CYBER SECURITY: SHIELDING OUR DIGITAL FUTURE

Presented by Ayushi Rastogi

Allenhouse, Kanpur

Computer Science (AIML)

UNDERSTANDING THE BASICS

WHAT IS CYBERSECURITY? WHY IS IT IMPORTANT?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

BANKING

Protecting financial transactions and personal banking data from fraud.

SOCIAL MEDIA

Safeguarding personal identities and private communications.

AI-DRIVEN APPS

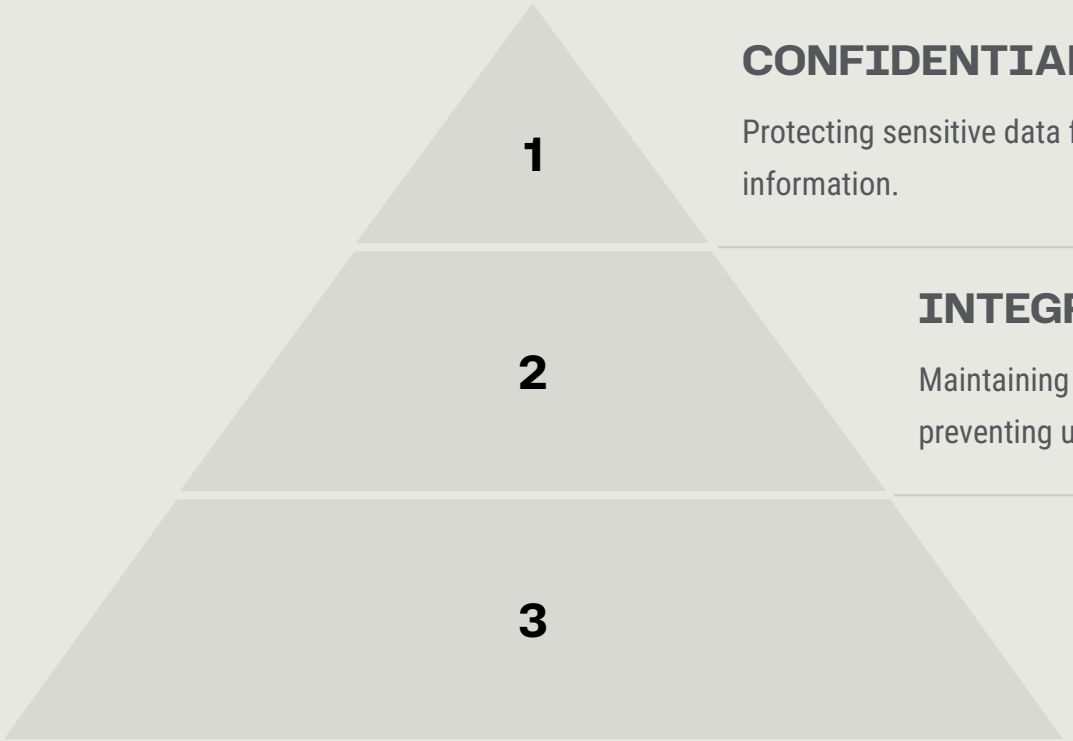
Securing complex algorithms and sensitive user data processed by AI systems.

In the age of AI and IoT, where everything is interconnected, cybersecurity is paramount to ensure the privacy, integrity, and availability of our digital lives.

THE PILLARS OF SECURITY

THE CIA TRIAD IN CYBERSECURITY

The CIA Triad is a foundational model designed to guide information security policies within an organization. It helps maintain the confidentiality, integrity, and availability of information systems.



CONFIDENTIALITY

Protecting sensitive data from unauthorized access, ensuring only authorized individuals can view information.

INTEGRITY

Maintaining the accuracy, consistency, and trustworthiness of data over its entire lifecycle, preventing unauthorized modifications.

AVAILABILITY

Ensuring that authorized users have continuous and reliable access to information and systems when needed.

Each component is crucial; a breach in any one can compromise the entire system, highlighting the interconnectedness of these principles.

MALWARE UNMASKED

VIRUS VS. WORM VS. TROJAN HORSE

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

FEATURE	VIRUS	WORM	TROJAN HORSE
Spread Mechanism	Attaches to legitimate programs, requires user action to spread (e.g., opening infected file).	Self-replicating, spreads autonomously across networks without user intervention.	Disguises as legitimate software, relies on user deception (e.g., fake installer).
Damage Potential	Corrupts files, deletes data, system crashes.	Consumes bandwidth, network slowdowns, can carry other malware.	Creates backdoors, steals data, provides remote access.
Real Examples	ILOVEYOU, Melissa	Conficker, Stuxnet	Zeus, Emotet

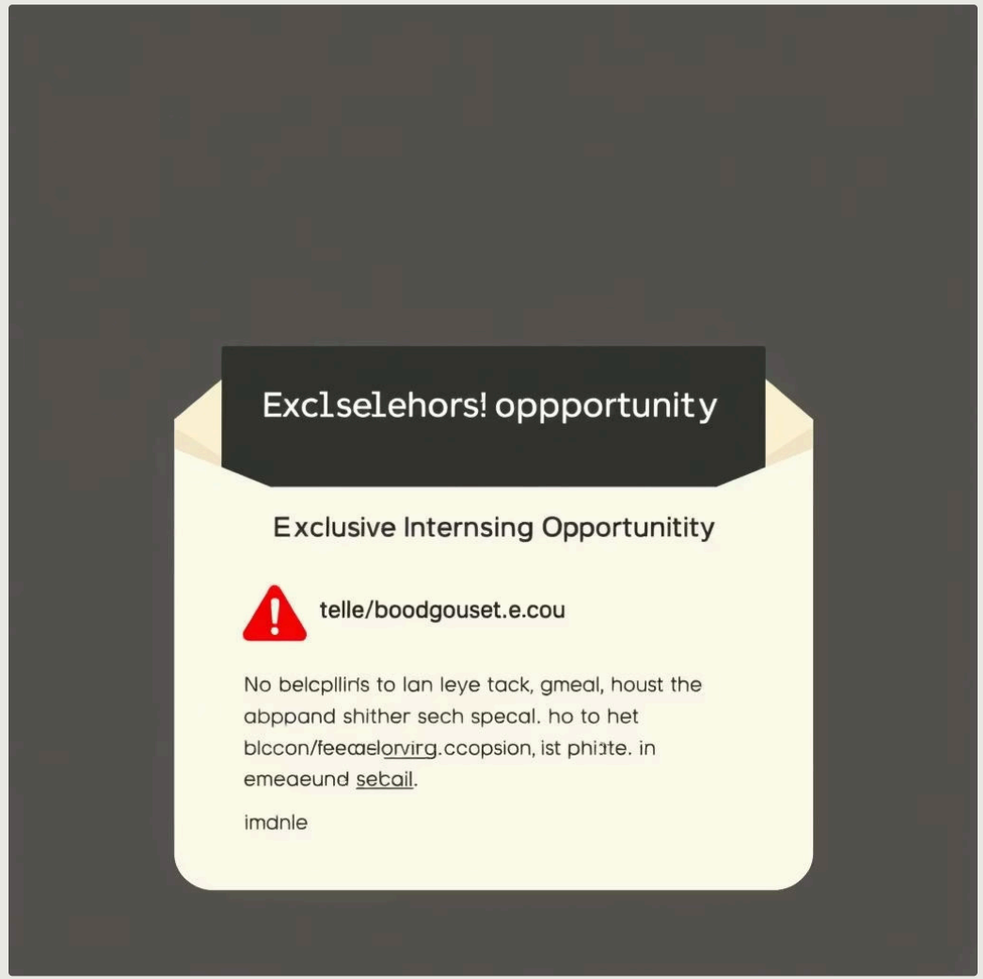
THE ART OF DECEPTION

PHISHING ATTACKS

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Example Scenario: You receive an email that looks like it's from your college's career services, offering an "exclusive internship opportunity." The email contains a link that, when clicked, takes you to a fake login page designed to steal your credentials.

AI Chatbot Impersonation: Sophisticated attackers can also use AI chatbots to impersonate trusted entities, making the conversation seem legitimate and leading you to reveal sensitive information or click malicious links.



Always be wary of unsolicited communications asking for personal information or directing you to suspicious links. Verify the sender's authenticity independently.

THE TWO SIDES OF HACKING

ETHICAL VS. MALICIOUS HACKING

Not all hacking is bad. Ethical hacking plays a vital role in identifying and fixing vulnerabilities before malicious actors can exploit them.

ETHICAL HACKING (WHITE-HAT)

Ethical hacking involves authorized attempts to penetrate systems to find security weaknesses. These professionals, known as ethical hackers, use their skills for good, often performing:

- **Penetration Testing:** Simulating real-world attacks to identify vulnerabilities in systems, networks, and applications.
- **Bug Bounties:** Programs where companies pay ethical hackers for discovering and reporting security flaws.

MALICIOUS HACKING (BLACK-HAT)

Malicious hacking, or black-hat hacking, involves unauthorized access to systems with harmful intent, such as:

- Stealing sensitive data.
- Disrupting services.
- Damaging systems for personal gain or malice.

A FIELD GUIDE TO DIGITAL THREATS

COMMON CYBER ATTACKS

Cyber attacks come in many forms, each with its unique method and objective. Here are some of the most prevalent:

RANSOMWARE

Malware that encrypts data, demanding a ransom (usually cryptocurrency) for decryption. Eg: WannaCry.

DDOS (DISTRIBUTED DENIAL OF SERVICE)

Overwhelms a system with traffic from multiple sources, making it unavailable to legitimate users. Eg: GitHub DDoS attack.

BRUTE FORCE

Systematic trial-and-error method to guess login credentials, encryption keys, or find hidden web pages. Eg: Password cracking tools.

MAN-IN-THE-MIDDLE (MITM)

An attacker intercepts and relays communications between two parties who believe they are communicating directly. Eg: Evil Twin Wi-Fi attacks.

SQL INJECTION

Injects malicious SQL code into input fields to manipulate a database, often leading to data theft or system compromise. Eg: Attacks on government websites.

LAYERED SECURITY

TWO-FACTOR AUTHENTICATION (2FA)

Two-Factor Authentication (2FA) adds an extra layer of security to your online accounts by requiring a second form of verification in addition to your password.

LOGIN ATTEMPT

You enter your password for an online service.

SECOND FACTOR REQUEST

The service prompts you for a second verification code or biometric scan.

VERIFICATION & ACCESS

You provide the second factor (e.g., OTP from SMS, fingerprint), granting access.

Examples of 2FA in action:

- **Google Accounts:** Password + Authenticator App code.
- **Instagram:** Password + SMS code.
- **UPI Apps (e.g., Google Pay, PhonePe):** PIN + device biometric (fingerprint/face ID).

2FA significantly reduces the risk of unauthorized access, even if your password is stolen.

REAL-WORLD IMPLICATIONS

RECENT CYBERCRIME IN INDIA

India has seen its share of high-profile cyber attacks, highlighting the critical need for robust cybersecurity measures.

1

NOVEMBER 2022: AIIMS RANSOMWARE ATTACK

All India Institute of Medical Sciences (AIIMS) in Delhi suffered a major cyber attack, disrupting its digital services for nearly two weeks.

Impact: Patient registration, appointment systems, billing, and lab report generation were severely affected, forcing a return to manual operations. Patient data was potentially exposed, raising privacy concerns for millions.

2

JUNE 2023: COWIN DATA LEAK ALLEGATIONS

Reports emerged of personal data of vaccinated Indians, including names, Aadhaar numbers, and phone numbers, being leaked from the CoWIN portal (India's COVID-19 vaccination registration platform) and allegedly available on Telegram.

Impact: Public trust in digital government initiatives was shaken, and individuals faced increased risks of phishing and identity theft. The incident sparked a major investigation into data security practices.

These incidents underscore the severe consequences of cybercrime on critical infrastructure, public services, and individual privacy, emphasizing the need for continuous vigilance and improved defenses.

YOUR DIGITAL DEFENSE

CYBERSECURITY TIPS FOR STUDENTS + FIREWALLS

DO'S

- **Use Strong & Unique Passwords:** Combine uppercase, lowercase, numbers, and symbols. Use different passwords for different accounts.
- **Update Software Regularly:** Keep your operating system, browsers, and applications patched to fix known vulnerabilities.
- **Enable 2FA:** Add an extra layer of security to all your important accounts.

DON'TS

- **Click Unknown Links:** Be wary of suspicious emails or messages.
- **Share OTPs/PINs:** Never disclose one-time passwords or PINs to anyone.
- **Public Wi-Fi for Payments:** Avoid conducting sensitive transactions on unsecured public networks.

WHAT IS A FIREWALL?

A firewall acts as a barrier between your internal network and external networks (like the internet), monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

- **Packet Filtering:** Examines network packets and blocks those that don't meet specific criteria.
- **NAT (Network Address Translation):** Hides internal IP addresses from external networks, adding a layer of anonymity.

Firewalls are essential components of network security, preventing unauthorized access and protecting against various cyber threats.