Introduction to cyber security

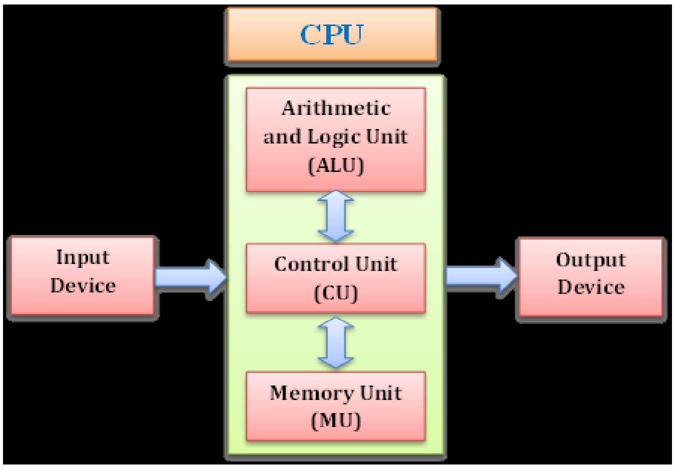
Definition : Cyber security is the practice of protecting digital systems, networks, and data from various forms of threats, attacks, and unauthorized access. It plays a vital role in safeguarding the confidentiality, integrity, and availability of information in the digital age.

Defining Cyberspace: Cyberspace is a virtual environment or digital domain in whichelectronic data, information, and communication are created, stored, processed, and exchanged.

Cyberspace is where online activities such as web browsing, email communication,social media interactions, online gaming, and various other digital transactions take place.

Overview of computer

Computer is an electronic device that receives input, stores or processes the input as per userinstructions and provides output in desired format.



The basic parts of a computer are as follows:

- **Input Unit:** Devices like keyboard and mouse that are used to input data and instructionsto the computer are called input unit.
- **Output Unit:** Devices like printer and visual display unit that are used to provide information to the user in desired format are called output unit.
- **Control Unit:** This unit controls all the functions of the computer. All devices or parts ofcomputer interact through the control unit.
- **Arithmetic Logic Unit:** This is the brain of the computer where all arithmetic operationsand logical operations take place.
- **Memory:** All input data, instructions are stored in the memory. Memory is of two types –primary memory and secondary memory. Primary memory resides within the CPU whereas secondary memory is external to it.

Characteristics of Computer

1. **Speed:** Computer can carry out 3-4 million instructions per second.
2. **Accuracy**: Computers exhibit a very high degree of accuracy. Errors that may occur are usually due to inaccurate data, wrong instructions.
3. **Reliability:** Computers can carry out same type of work repeatedly without throwing up errors due to tiredness or boredom.
4. **Versatility**: Computers can carry out a wide range of work from data entry and ticket booking to complex mathematical calculations and continuous astronomical observations.
5. **Storage Capacity**: A computer can store millions of records. These records may be accessed with complete precision. Computer memory storage capacity is measured in Bytes, Kilobytes (KB), Megabytes(MB), Gigabytes(GB), and Terabytes(TB). A computer has builtin memory known as primary memory.

Advantages of Computer

1. **Multitasking**: Multitasking is one of the main advantages of computers. The computer can perform millions or trillions of works in one second.
2. **Speed**: One of the most advantages of computers is their incredible speed which helps human to finish their task in a few seconds.
3. **Accuracy:** Computers perform not only calculations but also with accuracy.
4. **Communication:** The computer helps the user better understand and communicate with Other devices.

Disadvantages of computer

1. **Virus and hacking attacks**: A virus may be a worm and hacking are just unauthorized access over a computer for illegal purposes. Viruses can go to another system from email attachments, viewing an infected website advertisement, through removable devices like USBs, etc.
2. **Online Cyber Crimes:** Online cyber-crime means computers and networks may have been utilized in order to commit a crime. Cyberstalking and fraud are the points that come under online cyber-crime.
3. **Health Problems**: Prolonged use of computers to work leads to various health problems. Working for long hours with a computer may affect the sitting posture of the user and sometimes irritates the eyes.

Overview of web technology

Web Technology refers to the various tools and techniques that are utilized in the process of communication between different types of devices over the Internet. A web browser is used to access web pages. Web browsers can be defined as programs that display text, data, pictures, animation, and video on the Internet.

Web Technology can be classified into the following sections:

1.World Wide Web (WWW): The World Wide Web is based on several different technologies: Web browsers, Hypertext Mark-up Language (HTML), and Hypertext Transfer Protocol (HTTP).
2**. Web Browser:** The web browser is an application software to explore WWW (World Wide Web). It provides an interface between the server and the client and requests to the server for web documents and services.
3. Web Server: Web server is a program which processes the network requests of the users and serves them with files that create web pages. This exchange takes place using Hypertext Transfer Protocol (HTTP). Web Pages: A webpage is a digital document that is linked to the World Wide Web and viewable by anyone connected to the internet has a web browser.
4. Web Development: Web development refers to the building, creating, and maintaining of websites. It includes aspects such as web design, web publishing, web programming, and database management. It is the creation of an application that works over the internet i.e. websites.

Architecture of cyber space or cyber security

A cyber security architecture combines security software and appliance solutions, providing the infrastructure for protecting an organization from cyber-attacks. The architecture of cyberspace refers to the underlying structure and organization of the digital realm, which encompasses the internet, computer networks, and virtual environments. It involves various components and layers that enable the transmission, storage, and retrieval of information.

1. **Physical Infrastructure**: The physical architecture of cyberspace includes the network of cables, routers, switches, and servers that form the backbone of the internet. This infrastructure allows data to be transmitted across long distances through wired or wireless connections.

2. **Network Protocols**: Network protocols define the rules and standards for data transmission between devices on a network. Protocols like TCP/IP (Transmission Control Protocol/Internet Protocol) govern how data is packaged, addressed, and routed across the internet.

3. **Internet Service Providers (ISPs):** ISPs are companies that provide internet connectivity to users. They play a crucial role in the architecture by connecting individual devices to the larger network, enabling access to cyberspace.

4. **Domain Name System (DNS**): The DNS is responsible for translating human-readable domain names (e.g., www.example.com) into IP addresses that computers can understand. It acts as a distributed database, mapping domain names to their corresponding IP addresses.

5. **Data Centers :** A data center is a centralized cluster of computing and networking equipment that stores and processes business-critical information for an enterprise in one physical location.

6. **Cyber security layers:** security layers refer to the several levels of security controls that may be used to defend against online attacks.

7. **Internet service provider** : An ISP (internet service provider) is a company that provides individuals and organizations access to the internet and other related services. An ISP has the equipment and the telecommunication line access required to have a point of presence on the internet for the geographic area served.

8. **Social media platform and online communication**: Social media is a collective term for websites and applications that focus on communication, community-based input, interaction, content-sharing and collaboration. People use social media to stay in touch and interact with friends, family and various communities. Businesses use social applications to market and promote their products and track customer concerns.

9. C**loud computing :** Cloud computing, commonly referred to as "the cloud," is the delivery of hosted services — like storage, servers, and software — through the internet. Cloud computing allows businesses to reduce costs, accelerate deployments, and develop at scale.

10. C**yber laws and regulation** : Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes.

Communication technology

It refers to the tools, systems, and methods that facilitate the exchange of information and data between individuals, organizations, or devices. It has evolved significantly over the years and plays a crucial role in various aspects of our personal and professional lives. There are numerous subsets of communication, these include

- Writing skills
- Oral communication
- Presentation skills
- Active listening
- Nonverbal communication

Purpose Communication serves many purposes for people:

- To inform others of something
- To express feelings
- To influence somebody in a particular direction
- To collaborate with others

1. Telecommunication: Telecommunication technology enables voice and data transmission over long distances. This includes landline phones, mobile phones, and the infrastructure that supports them, like cell towers and undersea cables.

2. Internet: The internet is a global network that connects billions of devices worldwide. It enables various communication methods, such as email, instant messaging, video conferencing, and social media.

3. Email: Email is one of the most common methods of electronic communication. It allows individuals and organizations to send text messages, documents, and multimedia files to one another over the internet.
4. Instant Messaging: Instant messaging apps and platforms like WhatsApp, Facebook Messenger, and Slack allow real-time text and multimedia communication between individuals or groups.
5. Social Media: Social media platforms like Facebook, Twitter, Instagram, and LinkedIn provide tools for sharing content, networking, and communicating with a global audience.
6. Video Conferencing: Video conferencing tools like Zoom, Microsoft Teams, and Skype enable face-to-face communication over the internet, making it possible for people to hold virtual meetings and collaborate from different locations.

Web Technology

Web technology refers to the tools, software, protocols, and standards used for building and maintaining websites and web applications.

1. Hypertext Markup Language (HTML): HTML is the standard markup language used to create web pages. It defines the structure and content of a web page, including text, images, links, and other elements.
2**. Cascading Style Sheets (CSS**): CSS is used for styling web pages. It controls the presentation and layout of HTML elements, allowing web designers to control fonts, colors, spacing, and more.
3. JavaScript: JavaScript is a programming language that allows for dynamic and interactive web content. It can be used for client-side scripting to create responsive user interfaces and add functionality to web pages.
4. HTTP and HTTPS: Hypertext Transfer Protocol (HTTP) is the protocol used for transferring data over the web. HTTPS (HTTP Secure) is a secure version of HTTP that encrypts data to protect it from eavesdropping and tampering.
5. Web Servers: Web servers are software applications or hardware devices that store and serve web content to users' browsers. Popular web server software includes Apache, Nginx, and Microsoft Internet Information Services (IIS).
6. Databases: Web applications often rely on databases to store and retrieve data. Technologies like SQL and NoSQL databases (e.g., MySQL, MongoDB) are used for this purpose.
7. Web Frameworks: Web frameworks provide pre-built templates and tools for web application development. Examples include Ruby on Rails, Django, and Angular.
8. Web Browsers: Web browsers like Google Chrome, Mozilla Firefox, and Microsoft Edge render and display web pages for end-users. They also support various web technologies and standards.

Internet

The internet is a global network of interconnected computers and computer networks that communicate using a common set of protocols. It has revolutionized the way people communicate, access information, conduct business, and much more.

Here are some key points about the internet:

1. Network of Networks: The internet is not a single network but a vast collection of interconnected networks. These networks range from small, local networks within homes and offices to large, global networks operated by internet service providers (ISPs).

2. Protocols: The internet relies on standardized communication protocols, including the Internet Protocol (IP) for addressing and routing data packets, Transmission Control Protocol (TCP) for reliable data transfer, and various application layer protocols for services like email (SMTP), web browsing (HTTP), and file transfer (FTP).

Advantages of the Internet

- **Online Banking and Transaction**: The Internet allows us to transfer money online through the net banking system. Money can be credited or debited from one account to the other.
- **Education, Online Jobs, Freelancing:** Through the Internet, we are able to get more jobs via online platforms like Linkedin and to reach more job providers. Freelancing on the other hand has helped the youth to earn a side income and the best part is all this can be done via the INTERNET.
- **Entertainment**: There are numerous options for entertainment online we can listen to music, play games can watch movies, and web series, and listen to podcasts, YouTube itself is a hub of knowledge as well as entertainment.
- **New Job Roles**: The Internet has given us access to social media, and digital products so we are having numerous new job opportunities like digital marketing and social media marketing online businesses are earning huge amounts of money just because the Internet is the medium to help us to do so.
- **Best Communication Medium**: The communication barrier has been removed from the Internet. You can send messages via email, Whatsapp, and Facebook. Voice chatting and video conferencing are also available to help you to do important meetings online.

Disadvantages of the Internet

- **Time Wastage**: Wasting too much time on the internet surfing social media apps and wasting time on scrolling social media apps.
- **Bad Impacts on Health:** Spending too much time on the internet causes bad impacts on your health physical body needs some outdoor games exercise and many more things. Looking at the screen for a longer duration causes serious impacts on the eyes.
- **Cyber Crimes:** Spam, viruses, hacking, and stealing data are some of the crimes which are on the verge these days. Your system which contains all the confidential data can be easily hacked by cybercriminals.

- **Effects on Children:** Small children are heavily addicted to the Internet watching movies, and games all the time is not good for their overall personality as well as social development.

World Wide Web (WWW)

History :- It is a created, by Timothy Berner Lee in 1989, for researchers to work together effectively at CERN, is an organization named the World Wide Web Consortium (W3C), which was developed for further development of the web. This organization is directed by Tim Berner's Lee, aka the father of the web. The World Wide Web (WWW), often simply referred to as the web, is a system of interconnected documents and resources on the internet.

1.Hypertext: The WWW is built on the concept of hypertext, which allows documents to contain hyperlinks that can be used to navigate between related documents. These hyperlinks are typically displayed as text or interactive elements on web pages.

2. URLs: Uniform Resource Locators (URLs) are used to specify the address of web resources on the WWW. A URL consists of a protocol (e.g., HTTP or HTTPS), a domain name (e.g., www.example.com), and a specific path to a resource (e.g., /page1.html).

3. World Wide Web Consortium (W3C): The W3C is an international community that develops and maintains web standards and guidelines to ensure the long-term growth and compatibility of the web. It establishes standards like HTML5 and CSS.

Difference between World Wide Web and the Internet

World Wide Web	**Internet**
All the web pages and web documents are storedthere on the World wide web and to find all that stuff you will have a specific URL for each website.	The Internet is a global network of computers that is accessed by the Worldwide web.
The world wide web is a service.	The Internet is an infrastructure.
The world wide web is a subset of the Internet.	The Internet is the superset of the world wideweb.
The world wide web is software-oriented.	The Internet is hardware-oriented.
The world wide web uses HTTP.	The Internet uses IP Addresses.
The world wide web can be considered as a bookfrom the different topics inside a Library.	The Internet can be considered a Library

Advent(History) of The Internet

The advent of the internet marked a significant turning point in the history of communication, technology, and society. Here's a brief overview of the key milestones and events that led to the development of the internet:

1. 1960sThe Precursor: ARPANET: The precursor to the modern internet was ARPANET (Advanced Research Projects Agency Network), funded by the U.S. Department of Defense's DARPA (Defense Advanced Research Projects Agency). ARPANET was developed to facilitate communication between researchers and was the first network to use packet switching, a fundamental technology for data transmission.

2. 1970sTCP/IP: In the early 1970s, Vint Cerf and Bob Kahn developed the Transmission Control Protocol (TCP) and the Internet Protocol (IP), collectively known as TCP/IP. This set of protocols became the basis for the internet, allowing various networks to communicate with each other.

3. 1980sThe Internet is Born: In 1983, the ARPANET adopted TCP/IP as its standard protocol, marking the transition from ARPANET to the internet. The term "internet" was coined to describe the global network of interconnected networks.

4. 1989Invention of the World Wide Web: British computer scientist Sir Tim Berners-Lee developed the World Wide Web, introducing the concepts of URLs, HTTP, and HTML. This innovation made the internet more accessible to the general public by creating a user-friendly way to access and share information.

5. 1990sCommercialization and Expansion: The 1990s saw the commercialization of the internet, with the development of internet service providers (ISPs) and the popularization of the web. Companies like Netscape Navigator and Yahoo played significant roles in this expansion.

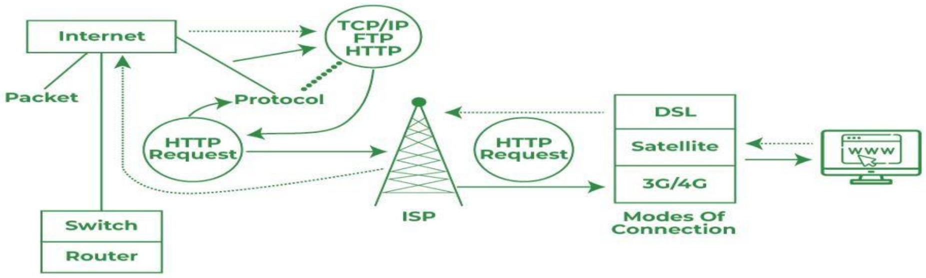
6. Late 1990sDot-com Bubble: The late 1990s witnessed the dot-com bubble, characterized by a speculative frenzy around internet-related companies. While many companies did not survive, this period paved the way for the growth of the digital economy.

7. Early 2000sBroadband and Social Media: The 2000s brought widespread adoption of broadband internet, making it faster and more accessible to users. Social media platforms like Facebook, Twitter, and YouTube emerged, transforming how people connect and share information online.

Internet infrastructure for data transfer

The internet infrastructure for data transfer is a critical component of the global network that enables the seamless exchange of data between devices and systems across the world. This infrastructure encompasses a range of elements and technologies that work together to facilitate data transfer.
Connecting two computers with the help of any communication method.
To solve the connection issue, protocols were introduce
It is a standardized method of performing certain tasks and data formatting so that two or more devices can communicate with each other.

Ethernet – If both systems are connected over the same network
IP (Internet Protocol) – for receiving and sending packets from network to network
TCP (Transmission Control Protocol) – To ensure that those packets are arriving successfully in the same order,
HTTP (Hyper Text Transfer Protocol) – for formatting data over websites and apps .
Routers and Switches: Routers and switches are network devices that direct data packets to their intended destinations. Routers determine the most efficient path for data to travel between networks.



1.Firstly, you’ll be required to connect your system or PC with any router or modem to establish a connection. This connection is the base of the internet connection.
2. When you open the browser and start typing something like “www.google.com”, your system will push a query command to your ISP (Internet Service Provider) that is connected with other servers that store and process data.
3. Now, the web browser will start indexing the URL that you’ve entered and will fetch the details in numeric format (in their own language to identify the address (unique) that you’re trying to reach.
4. Next is, now your browser will start sending the HTTP request where you’re trying to reach and sends a copy of the website on the user’s system. Note: The server will send data in the form of small packets (from the website to the browser)
5. Once all the data (of small packets) will be received at the user’s end (PC/Laptop), the browser will start arranging all those small packets and later will form a collective file (here, the browser will gather all the small packets and rearrange them just like a puzzle) and then you’ll be able to see the contents of that website.

What are the Modes of Connecting through the Internet?

There are certain ways of getting connected to the Internet and going online. So, for that, you need an ISP (Internet Service Provider), the type of ISP you'll be choosing will depend upon the availability in your area and what kind of services they're offering to their customers. Here we are listing some universal modes of the internet:

- **DSL:** This technology (Digital Subscriber Line) uses a Broadband connection which is in trend for the past few years. Your ISP will connect your premises with the help of telephone wire despite the fact that you own a telephone.
- **Dial-Up:** People used to connect their system with the help of a dial-up connection, and it is one of the slowest types of Internet connection. This is used to enable internet connectivity with the help of a telephone connection and the user must have multiple connections then only they can use a Dial-up connection.
- **Cable TV Connection:** It is being used to connect your system to the Internet, and for that, you, ISP will connect it via cable TV wire. It also uses Broadband technology and you really don't need to have a Cable connection for that. Cable is considered as most accessible as and faster than dial-up and DSL that we have for connection.
- **Satellite:** It also uses broadband technology but without interacting with any cable connection. Hence, it connects wirelessly with the help of a satellite and this enables its availability anywhere in the world.
- **3G/4G/5G:** This is the new age technology in the entire world. It connects wirelessly via different ISPs and is widely used in cell phones. But they aren't considered as stable as DSL or cable and most importantly they come with a DATA LIMITATION cap for each month.

Internet Governance

Internet governance refers to the processes, rules, and organizations that oversee and coordinate various aspects of the global internet. It encompasses a wide range of issues, including technical standards, access, privacy, security, and the resolution of disputes. Internet governance is a multi-stakeholder model, involving input and collaboration from governments, the private sector, civil society, and the technical community.

1. **Multistakeholder Model**: Internet governance follows a multistakeholder approach, which means that various stakeholders, including governments, businesses, nongovernmental organizations, and technical experts, have a role in shaping internet policies and standards.

2. **Key Organizations:** Internet Corporation for Assigned Names and Numbers (ICANN): ICANN is responsible for managing the domain name system (DNS) and allocating IP addresses. It plays a crucial role in coordinating the internet's technical infrastructure. Internet Engineering Task Force (IETF): The IETF develops and publishes internet standards and protocols, ensuring the technical aspects of internet governance are maintained.

   World Wide Web Consortium (W3C): The W3C develops and maintains web standards such as HTML, CSS, and web accessibility guidelines.
   Internet Governance Forum (IGF): The IGF is a global platform for discussing internet governance issues and policies. It promotes an open, inclusive, and collaborative approach to governance.

3. **Domain Name System (DNS):** The DNS is a critical part of internet governance, as it translates domain names (e.g., www.example.com) into IP addresses, allowing users to access websites. ICANN plays a central role in managing the DNS.

4. **Internet Policies**: Governments and international bodies may create policies and regulations that impact the internet. This includes issues related to data protection, privacy, cybercrime, and content control.

   5. Content Regulation: Internet governance also encompasses the regulation of online content, with debates surrounding issues like hate speech, fake news, and harmful content.

Internet Society

The Internet Society (ISOC) is a global nonprofit organization that advocates for an open, accessible, and secure internet for everyone. It was founded in 1992 and is headquartered in Reston, Virginia, USA. The Internet Society's mission is to promote the development and use of the internet for the benefit of all people throughout the world.

1.Advocacy for an Open Internet: ISOC advocates for the principles of an open and free internet, where information is freely accessible, and users have the freedom to communicate and innovate. They work to ensure that the core values of the internet, such as openness, inclusivity, and global collaboration, are preserved.

2. Technical Expertise: The Internet Society plays a significant role in maintaining the technical standards and protocols that underpin the internet. They support the Internet Engineering Task Force (IETF) and other technical organizations that work on internet standards and best practices.

4. **Promotion of Internet Access:** ISOC is dedicated to expanding internet access around the world. They support initiatives that aim to bridge the digital divide and provide underserved communities with internet connectivity.

5. **Internet Governance**: The organization actively participates in internet governance discussions and forums, promoting a multistakeholder approach that includes governments, businesses, civil society, and the technical community.

6. **Internet Safety and Security:** ISOC is committed to enhancing internet safety and security. They work on initiatives related to Cyber security, privacy, and encryption, helping to protect users and organizations online.

7. **Community Building:** The Internet Society connects a global network of members, chapters, and partners. They facilitate discussions and collaborations among various stakeholders to address challenges and opportunities in the digital age.

8. **Public Policy** and Advocacy: ISOC engages in public policy and advocacy efforts to influence legislation and regulations that impact the internet. They promote policies that are in line with the principles of an open and accessible internet.

9. **Capacity Building**: ISOC provides training, resources, and support to strengthen the technical and policy expertise of individuals and organizations working with or on the internet.

10. **Internet Hall of Fame**: The Internet Society runs the Internet Hall of Fame, which recognizes individuals who have made significant contributions to the development and growth of the internet. 10. Events and Conferences: The organization hosts conferences, workshops, and events to facilitate discussions and knowledge sharing about internet-related topics.

REGULATION OF CYBERSPACE

The regulation of cyberspace refers to the legal and policy frameworks established by governments and international organizations to govern and oversee activities in the digital realm, including the internet. These regulations are essential for addressing a wide range of issues such as Cyber security, data privacy, intellectual property, online content, and more.

1. **Cyber security Regulation**: Governments and international bodies create regulations and standards to enhance Cyber security. These regulations often require organizations to implement measures to protect their systems and data, and they may also outline breach notification requirements.

2. **Data Privacy Laws**: Data privacy regulations, like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), aim to protect individuals' personal data. They govern how organizations collect, process, and store personal information and may grant individuals rights over their data.

3. **Intellectual Property Laws**: Intellectual property regulations in cyberspace cover copyright, patents, trademarks, and trade secrets. They aim to protect the rights of content creators and inventors and prevent online piracy and infringement.

4. **Content Regulation**: Regulations address issues like hate speech, fake news, and harmful content. They may impose restrictions on the type of content that can be posted online and define the responsibilities of online platforms in monitoring and moderating content.

5. **Net Neutrality**: Net neutrality regulations ensure that internet service providers (ISPs) treat all internet traffic equally, without discrimination or prioritization based on content, source, or destination.

6. **Electronic Transactions and E-Commerce Laws**: These regulations define the legal framework for online transactions, contracts, and electronic signatures. They ensure that ecommerce activities are enforceable and secure.

7. **Jurisdiction and Cross-Border Legal Issues**: Cyberspace operates across international borders, which raises complex jurisdictional challenges. Regulations often define which laws apply in cross-border legal disputes and extradition requests related to cybercrimes.

8. **Government Surveillance** and Privacy: The balance between government surveillance for security purposes and individual privacy is regulated by laws that govern surveillance practices and data access by government agencies.

9. **Encryption Policies**: Governments may establish regulations regarding encryption technologies and access to encrypted data in the interest of national security or criminal investigations.

10. **International Agreements and Treaties**: International agreements, such as the Budapest Convention on Cybercrime, facilitate cooperation among countries in combating cybercrimes and enforcing regulations on a global scale.

Concept of Cyber security

Cyber security is the practice of protecting computer systems, networks, and digital data from theft, damage, or unauthorized access. It encompasses a wide range of measures, technologies, processes, and best practices designed to safeguard digital information and the systems that process it. The primary goal of Cyber security is to ensure the confidentiality, integrity, and availability of data and computing resources. Here are the key concepts of Cyber security:

1. **Confidentiality**: Confidentiality ensures that data is only accessible by authorized individuals or systems. Measures to achieve confidentiality include encryption, access controls, and data classification.

2. **Integrity**: Data integrity ensures that data remains accurate, reliable, and unaltered during storage and transmission. Hashing and digital signatures are used to verify the integrity of data.

3. **Availability**: Availability ensures that systems and data are accessible when needed. Measures to ensure availability include redundancy, failover systems, and DDoS protection.

4. **Authentication:** Authentication verifies the identity of users and systems. This is typically done through the use of usernames, passwords, multi-factor authentication (MFA), and biometrics.

5. **Authorization**: Authorization specifies what users and systems are allowed to do once authenticated. Access control lists, role-based access control, and permissions are used to manage authorization.

6. **Firewalls**: Firewalls are security devices or software that filter network traffic, allowing or blocking data packets based on predefined security rules. They help protect against unauthorized access and network threats.

7. **Intrusion Detection and Prevention Systems** (**IDS**/**IPS**): IDS and IPS systems monitor network traffic for suspicious or malicious activity. IDS detects threats, while IPS can actively block or mitigate threats.

8. **Antivirus** and Anti-Malware: These software applications are used to detect, block, and remove malicious software (malware), such as viruses, worms, Trojans, and spyware.

9. **Encryption**: Encryption transforms data into a secure format that can only be decrypted with the proper encryption key. It is used to protect data both at rest (stored) and in transit (during transmission).

10. **Patch Management**: Regularly updating software and firmware with security patches is essential to fix known vulnerabilities and reduce the risk of exploitation.

Cyber Security Issues &Challenges

Today cyber security is the main component of the country's overall national security and economic security strategies. In India, there are so many challenges related to cyber security. With the increase of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured.

These security analysts face many Issues &Challenges related to cyber security such as securing confidential data of government organizations, securing the private organization servers, etc.

The recent important cyber security Issues &Challenges are described below:

1. **Ransomware Evolution** :- Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cyber security, data professionals, IT, and executives. Ransomware attacks are growing day by day in the areas of cybercrime. IT professionals and business leaders need to have a powerful recovery strategy against the malware attacks to protect their organization.

2. **Block chain Revolution** :- Block chain technology is the most important invention in computing era. It is the first time in human history that we have a genuinely native digital medium for peer-to-peer value exchange. The block chain is a technology that enables cryptocurrencies like Bitcoin. The block chain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust. It is difficult to predict what block chain systems will offer in regards to cyber security. The professionals in cyber security can make some educated guesses regarding block chain. As the application and utility of block chain in a cyber security context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cyber security approaches.

3. **IoT Threats** :-IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks. When IoT things were designed, it is not considered in mind about the used in cyber security and for commercial purposes. So every organization needs to work with cyber security professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the risk.

4. **AI Expansion** :- AI short form is Artificial intelligence. According to John McCarthy, father of Artificial Intelligence defined AI: "The science and engineering of making intelligent machines, especially intelligent computer programs." It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include speech recognition, Learning, Planning, Problem-solving, etc. The key benefits with AI into our cybersecurity strategy has the ability to protect and defend an environment when the malicious attack begins, thus mitigating the impact. AI take immediate action against the malicious attacks at a moment when a threats impact a business. IT business leaders and cybersecurity strategy teams consider AI as a future protective control that will allow our business to stay ahead of the cybersecurity technology curve.

5. **Serverless Apps Vulnerability :-** Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc. The serverless apps invite the cyber attackers to spread threats on their system easily because the users access the application locally or off-server on their device. Therefore it is the user responsibility for the security precautions while using serverless application. The serverless apps do nothing to keep the attackers away from our data. The serverless application doesn't help if an attacker gains access to our data through a vulnerability such as leaked credentials, a compromised insider or by any other means then serverless.

MODULE 02: CYBER CRIME AND CYBER LAW

Cyber Crime:

Any criminal activity carried out over the internet is referred to as cybercrime. Cybercrimes are crimes that involve criminal activities done through cyberspace by devices connected to the internet. At times, cybercrimes are also called 'computer crimes.' Most cybercriminals commit cybercrimes with mainly three motives- monetary, personal, or political.

The first incident of cybercrime was documented in 1973. A computer was used by a teller at a New York bank to pilfer over two million dollars. The first email spam was sent in 1978.

Though cybercrimes do not physically affect anyone, they tend to seriously harm the reputation, finances, and privacy of the targeted persons. Further, another crucial characteristic of cybercrimes is the determination of jurisdiction. Since the identity of the cybercriminal can be completely erased and mostly stays concealed in cyberspace, it is very difficult to identify him/ her.

As far as India is concerned, the term cybercrime is not defined under any legal provision. However, different types of cybercrimes are illustrated under the Information Technology Act, 2000. Further, certain provisions of the Indian Penal Code, 1860 (hereinafter referred to as 'the IPC') are applicable to various
Cybercrimes.

Meaning of Cyber Crime:

Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.
Cybercriminals or hackers who want to generate money, commit a majority of cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, pornographic material, and other unlawful data.

To make money, cybercriminals engage in a range of profit-driven criminal acts, including stealing and reselling identities, gaining access to financial accounts, and fraudulently utilizing credit cards to obtain funds.

Classification of cyber crimes

Cybercrimes can be classified under three heads, depending on the groups they are targeted. They are:

A. Cybercrimes against individuals,
B. Cybercrimes against organizations, and
C. Cybercrimes against society at large and government .

A. Cybercrimes against individuals:

Generally, ordinary individuals are the most vulnerable targets of cybercriminals. This is due to various reasons like lack of information, guidance, and cyber-security. The following are some of the main cybercrimes committed targeting individuals.

1. Cyberbullying:

Cyberbullying refers to bullying someone by threatening, harassing or embarrassing the victim using technology digital device. Generally, cyberbullying includes the following activities on the internet:

- Humiliating/embarrassing content posted online about the victim of online bullying,
- Hacking social media accounts
- Posting vulgar messages on social media
- Threatening the victim to commit any violent activity
- Child pornography or threatening someone with child pornography.

2. Cyberstalking

Browsing anyone's internet history or online activity, and sending obscene content online with the help of any social media, software, application, etc. to know about that particular person is called cyberstalking. Cyberstalkers take advantage of the inconspicuousness provided by the internet. They are generally not detectable by the victim, as it is very easy for cyberstalkers to open spam accounts just to stalk any person; once the stalker deletes the account, his/ her identity completely vanishes.

3. Cyber defamation

Cyber defamation means injuring the other person's reputation via the internet through social media, Emails etc. There are two types of Cyber defamation: **libel and slander.**

- ***Libel***: It refers to any defamatory statement which is in written form. For instance, writing
  defamatory comments on posts, forwarding defamatory messages on social media groups, etc. are a part of cyber defamation in the form of libel.
- ***Slander***: It refers to any defamatory statement published in oral form. For instance, uploading videos defaming someone on YouTube is a part of cyber defamation in the form of slander.

4. Phishing

Phishing refers to the fraudulent practice of sending emails under the pretext of reputable companies to induce individuals to reveal personal information, such as passwords, credit card numbers, etc., online. Phishing refers to the impersonation of a legitimate person and fraudulently stealing someone's data. Through phishing attacks, cybercriminals not only exploit innocent individuals but also spoil the reputation of well-known companies.

5. Cyber fraud

As the name suggests, cyber fraud refers to any act of fraud committed with the use of a computer. Any person who dishonestly uses the internet to illegal deceive people and gets personal data, communication, etc. with a motive to make money is called a cyber fraud. Examples of cyber fraud include sending emails containing fake invoices, sending fake emails from email addresses similar to the official ones, etc.

6. Cyber theft

Cyber theft is a type of cybercrime which involves the unauthorized access of personal or other information of people by using the internet. The main motive of the cyber criminals who commit cyber theft is to gather confidential data like passwords, images, phone numbers, etc. and use it as leverage to demand a lumpsum amount of money. The unauthorized transmission of copyrighted materials, trademarks, etc. over the internet is also a part of cyber theft. Cyber thefts are committed through various means, like hacking, email/ SMS spoofing, etc. Yahoo!, Inc. v. Akash Arora (1999), which was one of the initial cases related to cyber theft in India. In this case, the defendant was accused of using the trademark or domain name ‘yahooindia.com,’.

7. Spyware

Spyware is a type of malware or malicious software, when it is installed, it starts accessing and computing the other person’s device without the end user’s knowledge. The primary goal of this software is to steal credit card numbers, passwords, One-Time Passwords (OTPs), etc.

B. Cybercrimes against organizations

The cyber crimes mainly targeting individuals may help cybercriminals get only a meagre amount of ransom, depending on the financial status of the targeted individuals. On the other hand, cyber-attacking large companies or organisations can help them get their hands on extremely confidential data of both private and public institutions or entities. Cyber attacks on organizations are generally launched on a large scale to get a lump sum amount of ransom. Since such attacks drastically damage the companies’ daily operations, most companies try to resolve them as fast as possible. The following are the kinds of cyber crimes launched targeting organizations.

1. Attacks by virus

A computer virus is a kind of malware which connects itself to another computer program and can replicate and expand when any person attempts to run it on their computer system. For example, the opening of unknown attachments received from malicious emails may lead to the automatic installation of the virus on the system in which it is opened. These viruses are extremely dangerous, as they can steal or destroy computer data, crash computer systems, etc. The attackers program such malicious viruses to get hold of organizations’ official or confidential data. The illegally retrieved data is then used as leverage to extort ransom from the organizations.

2. Salami attack

It is one of the tactics to steal money, which means the hacker steals the money in small amounts. The damage done is so minor that it is unnoticed. Generally, there are two types of Salami attacks- In Salami slicing, the attacker uses an online database to obtain customer information, such as bank/credit card details. Over time, the attacker deducts insignificant amounts from each account. These sums naturally add up to large sums of money taken from the joint accounts invisibly.

3. Web Jacking

Web Jacking refers to the illegal redirection of a user’s browser from a trusted domain’s page to a fake domain without the user’s consent. By using the method of Web Jacking, people visiting any well-known or reliable website can be easily redirected to bogus websites, which in turn lead to the installation of malware, leak of personal data, etc. Web jackers intend to illegally collect confidential information of users by enticing them to click on any link which may seem genuine at the first glance.

4. Denial of Service Attack

Denial of Service Attack or DoS, is a cyber attack on computer devices or systems, preventing the legal users or access of the system from accessing them. The attackers generally attack systems in such a manner by trafficking the targeted system until it ultimately crashes. DoS attacks cost millions of dollars to the corporate world, as it curbs them from using their own systems and carrying out their activities. The attack may be also used to incorporate ransomware into corporate systems.

5. Data diddling

Data diddling is a cybercrime which involves the unauthorized alteration of data entries on a computer. It may be done either before or during the entry of such data. It is generally committed by way of computer virus attacks. At times, to conceal the alteration, the altered data is changed to its original data after retrieving the required information. Usually, the strategic or statistical data of large companies.

C. Cyber crimes against society at large

Apart from the cybercrimes committed targeting individuals in society, various other cyber attacks are launched against the community at large. Such cybercrimes may be aimed either against any particular section of society or the entire country. The following are a few types of cybercrimes against the community at large.

1. Cyber pornography

As per Merriam-Webster Dictionary, pornography is the depiction of erotic behaviour (as in pictures or writing) intended to cause sexual excitement. Accordingly, cyber pornography refers to using the internet to display, distribute, import, or publish pornography or obscene materials.

The following activities are punishable;

- Uploading pornographic content on any website, social media, etc. where third parties may access it.
- Transmitting obscene photos to anyone through email, messaging, social media, etc.

2. Cyber terrorism

Cyber terrorism means using cyberspace to hurt the general public and damage the integrity and sovereignty of any country. Cyber terrorism is generally carried out in the following ways:

- Hacking government-owned systems of the target country and getting confidential information.
- Destructing and destroying government databases and backups by incorporating viruses or malware into the systems.
- Disrupting government networks of the target nation.
- Distracting the government authorities and preventing them from focusing on matters of priority.

3. Cyber Espionage

Cyber espionage refers to the unauthorized accessing of sensitive data or intellectual property for economic, or political reasons. It is also called ‘cyber spying’. In most cases of cyber espionage, spies in the form of hackers are deliberately recruited to launch cyber attacks on the government systems of enemy nations to stealthily collect confidential information. The cross-border exposure of sensitive data related to any country can continue as long as it stays undetected.

The information gathered through cyber espionage is then used by the gathering country to either combat or launch military or political attacks on the enemy country. Generally, the following data are gathered through cyber espionage:

- Military data
- Academic research-related data
- Intellectual property
- Politically strategic data, etc.
-

<u>Common Cyber Crimes:</u>

A. Cyber Crime targeting computers and mobiles:

In India, cyber crime has become a major concern in recent years, with more and more people using computers and mobiles for various purposes. Criminal activities that are committed through the use of computers, networks, or other digital devices. Some of the common types of cyber crime in India include hacking, phishing, identity theft, online fraud, cyberstalking, and cyberbullying.

Cyber criminals often target computers and mobiles to gain access to sensitive information such as passwords, bank account details, and personal data. Cyber crime can have serious consequences for individuals and businesses, including financial losses, reputational damage, and even physical harm.

Example for Security threats:

a. Web-Based Threats – These types of threats happen when people visit sites that appear to be fine on the front-end but in reality, automatically download malicious content onto the mobile devices. Also, many mobile applications continue to sync their data in the background which poses a threat. These threats usually go unnoticed by the users.

b. Phishing Through Links : Some legitimate-looking links are sent through messages, emails, or social media platforms. They extract personal information by tricking with several schemes. It is not possible to categorize them as real or fake as they copy the original website.

c. Forced Downloads : When you visit a page through anonymous links, it automatically directs you to the download page. This method is called drive-by downloads.

d. Physical Threats – These threats happen when someone physically tries to access your device. When you lose your mobile, or it is stolen there is a possibility for physical threats. Mobile devices carry your transactional data as well as has connected applications to your bank accounts, which is a threat to your privacy breach.

e. No Password Protection : With keeping all measures to secure your data, it is surprising to know that some people find it difficult to use a password on their devices, or they rather use a password that is easy to crack by hackers. This leads to physical threats.

f. Encryption : While using carrier networks they generally provide good encryption while accessing servers. But while accessing some client and enterprise servers they are explicitly managed. They are not end-to-end encrypted which can lead to physical threats.

g. Network-Based Threats – Mobile network includes both Cellular and Local network support such as Bluetooth and Wi-Fi. These are used to host network threats. These threats are especially dangerous as the cyber-criminals can steal unencrypted data while people use public WiFi networks.

h. Public WiFi : While we are using our devices for every task, at public places we are provided with public open WiFi which tends to be legitimate while they are controlled by hackers which results in data leakage.

i. Network Exploits : Network exploits are due to the vulnerabilities in the operating system in your mobile devices. Once this software is connected to the network they are capable of installing malware onto the device without being known.

j. Application-Based Threats – Websites available for software downloads are home to these threats. They tend to be genuine software but in fact are specially designed to carry malicious activities.

k. **Malware :** Malware is designed to send unwanted messages to recipients and further use your personal and business information by hacking your devices.

l. **Spyware** : They are the software that are used to collect specific information about an organization or person which later can be used for fraud and identity threats.

Steps to prevent from Security Threats –

- Prefer using communication apps that encrypt data transfers.
- Update your device software regularly to ensure protection against spyware threats.
- Create unique passwords for different accounts created while using mobile devices.
- Delete the non-active apps to limit the threat to data access and privacy.
- Categories your applications under Blacklist and Whitelist.
- Check for apps accessing location and storage.
- Do not allow forced downloads from browser.
- Check on security that stops sharing of network unnecessary.
- Do not add your data to public servers.

To prevent cyber crime, it is important to take measures such as using strong passwords, keeping software up-to-date, avoiding suspicious emails and websites, and being cautious about sharing personal information online.The Indian government has also taken steps to combat cyber crime by setting up specialized agencies such as the Cyber Crime Investigation Cell (CCIC) and the National Cyber Security Coordination Centre (NCSC). However, there is still a need for greater awareness and education about cyber security among the general public, especially in rural areas where internet usage is increasing rapidly.

B. Cyber Crime against women and children:

Cyber crime against women refers to any criminal activity that targets women using digital technology or the internet.

- One common form of cyber crime against women is online harassment or cyberbullying. This can include sending threatening or abusive messages, spreading rumors or false information, or posting explicit content without consent.
- Revenge porn is another prevalent form of cyber crime targeting women. It involves the non-consensual sharing of intimate images or videos online, often with the intention to shame, blackmail, or harass the victim.
- Online stalking is also a significant concern for women. This involves someone obsessively monitoring a person's online activities, gathering personal information, and potentially using it to harm or intimidate them.

- Phishing scams targeting women are on the rise. These scams involve tricking individuals into revealing sensitive information such as passwords, credit card details, or social security numbers through deceptive emails, websites, or messages.
- Identity theft is another cyber crime that can disproportionately affect women. Criminals may steal personal information to commit fraud in the victim's name, leading to financial loss and damage to their reputation.
- Online grooming is a serious concern for young girls and teenagers. Predators may use social media platforms and other online spaces to build trust with their victims and exploit them for sexual purposes.
- Women are also vulnerable to online fraud schemes such as romance scams. Criminals create fake profiles on dating websites or social media platforms to establish romantic relationships with unsuspecting victims and then manipulate them into sending money.

  It is important for women to be aware of these risks and take precautions when using digital technology. This includes regularly updating passwords, being cautious about sharing personal information online, and reporting any instances of cyber crime to the appropriate authorities.

Cyber crime against children

Cyber crime against children refers to any criminal activity that targets or exploits children using digital technology.

- One common form of cyber crime against children is online child exploitation, which includes child pornography, grooming, and sexual exploitation.
- Grooming is the process by which an adult builds an emotional connection with a child to gain their trust for the purpose of sexual abuse or exploitation.
- Child pornography involves the production, distribution, or possession of sexually explicit images or videos of children.
- Sextortion is another form of cyber crime where perpetrators coerce children into providing sexually explicit images or videos and then use those materials to blackmail and exploit them further.
- Online bullying and harassment are also prevalent forms of cyber crime against children. This includes cyberbullying through social media platforms, online forums, or messaging apps.
- Identity theft is another concern as criminals may steal a child's personal information to commit fraud or other illegal activities.

  It's important for parents and guardians to educate themselves and their children about online safety measures such as privacy settings, safe internet browsing habits, and responsible social media usage. Reporting any suspicious activities or incidents to law enforcement authorities is crucial in combating cyber crime against children. Governments and organizations around the world are working together to develop laws and regulations that protect children from cybercrime.

Cyber Crime Prevention against Women and Children (CCPWC) Scheme is to have an effective mechanism to handle cybercrimes against women and children in the country. The main Components of the CCPWC Scheme,

- Online Cybercrime reporting Unit
- Forensic Unit
- Capacity Building Unit
- Research & development Unit
- Awareness Creation Unit

C. Cyber Financial Frauds:

Cyber financial frauds involve unauthorized access, theft, or manipulation of financial data or transactions using digital platforms.

Types of financial fraud: Common types include phishing scams, identity theft, credit card fraud, online banking fraud, and investment scams.

1. Phishing: This is a technique where fraudsters impersonate legitimate entities to trick individuals into revealing sensitive information like passwords or credit card details.

2. Identity theft: It occurs when someone steals personal information to impersonate another individual and carry out fraudulent activities.

3. Online banking fraud: Criminals may exploit vulnerabilities in online banking systems to gain unauthorized access, transfer funds, or conduct fraudulent transactions.

4. Investment scams: These frauds involve false promises of high returns or fictitious investment opportunities to deceive individuals into providing money.

Prevention: To protect against cyber financial frauds, individuals should be cautious while sharing personal information online, use strong and unique passwords, regularly monitor financial accounts, and be vigilant of suspicious emails or websites.

D. Social Engineering Attacks:

Social engineering attacks manipulate human psychology to deceive individuals into divulging sensitive information or performing actions that benefit the attacker.
Social engineering attacks often involve impersonation, pretexting, baiting, phishing, or tailgating to gain trust and exploit vulnerabilities.

1. Impersonation: Attackers may pretend to be someone trustworthy, like a colleague, IT support, or a customer service representative, to trick individuals into revealing information or granting access.
2. Pretexting: This technique involves creating a fabricated scenario or pretext to manipulate victims into providing sensitive information or performing certain actions.
3. Baiting: Attackers offer something enticing, like a free USB drive or a gift card, to trick individuals into taking actions that compromise their security.
4. Phishing: Phishing is a social engineering technique where attackers use deceptive emails or websites to trick individuals into revealing personal information.

Prevention: Individuals can protect themselves from social engineering attacks by being cautious of requests for sensitive information, verifying the identity of individuals before sharing information, avoiding clicking on suspicious links or downloading unknown files, and staying informed about common scam tactics.

E. Malware Attacks and Ransomware Attacks:

i. Malware Attacks:

Malware refers to malicious software designed to infiltrate and damage computer systems, steal data, or gain unauthorized access.

Types of malware: Common types include viruses, worms, Trojans, spyware, and adware.

1. Viruses: Viruses attach themselves to legitimate programs or files and spread by replicating themselves. They can cause damage to files, slow down systems, or even render them unusable.
2. Worms: Worms are self-replicating malware that spread over networks, exploiting vulnerabilities in computer systems and causing disruption.
3. Trojans: Trojans appear as legitimate software but contain hidden malicious code. They can give attackers unauthorized access to a system or steal sensitive data.
4 Spyware: Spyware secretly collects information about a user's activities, such as browsing habits or keystrokes, and sends it to a third party without the user's consent.
5. Adware: Adware displays unwanted advertisements, often in the form of pop-ups, and can collect user information for targeted advertising purposes.

ii. Ransomware Attacks:

Ransomware is a type of malware that encrypts a victim's files or locks them out of their systems, demanding a ransom in exchange for restoring access.

- **Encryption:** Ransomware uses strong encryption algorithms to render files inaccessible, making them useless until a decryption key is provided.

- **Payment:** Attackers typically demand payment in cryptocurrencies like Bitcoin to make it difficult to trace the transactions.
- **Consequences:** Ransomware attacks can lead to significant financial losses, data breaches, operational disruptions, and reputational damage for individuals and organizations.

Prevention: Regularly updating software, using strong and unique passwords, employing robust security solutions, and regularly backing up data are key preventive measures against ransomware attacks.

F. Zero-Day and Zero-Click Attacks:

- **Zero-Day Attacks:**

Zero-day attacks are cyber attacks that exploit software vulnerabilities that are unknown to the software vendor or have not been patched yet.

- **Vulnerabilities:** Zero-day vulnerabilities can exist in operating systems, software applications, web browsers, or other software components.
- **Exploitation:** Attackers discover and exploit these vulnerabilities before the software developers become aware of them or release a patch to fix them.
- **Damage Potential:** Zero-day attacks can have severe consequences as there is no known defense or protection against them at the time of their discovery.
- **Stealthy Nature:** Zero-day attacks are often highly targeted and designed to stay undetected by security measures and traditional security solutions.

Prevention and Mitigation: Organizations and software vendors need to have strong vulnerability management practices, including regular security updates, threat intelligence, and proactive monitoring to detect and respond to zero-day attacks.

- **Zero-Click Attacks**:

Zero-click attacks refer to cyber attacks that exploit vulnerabilities in software or devices without any interaction or action required from the user.

- **Delivery Methods:** Zero-click attacks can be delivered through various means, such as malicious emails, instant messaging apps, or even through network traffic.
- **Exploitation:** Cybercriminals take advantage of security flaws in software or devices to execute malicious code and compromise systems without the victim's knowledge.
- **Targeted Exploitation:** Zero-click attacks often target specific software versions or device configurations, making them more challenging to defend against.

- **Sophistication:** Zero-click attacks are highly sophisticated, relying on techniques like remote code execution, memory corruption, or privilege escalation to gain control over the targeted system.

Prevention and Mitigation: To protect against zero-click attacks, it is crucial to keep software and devices up to date with the latest security patches, use robust security solutions, and employ network segmentation to limit the potential impact of an attack.

Modus operandi of cyber criminals:

1. **Theft:** Cyber criminals often engage in identity theft to impersonate individuals for fraudulent activities. They may gather personal information through phishing emails, data breaches, or social engineering techniques.

1. **Phishing:** Phishing is a common tactic used by cyber criminals to trick individuals into revealing sensitive information such as passwords, credit card numbers, or login credentials. They often impersonate trusted entities via email, text messages, or fake websites.
2. **Malware Distribution:** Cyber criminals may distribute malware through various means, including malicious email attachments, infected websites, or software downloads. Once installed, the malware can gain unauthorized access, steal data, or cause other malicious activities.
3. **Ransomware Attacks:** Ransomware attacks involve encrypting victims' files or systems and demanding a ransom for their release. Cyber criminals leverage social engineering, email attachments, or exploit software vulnerabilities to deliver and execute ransomware.
4. **Data Breaches:** Cyber criminals target organizations to gain unauthorized access to sensitive data, including personal information, financial records, or intellectual property. They may exploit vulnerabilities in networks, weak passwords, or use social engineering techniques to infiltrate systems.
5. **Online Scams:** Cyber criminals often engage in online scams to deceive individuals into providing money or sensitive information. Common examples include romance scams, lottery scams, investment scams, or fake tech support scams.
6. **Credential Stuffing:** In credential stuffing attacks, cyber criminals use stolen usernames and passwords from data breaches to gain unauthorized access to other online accounts of victims who reuse their credentials.
7. **Business Email Compromise (BEC):** BEC attacks involve cyber criminals impersonating a high-ranking executive or a trusted party within an organization to trick employees into transferring funds or disclosing sensitive information.
8. **Cryptojacking**: Cyber criminals may exploit victims' computing resources to mine crypto currencies without their knowledge or consent. They achieve this by infecting systems with malware that runs in the background.
9. **Dark Web Activities:** Cyber criminals utilize the anonymity of the dark web to engage in various illicit activities, including the sale of stolen data, hacking tools, drugs, weapons, and more.

Remedial and mitigation measures:

Reporting Cyber Crimes:

1. **Reporting Channels:** Cyber crimes should be reported to the appropriate authorities, such as local law enforcement agencies, national cybercrime units, or dedicated cybercrime reporting portals established by governments or cybersecurity organizations.
2. **Evidence Preservation:** It is crucial to preserve any evidence related to the cyber crime, including screenshots, emails, or system logs, as it can aid in the investigation and prosecution of the offenders.
3. **Provide Details:** When reporting a cyber crime, provide as many details as possible, including the nature of the incident, any suspicious emails or messages received, relevant IP addresses, and timestamps of the events.

Remedial Measures:

1. **Incident Response:** In the event of a cyber crime, organizations should have an incident response plan in place to quickly identify, contain, and mitigate the impact of the attack. This includes isolating affected systems, restoring backups, and applying patches or security updates.
2. **Forensic Investigation:** Engaging professional forensic investigators can help identify the source and extent of the cyber crime, gather evidence, and aid in legal proceedings.
3. **Data Recovery:** If data is compromised or encrypted due to a cyber attack, organizations should have backups in place to restore affected systems and minimize data loss.

Mitigation Measures:

1. **Strong Security Practices:** Implement robust security measures, such as firewalls, antivirus software, and intrusion detection and prevention systems, to protect against cyber threats.
2. **Regular Updates and Patching:** Keep software, operating systems, and firmware up to date with the latest security patches to mitigate vulnerabilities that cyber criminals may exploit.
3. **Employee Education:** Provide cybersecurity awareness and training programs to employees to educate them about common cyber threats, phishing techniques, and safe online practices.
4. **Multi-factor Authentication (MFA):** Implement MFA wherever possible to add an extra layer of security, making it harder for cyber criminals to gain unauthorized access to accounts or systems
5. **Data Encryption:** Encrypt sensitive data, both in transit and at rest, to ensure that even if it is intercepted or stolen, it remains unreadable and unusable for unauthorized individuals.

6. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address any weaknesses or potential entry points for cyber criminals.

Legal perspective of cybercrime in India:

1. Information Technology Act, 2000: In India, cybercrime is primarily governed by the Information Technology Act, 2000 (IT Act). This law was established to address various cyber offenses and provide a legal framework for electronic transactions, digital signatures, and data protection.

2. Cyber Crimes: The IT Act defines several cyber offenses, including unauthorized access to computer systems, data theft, identity theft, hacking, cyberstalking, cyberbullying, phishing, spreading of malicious software, and more.

3. Penalties and Punishments: The IT Act prescribes penalties and punishments for various cyber crimes. Offenders can face imprisonment, fines, or both, depending on the severity of the offense. The punishment can range from a few months to several years, depending on the specific cybercrime committed.

4. Cyber Crime Investigation Cells: India has established cyber crime investigation cells at both national and state levels, such as the Cyber Crime Investigation Cell (CCIC) and Cyber Crime Police Stations. These specialized units are responsible for investigating and prosecuting cyber criminals.

5. Reporting Cyber Crimes: Individuals or organizations can report cyber crimes to the local police station or the nearest cyber crime investigation cell. Additionally, the Ministry of Home Affairs has established the Cyber Crime Reporting Port(www.cybercrime.gov.in) for reporting cyber crimes online.

6. Digital Evidence: The IT Act recognizes the admissibility of electronic records as evidence in court proceedings. Digital evidence, such as emails, chat logs, or computer forensic reports, can be submitted and considered during the investigation and trial of cyber crime cases.

7. International Cooperation: India participates in international efforts to combat cybercrime. It has signed agreements and treaties with several countries to facilitate cooperation in investigating and prosecuting cyber criminals across borders.

8. **Amendments and Updates:** The IT Act has undergone amendments over the years to address emerging cyber threats and strengthen cybercrime provisions. For example, the Information Technology (Amendment) Act, 2008 introduced additional provisions to tackle cyber terrorism, data privacy, and intermediary liability. It is important to consult with legal professionals or refer to official sources for comprehensive and up-to-date information on the legal aspects of cybercrime in India.

Punishment For Cyber Crime

In order to control the rise in cybercrime cases, specific punishments are imposed under the India Penal Code, 1860 and the Information Technology Act 2000. Below are the Sections that identify the punishments imposed on an individual committing cybercrime.

I. Under The Indian Penal Code

- **Section 292**: This Section deals with the sale of obscene materials either in the form of a book, paper, drawing, writing, pamphlet, painting, etc., or sexually explicit acts harming the surroundings. An individual or a group involved in such an offence is punished with imprisonment and a fine. On a first conviction, the punishment is imprisonment for two years and Rs. 2000 fine whereas on a second or subsequent conviction, the punishment is imprisonment for a term that may extend to five years and Rs. 5,000 fine.

- **Section 354C**: It deals with the offence of voyeurism, where an individual watches or captures, or publicizes the image of a woman engaged in a private Act without her consent. Under the provisions of this Section of IPC, such an offender or criminal is punished with imprisonment of 1 to 3 years and 3 to 7 years for first-time and second-time offenders respectively.

- **Section 354D**: This section deals with stalking both physical and cyberstalking. As per this Section, "Any man who follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman or monitors the use by a woman of the interest, email or any other form of electronic communication, commits the offence of stalking." An offender will be punished with imprisonment that may extend to three years for the first offender and five years for the second offender.

- **Section 379**: If a person commits theft either electronically or physically, he or she will be punished under the provisions of this Section. It states that "whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years or with fine, or with both."

- **Section 411**: If a person receives any stolen property such as a computer, mobile phone, or data then he or she will be punished for three years or fine or both.

- **Section 419**: This Section deals with fraud such as email phishing or committing the crime of password theft for impersonating and collecting data for personal benefit. According to this Section, "Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both."

- **Section 420:** It also deals with fraud cases especially 'cheating and dishonestly inducing delivery of property'. Whoever dishonestly induces one's property, "the person deceived to deliver any property to any person r to make or alter or destroy the whole or any part of a valuable security… and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine."

- **Section 465**: The punishment for forgery, email spoofing, preparation of false documents, etc., are dealt with in Section 465 of the IPC. It states that anyone who commits forgery should be punished with imprisonment extending to two years, a fine, or both.

- **Section 468**: This Section deals with the forgery of documents or electronic records for committing other serious crimes such as cheating. As per the provisions of this Section, whoever commits such a crime shall be punished with imprisonment which may extend to seven years with a fine. It is a non-bailable offence.

- **Section 469**: According to this Section, forgery for the purpose of harming reputation is a punishable offence. Section 469 states that "Whoever commits forgery, 1[intending that the document or electronic record forged] shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."

- **Section 500**: It states that "Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both." This means that any individual who sends abusive messages or defamatory content via email or any other electronic form is dealt with as per the provisions of Section 500 of the IPC.

- **Section 504**: If anyone insults, tries to provoke, or threatens another person with the motive of affecting their peace via any electronic form of communication will be attracted by Section 504 of the IPC. As per its provisions, an individual involved in such an offence is punished with imprisonment which may extend to two years or a fine or both.

- **Section 506**: This Section deals with the 'punishment for criminal intimidation'. If an individual tries to intimidate another individual shall be punished with imprisonment which may extend to two years or a fine or both. This criminal intimidation can either be physical or through electronic means.

- **Section 509**: It states that "Whoever intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both."

II. Under the Information Technology Act

- **Section 43 (a-h)**: It covers 8 instances (a-h) where "If any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network,"

- **Section 65**: 'Tampering with computer source documents' is an offence that is punishable under Section 65 of the Information Technology Act. It states that "Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system, or computer network when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both".

- **Section 66 (A-F)**: This Section deals with punishments for computer-related offences such as sending offensive messages, receiving stolen computer resources, identity theft, cheating by impersonation, violation of privacy, and cyber-terrorism, punishments may extend to three years imprisonment or a fine of up to 5 lakhs, or both.

- **Section 67 (A-B)**: This Section of the Information Technology Act deals with the punishments related to the publishing or transmitting of obscene material containing sexually explicit act, etc., in an electronic format. The punishment on the first conviction is imprisonment which may extend to three years and with a fine extending to 5 lakh rupees. The punishment on the second conviction is imprisonment which may extend to five years and with a fine extending to 10 lakh rupees.