Cyber Security: Safeguarding the Digital World

Presented by Sameer

PSIT Kanpur, Computer Science

What is Cybersecurity?

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, damage, or theft. It involves a combination of technologies, processes, and controls designed to protect the integrity, confidentiality, and availability of information assets.

Digital Guardian

It acts as a shield, defending your online activities, from banking to social media, against malicious attacks and privacy breaches.

Protecting You

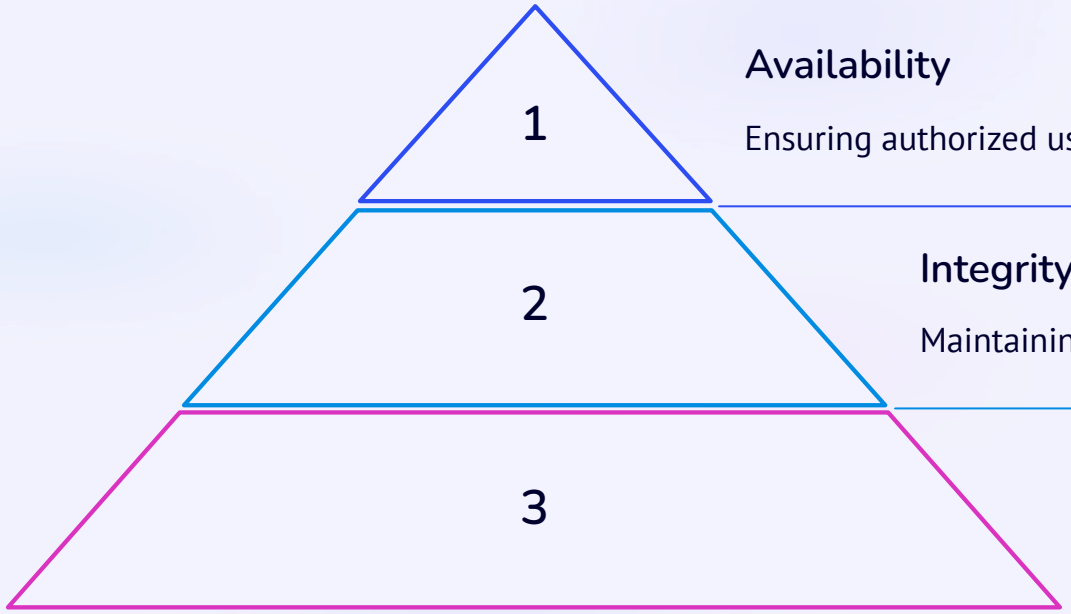
In today's interconnected world, cybersecurity is paramount for safeguarding personal information, financial assets, and critical infrastructure from ever-evolving threats.

Real-Life Relevance

Think about online banking, shopping, or even your social media. Without robust cybersecurity, these daily activities are vulnerable to fraud, identity theft, and data loss.

The CIA Triad in Cybersecurity

The CIA Triad is a fundamental model for information security, guiding policies and practices to protect data effectively.



Availability

Ensuring authorized users can access information when needed.

Integrity

Maintaining data accuracy and preventing unauthorized modification.

Confidentiality

Protecting information from unauthorized access and disclosure.

Each component is crucial for a comprehensive security posture, with the absence of any element compromising the entire system.

Virus vs. Worm vs. Trojan Horse

Understanding the differences between these common malware types is crucial for effective cyber defense.

Virus	Worm	Trojan Horse
Requires a host program to spread and activate, often attaching to legitimate files.	Self-replicating and self-propagating, able to spread across networks independently.	Disguises itself as legitimate software to trick users into installing it, often creating backdoors.
Spreads via infected files, often through downloads or email attachments.	Spreads through network vulnerabilities, without user interaction.	Relies on social engineering; users unknowingly install it, believing it's benign.

While all are malicious, their distinct propagation methods and behaviors demand different defensive strategies.

Phishing Explained

Phishing is a social engineering technique where attackers deceive individuals into revealing sensitive information, often through fake communications.

Attackers typically send emails or messages impersonating trusted entities like banks, social media platforms, or government agencies. These messages often create a sense of urgency or fear to prompt immediate action.

The goal is to trick the recipient into clicking a malicious link, downloading an infected attachment, or entering credentials on a fake login page that mimics a legitimate one.

For example, you might receive an email claiming to be from your bank, asking you to "verify your account details" due to suspicious activity, leading you to a fraudulent website.

Ethical vs. Malicious Hacking

Hacking isn't always malicious. Understanding the distinction is key to comprehending cybersecurity roles.

Ethical (White-Hat) Hacking

Ethical hackers use their skills to identify vulnerabilities in systems and networks with the owner's permission. They mimic malicious attacks to test an organization's security posture, reporting weaknesses before they can be exploited by bad actors.

Many ethical hackers participate in "bug bounty" programs, legally earning rewards for discovering and reporting security flaws.

Malicious (Black-Hat) Hacking

In contrast, malicious hackers exploit vulnerabilities for illegal purposes, such as stealing data, disrupting services, or deploying malware. Their actions are unauthorized and often result in significant financial loss and data breaches for victims.

This type of hacking is illegal and can lead to severe legal consequences, including imprisonment and hefty fines.

Five Common Cyber Attacks

Cybercriminals employ diverse methods to compromise systems and data. Here are five prevalent attack types:

DDoS (Distributed Denial-of-Service)

Overwhelms a system with traffic, making it unavailable to legitimate users.

Ransomware

Encrypts data or locks systems, demanding a ransom for decryption keys.

SQL Injection

Inserts malicious SQL code into input fields to manipulate database queries.

Brute Force

Tries many password combinations until the correct one is found.

Man-in-the-Middle (MitM)

Intercepts communication between two parties, often without their knowledge.

Two-Factor Authentication (2FA)

2FA adds an essential layer of security beyond just a password, significantly reducing the risk of unauthorized access.

2FA requires users to provide two different authentication factors to verify their identity. This typically involves something you know (like a password) combined with something you have (like a phone or a token) or something you are (like a fingerprint).

Even if a hacker steals your password, they can't access your account without the second factor. Common examples include a password combined with a one-time password (OTP) sent to your mobile phone, or biometric verification.

Implementing 2FA greatly enhances account security, making it a critical defense against phishing and credential theft.

Recent Cybercrime in India: AIIMS Ransomware Attack (2022)

The All India Institute of Medical Sciences (AIIMS) in Delhi suffered a major ransomware attack in November 2022, highlighting the vulnerability of critical infrastructure.

Attack Initiated

Malicious actors launched a ransomware attack, encrypting servers and disrupting services.

1

2

System Downtime

Hospital operations were severely affected, with patient registrations, appointments, and billing systems going offline.

Government Investigation

A high-level government investigation was launched to determine the source and scope of the breach.

3

4

Consequences

Significant patient data was potentially compromised, leading to privacy concerns and operational delays.

This incident underscored the urgent need for enhanced cybersecurity measures in vital sectors.

Student Cybersecurity Guide & Firewalls

Do's and Don'ts for Students

- **Do:** Use strong, unique passwords and enable 2FA.
- **Do:** Keep software updated (OS, antivirus, apps).
- **Do:** Use reputable antivirus software.
- **Don't:** Click suspicious links or download unknown attachments.
- **Don't:** Reuse passwords across multiple accounts.
- **Don't:** Disable security settings or ignore warnings.

Understanding Firewalls

A firewall acts as a barrier, monitoring and controlling incoming and outgoing network traffic based on predefined security rules. It's crucial for protecting networks, like your college Wi-Fi or home network, from unauthorized access.

Key components include packet filtering (checking data packets), proxy services (intermediaries for requests), and Network Address Translation (NAT) for hiding internal IP addresses.