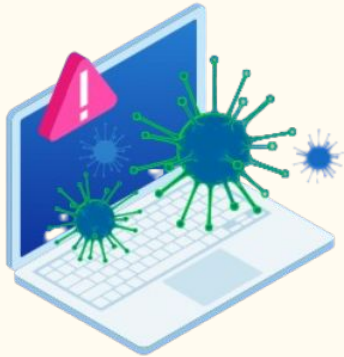
Ethical Hacking, also known as **white hat hacking**, is the **legal and authorized process of identifying and fixing security vulnerabilities** in computer systems, networks, or applications. Ethical hackers simulate the techniques used by malicious attackers but do so with the **permission** of the organization, with the goal of improving security rather than exploiting it. Difference between Ethical Hacking and Malicious hacking is given below:



Aspect	Ethical Hacking (White Hat)	Malicious Hacking (Black Hat)
Purpose	To identify and fix security vulnerabilities	To exploit vulnerabilities for personal gain or to cause harm
Permission	Performed with legal authorization from the system owner	Done without permission, violating laws and privacy
Legality	Legal and encouraged as part of proactive security measures	Illegal and punishable under cybercrime laws
Intent	Defensive: Protect systems and data	Offensive: Steal data, disrupt systems, or cause financial damage
Examples of Activity	Penetration testing, vulnerability assessment	Data theft, ransomware attacks, phishing, system defacement
Tools Used	Same tools as malicious hackers (e.g., Nmap, Burp Suite) but used ethically	Same tools but used unethically
Certification	Often certified (e.g., CEH – Certified Ethical Hacker)	No formal certification; operates anonymously or under false identities

6)List any five common types of cyber-attacks and describe them briefly.

Here are **five common types of cyber-attacks**, along with brief descriptions:



1. Malware

Definition: Malware (malicious software) is designed to damage, disrupt, or gain unauthorized access to computer systems.

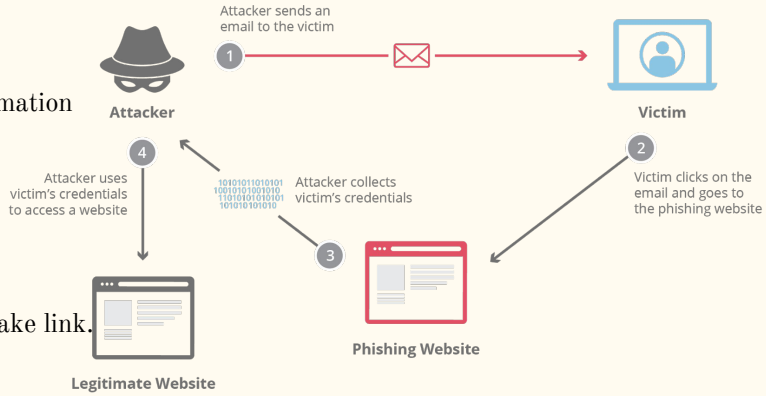
Types include:

- **Virus:** Attaches to files and spreads when opened.
- **Worm:** Spreads across networks without user action.
- **Trojan Horse:** Disguised as legitimate software.
- **Ransomware:** Encrypts files and demands ransom.

📌 **Example:** *WannaCry ransomware* attack affected thousands of organizations globally in 2017.

2. Phishing

Definition: A form of social engineering where attackers trick users into revealing sensitive information (like passwords or credit card numbers) by pretending to be a trusted source.



Common Forms:
Fake emails, websites, or messages imitating banks or services.

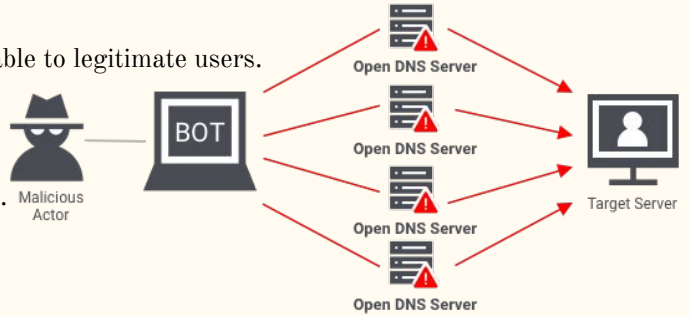
📌 **Example:** An email claiming to be from your bank asks you to verify your login by clicking a fake link.

3. Denial-of-Service (DoS) Attack

Definition: Overwhelms a system, server, or network with traffic to exhaust resources, making it unavailable to legitimate users.

Variant: Distributed DoS (DDoS)—launched from multiple systems simultaneously.

📌 **Example:** Attack on GitHub in 2018 that caused temporary service outages using massive data traffic.

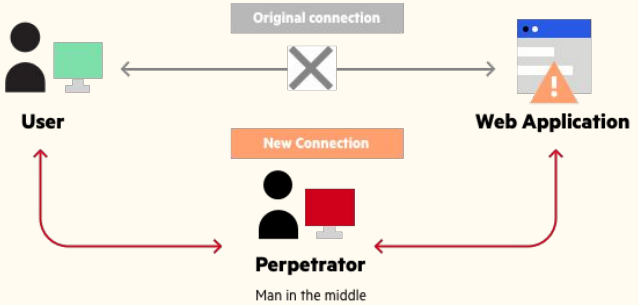


4. Man-in-the-Middle (MitM) Attack

Definition: An attacker intercepts communication between two parties to eavesdrop or manipulate the data.

Common Scenario: On unsecured public Wi-Fi, attackers can intercept login credentials.

📌 **Example:** A hacker capturing login credentials during a session between a user and a banking website.

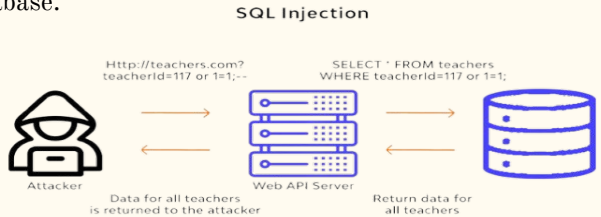


5. SQL Injection

Definition: Attackers insert malicious SQL queries into input fields of a website to access or manipulate the database.

Result: Unauthorized access to sensitive data like user accounts, passwords, etc.

📌 **Example:** An attacker logs into an admin panel without valid credentials by manipulating login fields.



7) How does two-factor authentication improve security?

Two-Factor Authentication (2FA) is a security process that requires users to provide **two different types of verification** before gaining access to an account or system. It strengthens traditional password-based security by adding an extra layer of protection.

🔐 **How 2FA Works:** It combines **two of the following** authentication factors:

1. **Something you know** — Password or PIN
2. **Something you have** — Mobile phone, OTP token, smart card
3. **Something you are** — Fingerprint, facial recognition, voice pattern

Feature	How It Improves Security
Prevents Unauthorized Access	Even if a hacker steals your password, they still can't log in without the second factor (like OTP).
Reduces Phishing Impact	Protects against password theft via phishing, as attackers lack access to the second factor.
Protects Sensitive Accounts	Especially valuable for banking, email, and social media accounts.
Secures Remote Access	Widely used in corporate VPNs and cloud applications.

🔍 **Real-World Example:**If someone obtains your Gmail password via a phishing attack but tries to log in from a new device, **Google prompts for a code sent to your phone**. Without that code, access is denied.

Conclusion:

2FA significantly **lowers the risk of unauthorized access**, even if login credentials are compromised. It's one of the simplest and most effective ways to **enhance account security** in today's cyber-threat landscape.

8) Describe any recent cybercrime incident in India. What were its consequences?

📰 **Recent Cybercrime Incident: Mobile Malware Fraud in Lucknow:**

On **July 20, 2025**, a resident of Nishatganj, Lucknow received a phone call claiming to be about **Aadhaar card upgradation**. The caller sent an APK file named *iMobile.apk* via WhatsApp. Upon installation, the app secretly installed a **Remote Access Trojan (RAT)**, granting cybercriminals full control over the victim's mobile device. As a result, unauthorized withdrawals totaling **₹8.70 lakh** were made from his linked debit card—often requiring OTP access, SMS interception, and remote operation of banking apps.

Key features of the scam:

- Used social engineering to gain trust.
- Delivered malware via malicious APK through WhatsApp.
- Enabled remote control of banking and messaging systems.

⚠️ **Consequences & Impact:**

- **Financial loss:** The victim lost ₹8.70 lakh, illustrating how quickly malware infections can drain digital accounts.
- **Data & device vulnerability:** RAT allowed full remote control—accessing SMS, handling OTPs, and compromising banking applications.
- **Broader warning:** Highlighted the increasing risk of mobile-based cyberattacks in India's digital ecosystem.
- **Regulatory and public awareness:** Incident was reported to **National Cyber Crime Helpline**, demonstrating prompt escalation and the value of response Infrastructure.

✅ **Broader Context:** This incident reflects a rising trend: cybercriminals using disguised apps and **social engineering via WhatsApp** to target victims. Such RAT-based attacks are potent because they combine trust manipulation with deep technical control of devices. These techniques are increasingly used in mobile banking fraud across urban centers in India.

Risk Factor	Description
Social engineering	Gaining user trust via impersonation of official entity
Malware delivery method	APK file sent over WhatsApp posing as a legitimate app
Technical control	RAT grants full access to SMS, banking apps, OTP interception
Financial theft mechanism	Remote initiation of debit card transactions without user consent

🛡️ Preventive Measures (Recommendations)

- **Avoid installing APKs** unless from official app stores (Google Play, Apple App Store).
- **Never share OTPs** or pass codes—even if prompted by someone claiming to be from an authority.
- **Verify unsolicited messages or calls** independently via official helplines.
- **Enable device-level security**: use updated antivirus/mobile security tools and regular system updates.
- **Report cyber fraud quickly** to local law enforcement and the National Cyber Crime Helpline.

In summary, this RAT-based mobile malware attack in Lucknow demonstrates how cybercriminals exploit use
The consequences—financial loss, compromised data, and device control—underscore the urgent need for awareness and proactive digital hygiene.

9) Create a cybersecurity awareness guide for college students, listing Do's and Don'ts.

🎓 **Cybersecurity Awareness Guide for College Students**

Stay Safe. Stay Smart. Stay Secure.

In today's digital-first world, college students are frequent targets of cybercriminals due to their extensive use of social media, online banking, and academic platforms. Practicing good cyber hygiene helps protect your personal data, financial information, and academic records.

✅ **Do's of Cybersecurity**

✔️ Action	🛡️ Why It Matters
Use strong & unique passwords	Prevents easy access to your accounts by attackers.
Enable two-factor authentication (2FA)	Adds an extra layer of security beyond passwords.
Update software & apps regularly	Fixes known security vulnerabilities.
Use a reputable antivirus software	Helps detect and remove malicious programs.
Log out of public/shared systems	Prevents others from accessing your information.
Use secure Wifi or VPN	Protects your data on public/untrusted networks.
Verify suspicious emails & links	Avoid phishing and social engineering attacks.
Backup important files	Ensures data recovery in case of ransomware or device loss.

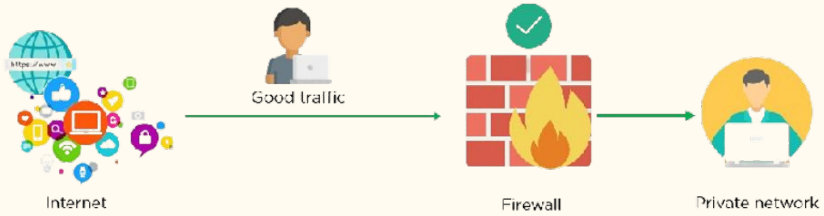
❌ Don’ts of Cybersecurity

🚫 Avoid This	⚠️ Risk It Creates
Don’t reuse the same password across sites	Increases exposure if one account is breached.
Don’t click unknown links or download untrusted attachments	May install malware or lead to phishing sites.
Don’t ignore software updates	Leaves your device vulnerable to known attacks.
Don’t share personal info on public forums or social media	Can be used for identity theft or social engineering.
Don’t use cracked/pirated software	May come bundled with malware and lacks security support.
Don’t leave devices unattended	Makes it easier for physical or remote breaches to happen.
Don’t trust unsolicited tech support calls	Common method for remote access scams.

Remember: Your digital identity is just as valuable as your physical one. A few good habits can prevent major losses and protect your academic and personal life from cyber threats. 🌐🔒

10) Discuss the major components and uses of a firewall in network security.

A **firewall** is a crucial network security device—either hardware or software—that monitors and filters incoming and outgoing network traffic based on predefined security rules. It acts as a **barrier between a trusted internal network and untrusted external sources** (like the internet).

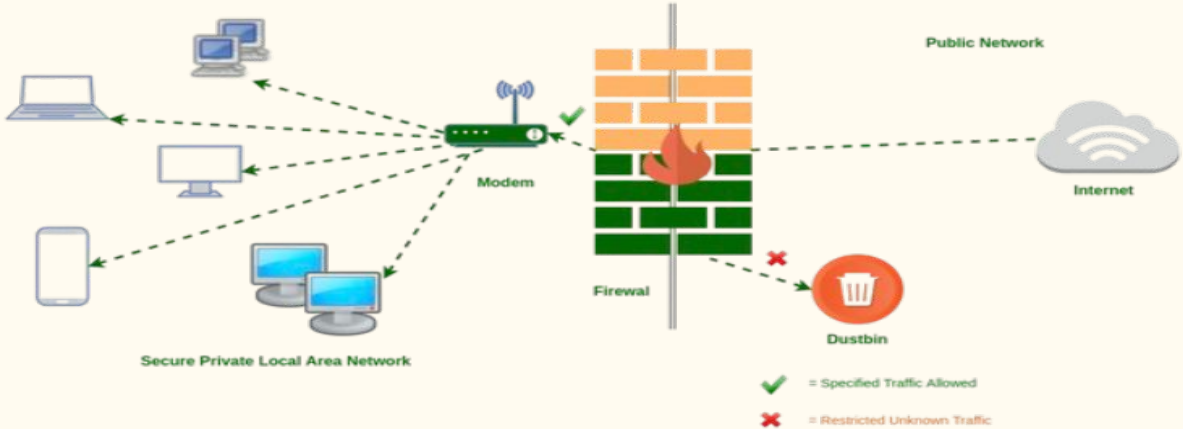


🔧Major Components of a Firewall

Component	Description
Packet Filter	Inspects packets and allows or blocks them based on source/destination IP, ports, and protocols.
Proxy Server	Acts as an intermediary between users and the internet, masking internal IPs and filtering content.
Network Address Translation (NAT)	Hides internal IP addresses by converting them to a public IP for internet communication.
Stateful Inspection	Tracks active connections and ensures packets match a known, safe session.
Application Layer Filtering	Analyzes data at the application layer (e.g., HTTP, FTP) to block malicious or unwanted content.
Logging and Alerting	Records traffic data and notifies administrators of suspicious activities.

🛡️ Uses of a Firewall

✅ Use Case	💡 Purpose
Preventing Unauthorized Access	Blocks external attacks trying to access internal systems.
Monitoring Network Traffic	Keeps track of all traffic entering and leaving the network.
Restricting Access to Specific Services	Can block social media, gaming, or file-sharing sites during work hours.
Protection Against Malware	Stops malicious traffic and prevents known threats from spreading.
Enforcing Security Policies	Ensures only authorized users and data types pass through.



🔐 **Summary:**

A firewall is your first line of defense in cybersecurity. It protects systems from **unauthorized access**, **monitors suspicious behavior**, and **enforces security policies**, making it a critical component of any secure network infrastructure.