Introduction to Cyber security

- **Definition**
  - Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
  - It is a set of principles aimed at protecting computing resources and online information from threats.
  - Cyber - the technology that includes systems, networks, programs, and data.
  - Security - the protection of systems, networks, applications, and information.
  - **Alias :**
    - **electronic information security**
    - **information technology security**

- **Importance**
  - Cyber attacks can be extremely expensive for businesses to endure
  - Data breach can also causes reputational damage
  - Cyber-attacks these days are becoming progressively destructive.
  - Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- **Challenges of CS**
  - **Increasing Sophistication of Cyber Attacks**
    - **Complexity**: Cyber-attacks have reached unprecedented levels of sophistication, making them difficult to detect and defend against.
    - **Advanced Persistent Threats (APTs)**: Attackers infiltrate networks and remain undetected for months or years, collecting valuable data or disrupting operations incrementally.
    - **Evolving Ransomware**: Beyond simple file encryption, modern ransomware includes threats to leak sensitive information if demands are unmet, increasing the severity of attacks.

- **Human Error**
  - **Weakest Link:** Human error is a major contributor to cybersecurity breaches in organizational security defenses.
  - **Common Mistakes:**
    - Using weak passwords or sharing credentials across multiple accounts.
    - Falling for phishing scams, where employees believe fraudulent emails are legitimate.
  - **Accidental Data Exposure:** Employees may unintentionally share sensitive information through unsecured channels, such as personal email or unencrypted cloud drives.

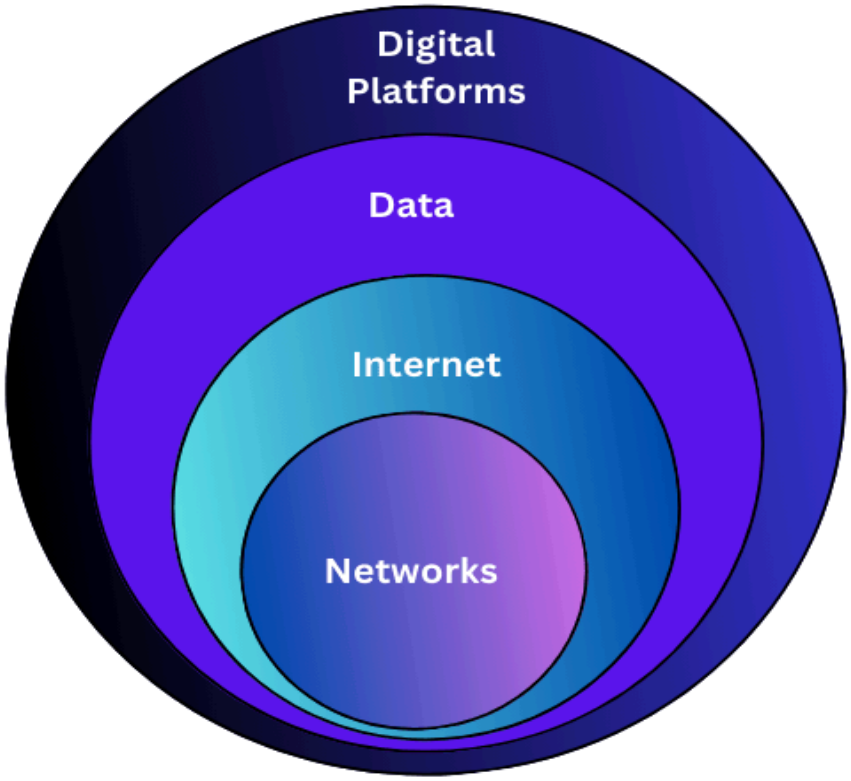
- **Rapidly Evolving Technology**
  - **Dual Nature:** While new technologies drive efficiency and innovation, they also introduce vulnerabilities that cybercriminals exploit.
  - **IoT Vulnerabilities:** IoT devices, such as home appliances and industrial systems, expands the attack surface. Many of these devices lack security features, making them easy targets.

- **Third-Party Risks**
  - **Vendor Dependencies**: Businesses increasingly rely on third-party vendors for operations, which heightens the risk of security breaches through these external partners.
  - **Security Gaps**: If vendors do not adhere to strict security, they can become weak points, compromising the entire supply chain.

- **Lack of Skilled Cybersecurity Professionals**
  - **Skills Shortage**: The growing frequency and complexity of cyber threats have increased the demand for qualified cybersecurity experts, but the supply of skilled professionals is insufficient.
  - **Impact**: This skills gap hinders organizations' ability to effectively detect, respond to, and mitigate cyber threats, leaving them vulnerable to attacks due to inadequate management of advanced security tools and strategies.

Introduction to Cyberspace

- **Definition**
  - Cyberspace is termed as a virtual and dynamic domain created by computer clones
  - It describes the immaterial space where interactions through digital networks, the internet, and computer systems take place
  - It is fundamentally dependent on technical advancement and innovation
  - All digital interactions in this space, including sending emails, visiting websites, and using social media are part of cyberspace
- **Components**



  - **Networks**
    - The foundation of cyberspace, comprising access networks, Metropolitan Area Networks (MANs), and Wide Area Networks (WANs).

        - These networks connect devices, enabling data relay across short distances or vast expanses.

- **The Internet**
    - A critical feature of cyberspace, serving as a complex network of networks.
    - Functions as a primary channel for communication, information distribution, and online business platforms.

- **Data**
    - The core element that connects users in cyberspace, transmitted at billions of bits per second.
    - Exists in various formats, including text, images, videos, and files.

- **Digital Platforms:**
    - Virtual systems provide services and resources through active interaction.
    - Examples include social media, search engines, cloud storage, and online marketplaces, forming the framework of the digital world.

Introduction to Cyber Crime and Cyber Law

- **Who are Cyber Criminals ?**
  - Cyber criminals are individuals or groups who use computers and the internet to commit crimes
  - They use digital tools and systems to exploit weaknesses in the system to steal personal information, money, or sensitive data, or to disrupt services.
  - Cyber criminals are motivated by:
    - Profit
    - Personal Grudges
    - Political Reasons
    - Challenge
  - They can operate alone or as part of organized groups, and their actions can impact individuals, businesses, and governments.
  - **Examples:** hacking into systems, spreading viruses, committing online fraud, and launching cyberattacks.

  - **Types of Cyber Criminals:**
    - **Type 1: Hungry for Recognition**
      - **Examples:** Hobby hackers, IT professionals, terrorist organizations.
      - **Characteristics:** Seek acknowledgment for their skills or actions, often publicizing their exploits.

    - **Type 2: Not Interested in Recognition**
      - **Examples:** Financially motivated, organized criminals.
      - **Characteristics:** Focus on profit, operating secretly to maximize financial gain without drawing attention.

    - **Type 3: Insiders**
      - **Examples:** Former employees seeking revenge, competitors using employees for economic advantage.

- **Characteristics:** Exploit internal access or knowledge to harm organizations or gain competitive edges.

Classification of Cyber crimes

- **Cyber Crimes Against Individuals**
  - **Email Spoofing:** cybercriminal forges the sender's email address to make the message appear as if it's from a legitimate source
  - **Spamming:** Sending unsolicited emails or messages in bulk. While some spam is harmless, others spread malware, conduct phishing, or promote scams, posing privacy risks.
  - **Cyber Defamation:** Harming a person's reputation by spreading false statements online
  - **Cyber Stalking:** Harassing or intimidating individuals through digital means, such as sending unwanted messages, tracking online activities, or creating fear
  - **Phishing:** Deceiving individuals into sharing confidential information (e.g: login credentials, financial data) via fake emails or websites that appear legitimate

- **Cyber Crimes Against Property**
  - **Credit Card Fraud:** Gaining unauthorized access to credit card information, leading to illegal purchases and financial losses
  - **Intellectual Property Theft:** Unauthorized use or distribution of copyrighted materials, patents, or trade secrets.
  - **Internet Time Theft:** Using another person's internet connection without permission
  - **Cyber Vandalism:** Defacing or damaging online property, such as altering websites or social media profiles.

- **Cyber Crimes Against Organisations**
  - **Unauthorized Access and Data Theft:** Intruding into an organization's systems without permission to steal confidential data.

        - **Denial of Service (DoS) Attacks:** Intruding into an organization's systems without permission to steal confidential data.
        - **Virus and Malware Attacks:** Malicious programs installed on a system to cause damage, steal information, or disrupt operations
        - **Salami Attacks:** Small amounts of money are stolen over a prolonged period, often remaining unnoticed due to the minor impact of each transaction
        - **Web Jacking:** An attacker takes control of an organisation's website, often redirecting it to a malicious site

    - **Cyber Crimes Against Society**
        - **Forgery:** Using computers to create counterfeit documents (e.g., currency, certificates) with high-quality printers and scanners, causing financial and reputational damage
        - **Cyber Terrorism:** Digital means to intimidate or harm people, organisations, or governments

Legal perspective of Cyber crime

- **Information Technology Act, 2000**
    - **Introduction:**
        - A legal framework proposed by the Indian Parliament, is the primary legislation in India dealing with cybercrime and electronic commerce
        - To provide a legal framework for e-commerce, ensuring lawful conduct of digital transactions, and reduce cyber crimes

    - **Enactment:**
        - The bill of this law was passed in the Budget by a group of Parliament members, headed by the then Minister of Information Technology
        - It was signed by the President on **9 May 2000**
        - Came into effect on **October 17, 2000**

- **Structure:**
  - Comprises 94 sections, organized into 13 chapters and 2 schedules

- **Purpose:**
  - The Indian cyber laws are governed by this act, with amendments to strengthen its provisions
  - Formulated to ensure the lawful conduct of digital transactions and the reduction of cyber crimes, on the basis of the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model)

- **Key Features:**
  - Facilitates registration of real-time records with the government.
  - Recognizes digital signatures to authenticate electronic records, offering greater reliability than handwritten signatures.
  - Addresses cyber crimes such as hacking, phishing, cyberstalking, identity theft, and cyberterrorism.

- **Advantages:**
  - Grants legal recognition to electronic communications (e.g., emails, messages), making them admissible as evidence in court
  - Supports e-commerce and e-business by providing a legal infrastructure.
  - Corporations get statutory remedies in the event of unauthorised access or hacking into their computer systems or networks

- **Disadvantage:**
  - Fails to address issues related to domain names and the rights/liabilities of domain owners
  - Despite prevalent copyright and patent issues, it does not adequately protect Intellectual Property Rights for computer

programs and networks.

- **Amendments**
  - **2008 Amendment:**
    - Came up with modifications to **Section 66A** of the IT Act, 2000
    - Section 66A was to penalize sending offensive messages electronically, including those spreading hatred or compromising national security
    - Struck down the section later due to vague definitions of "offensive," which led to misuse and excessive punishment

  - **2015 Amendment Bill:**
    - In 2015, another bill was initiated to amend Section 66A by aligning with **Article 19** with the aim of safeguarding the fundamental rights guaranteed to citizens by the country's Constitution
    - Declared Section 66A as violative of free speech rights.

- **Key Sections and Penalties**

Section	Offense	Penalty
Section 43	Applies to individuals who damage computer systems without permission	The owner can claim full compensation for damages
Section 65	Tampering with documents stored in a computer system	3 years imprisonment or ₹2 lakh fine or both
Section 66	Covers fraudulent or dishonest acts as described in Section 43	3 years imprisonment or ₹5 lakh fine, or both
Section 66B	Dishonestly receiving stolen computers communication devices	3 years imprisonment or ₹1 lakh fine, or both
Section 66C	Identity theft involving digital signature passwords, or other identification featur	3 years imprisonment or ₹1 lakh fine, or both
Section 66D	Cheating by impersonation using computer resources	3 years imprisonment or ₹1 lakh fine, or both
Section 66E	Invading Privacy	3 years imprisonment or ₹2 lakh fine, or both
Section 66F	Cyber terrorism	Life Imprisonment
Section 67	Sending explicit or obscene material electronically	5 years imprisonment and ₹10 lakh fine
Section 67A	Sending sexually explicit material	7 years imprisonment and ₹10 lakh fine
Section 67B	Depicting children in sexually explicit material and sharing such material electronically	7 years imprisonment and ₹10 lakh fine

- **An Indian perspective of Cyber crime**

    - **Internet Usage**: India ranks 4th globally in the number of internet users, increasing the scope for cyber crimes.
    - **Types of Crimes**: Includes traditional crimes (e.g., theft, forgery) and new offenses covered by the IT Act.
    - **Cyber laws:** Define and penalize cyber crimes like hacking, phishing, cyberstalking, identity theft, and cyberterrorism.
    - **IT Act:** Amended in 2008 to provide stronger laws to combat cyber crime.
    - **Digital signatures:** Used to authenticate electronic records and are more trustworthy than handwritten signatures.
    - **Children as victims:** Children can be victims of cyber crime, especially from pedophiles who exploit children's lack of understanding of the dangers of the internet.