UNIT-5 (INTRODUCTION TO FORENSIC SCIENCE AND LAW)

Ashna Bhatia
Ph.D. Scholar
SFS, NFSU, Gandhinagar

COMPUTER AND ITS FUNCTIONALITIES

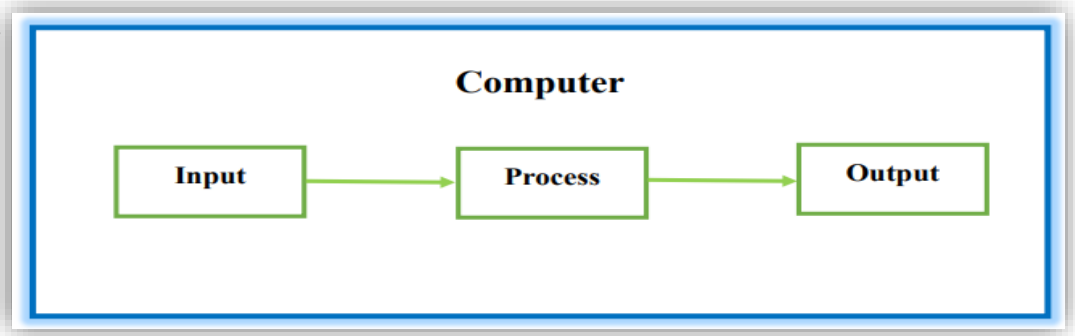
A **computer** is an advanced electronic device that takes raw data as input from the user and processes it under the control of a set of instructions (called **program**), produces a result (**output**), and saves it for future use.

There are three basic functionalities of a Computer System and they are:

1. *Input*
2. *Process*
3. *Output*

But in a very broad sense, any digital computer carries out the following five functions:

Step 1 - Takes data as input.
Step 2 - Stores the data/instructions in its memory and uses them as required.
Step 3 - Processes the data and converts it into useful information.
Step 4 - Generates the output.
Step 5 - Controls all the above four steps.



ADVANTAGES OF COMPUTER

1) High Speed

- The computer is a very fast device.
- It is capable of performing calculations of very large amounts of data.
- The computer has units of speed in microseconds, nanoseconds, and even picoseconds.
- It can perform millions of calculations in a few seconds as compared to a man who will spend many months performing the same task.

2) Accuracy

- In addition to being very fast, computers are very accurate.
- The calculations are 100% error-free.
- Computers perform all jobs with 100% accuracy provided that the input is correct.

3) Storage Capability

- Memory is a very important characteristic of computers.
- A computer has much more storage capacity than human beings.
- It can store large amounts of data.
- It can store any type of data such as images, videos, text, audio, etc.

4) Diligence

- Unlike human beings, a computer is free from monotony, tiredness, and lack of concentration.
- It can work continuously without any error and boredom.
- It can perform repeated tasks with the same speed and accuracy.

5) Versatility

- A computer is a very versatile machine.
- A computer is very flexible in performing the jobs to be done.
- This machine can be used to solve problems related to various fields.
- At one instance, it may be solving a complex scientific problem and the very next moment it may be playing a card game.

6) Reliability

- A computer is a reliable machine.
- Modern electronic components have long lives.
- Computers are designed to make maintenance easy.

7) Automation

- A computer is an automatic machine.
- Automation is the ability to perform a given task automatically. Once the computer receives a program i.e., the program is stored in the computer memory, then the program and instruction can control the program execution without human interaction.

8) Reduction in Paper Work and Cost

- The use of computers for data processing in an organization leads to a reduction in paperwork and results in speeding up the process.
- As data in electronic files can be retrieved as and when required, the problem of maintenance of a large number of paper files gets reduced.
- Though the initial investment for installing a computer is high, it substantially reduces the cost of each of its transactions.

DISADVANTAGES OF COMPUTER

1) No I.Q.

- A computer is a machine that has no intelligence to perform any task.
- Each instruction has to be given to the computer.
- A computer cannot make any decision on its own.

2) Dependency and Reduced Productivity:

- It functions as per the user's instruction, thus it is fully dependent on humans.
- Overreliance on computers can sometimes reduce productivity, especially if users get distracted by social media, gaming, or other online content.

3) Environmental Impact

- The operating environment of the computer should be dust-free and suitable.
- Computer manufacturing, energy consumption, and electronic waste contribute to environmental degradation.

4) No Feeling

- Computers have no feelings or emotions.
- It cannot make judgments based on feeling, taste, experience, and knowledge, unlike humans.

5) Health Issues:

- Prolonged computer use can lead to eye strain, back pain, and other physical health problems, often referred to as "computer vision syndrome" or musculoskeletal issues.

6) Privacy and Security Risks:

- Computers can be vulnerable to hacking, phishing, malware, and other security threats, which can lead to data theft or unauthorized access to sensitive information.

7) Social Isolation:

- Excessive computer use can lead to decreased social interaction and isolation, particularly when it replaces face-to-face communication.

8) High Initial and Maintenance Costs:

- Computers and their accessories can be expensive to purchase, maintain, and upgrade.

9) Data Loss:

- Computers can experience hardware failures, crashes, or accidental deletions, leading to the potential loss of important data.

10) Cyberbullying and Negative Online Content:

- Easy access to computers can expose users, especially young ones, to cyberbullying, inappropriate content, and misinformation.

11) Reduces Cognitive Skills:

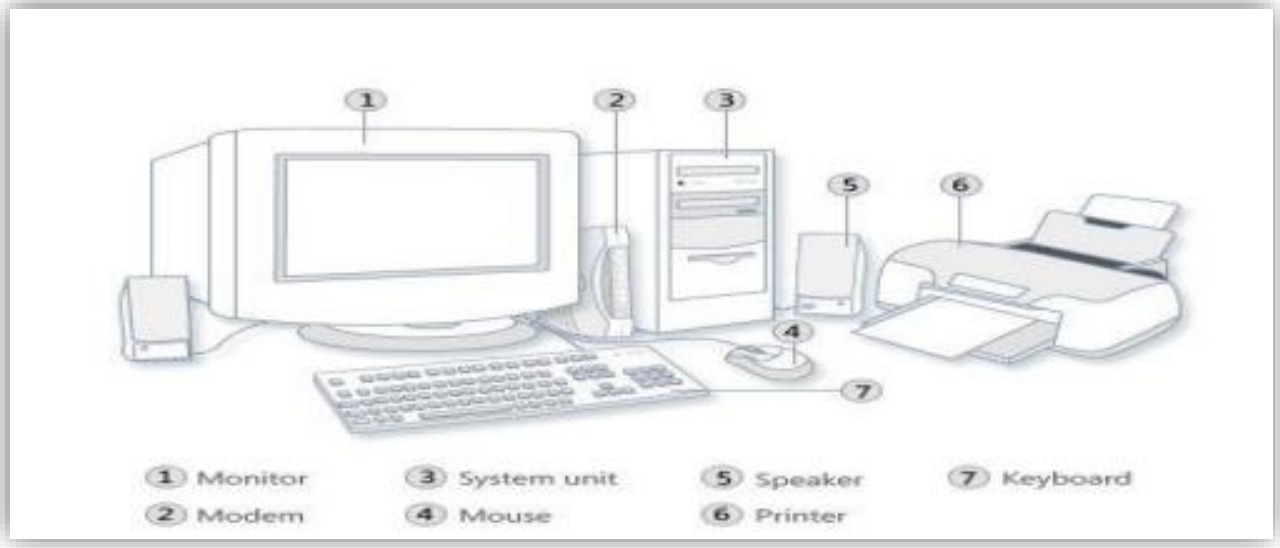
- Reliance on computers for calculations, spell-checking, and other tasks can reduce critical thinking, problem-solving, and memory skills over time.

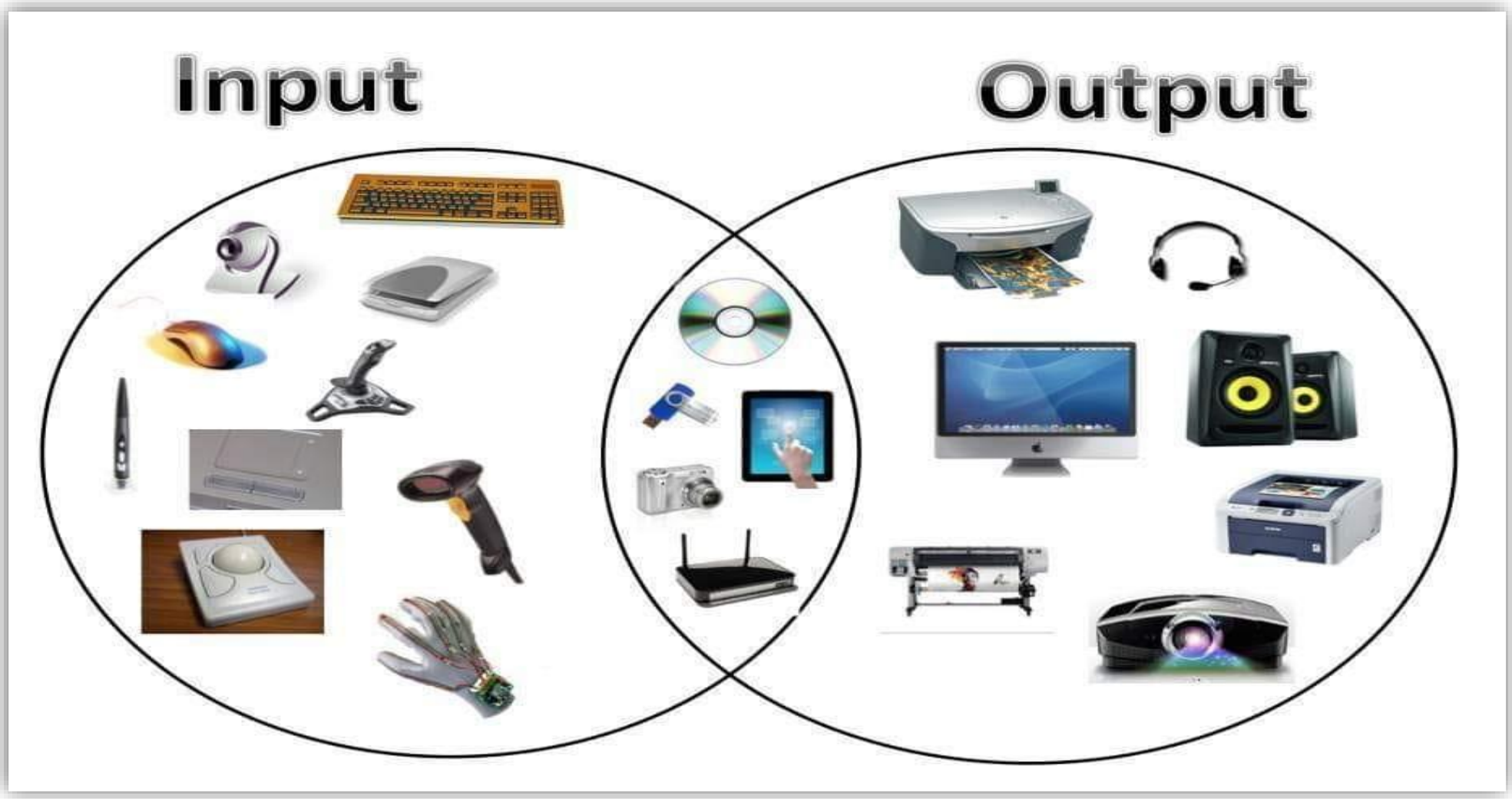
COMPONENTS OF A COMPUTER

Computers consist of **HARDWARE AND SOFTWARE.**

Hardware:

Computer hardware is the collection of physical elements that constitute a computer system. Computer hardware refers to the physical parts or components of a computer such as a monitor, mouse, keyboard, computer data storage, hard drive disk (HDD), system unit (graphic cards, sound cards, memory, motherboard and chips), etc. all of which are physical objects that can be touched.





INPUT DEVICES AND OUTPUT DEVICES

Input Devices:

An input device is any peripheral (a piece of computer hardware equipment to provide data and control signals to an information processing system such as a computer or other information appliance. Input device Translate data from a form that humans understand to one that the computer can work with. The most common are keyboard and mouse.

Examples of Input Devices –

Keyboard	Graphic Tablets	Electronic Whiteboard
Mouse (Pointing Device)	Cameras	Remote Control
Microphone	Pen Input	Digital Camera
Touch Screen	Video Capture Hardware	Light Pens
Scanner	Trackballs	Joystick
Webcam	Barcode Reader	Gamepad
Touchpads	MIDI Keyboard	

Note: The most commonly used keyboard is the QWERTY keyboard. Generally, standard Keyboard has 104 keys.

Output Devices:

An output device is any piece of computer hardware equipment used to communicate the results of data processing carried out by an information processing system (such as a computer) which converts the electronically generated information into human-readable form.

Examples of Input Devices –

Monitor	LCD Projection Panels	Printers (All Types)
Computer Output Microfilm (COM)	Plotters	Speakers
Projector		

Note:

Basic types of monitors are:

A. Cathode Ray Tube (CRT)
B. Liquid Crystal Displays (LCD)
C. Light-emitting diode (LED)

Printer types:

A. Laser Printer
B. Ink Jet Printer
C. Dot Matrix Printer

Central Processing Unit (CPU):

A CPU is the brain of a computer. It is responsible for all functions and processes. Regarding computing power, the CPU is the most important element of a computer system.

The CPU is comprised of three main parts :

❖*Arithmetic Logic Unit (ALU):* Executes all arithmetic and logical operations. Arithmetic calculations like addition, subtraction, multiplication and division. Logical operations like comparing numbers, letters, or special characters.

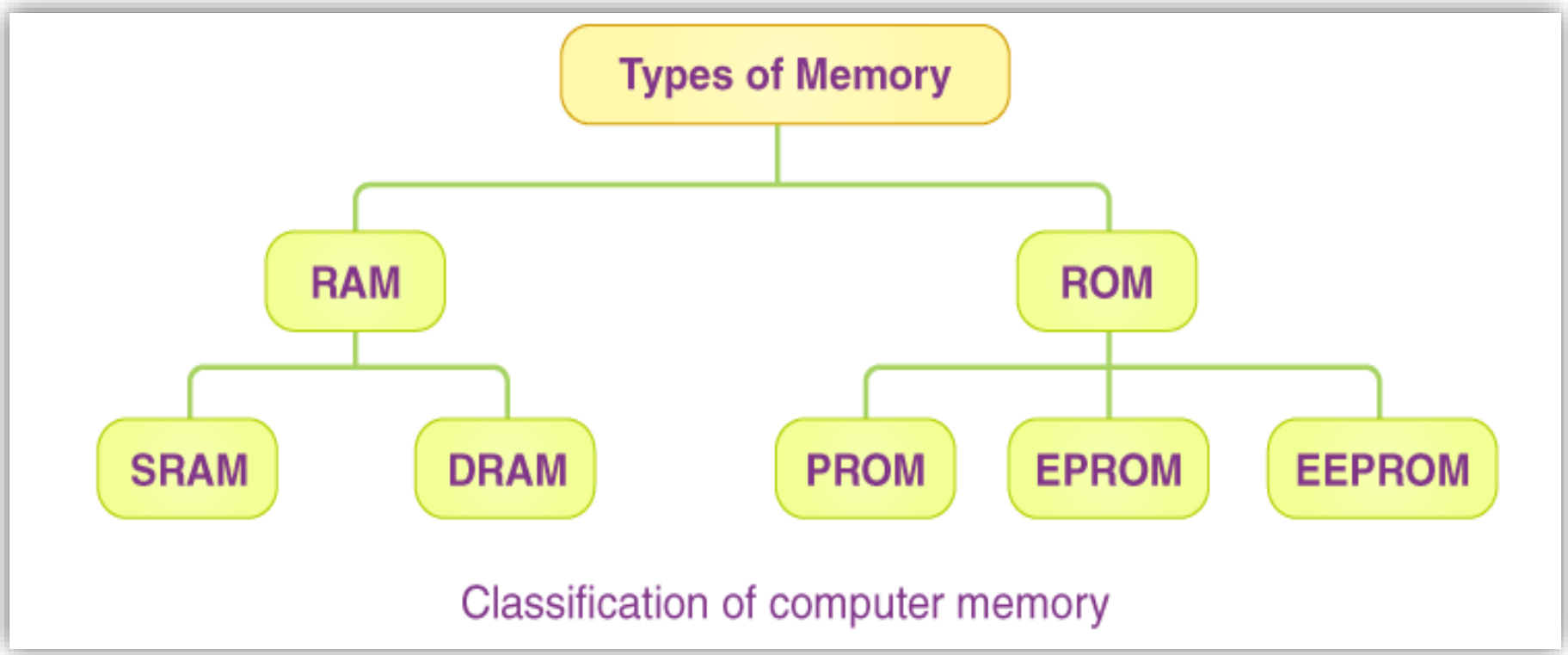
❖*Control Unit (CU):* controls and co-ordinates computer components.

1. Read the code for the next instruction to be executed.
2. Increment the program counter so it points to the next instruction.
3. Read whatever data the instruction requires from cells in memory.
4. Provide the necessary data to an ALU or register.
5. If the instruction requires an ALU or specialized hardware to complete, instruct the hardware to perform the requested operation.

❖*Registers:* Stores the data that is to be executed next, “very fast storage area”.

Primary Memory:

1. *RAM (Random Access Memory):* RAM is a memory scheme within the computer system responsible for storing data temporarily so that it can be promptly accessed by the processor as and when needed. It is volatile in nature, which means that data will be erased once the supply to the storage device is turned off. RAM stores data randomly and the processor accesses these data randomly from the RAM storage. RAM is considered "random access" because you can access any memory cell directly if you know the row and column that intersect at that cell.



Classification of computer memory

Secondary Memory:

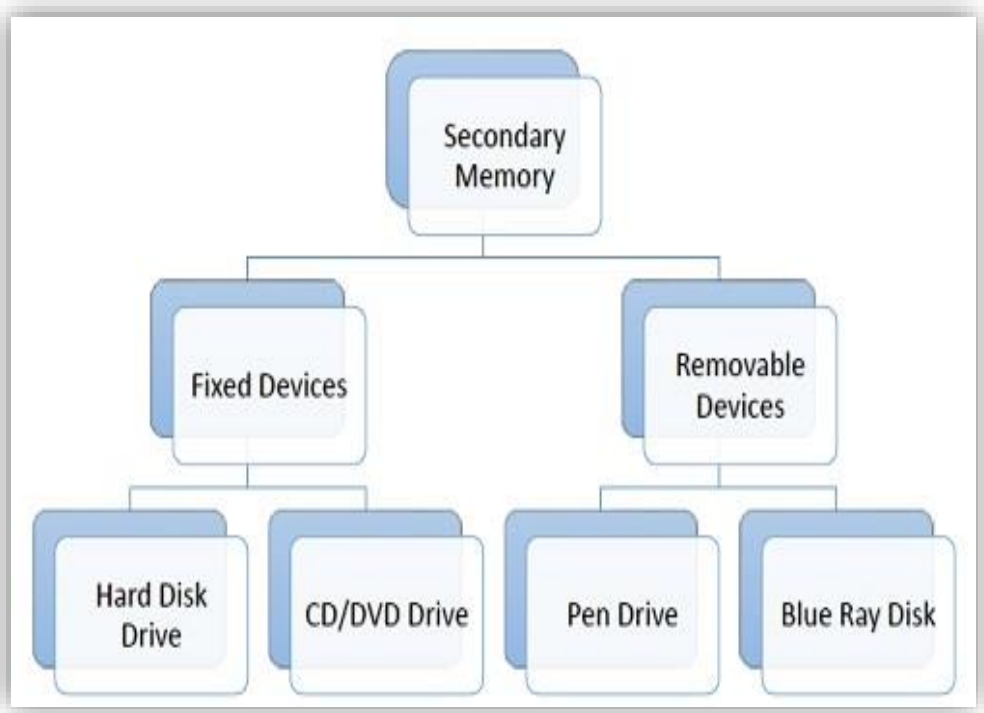
Stores data and programs permanently: it is retained after the power is turned off.

1. *Hard drive (HDD):* A hard disk is part of a unit, often called a “disk drive,” “hard drive,” or “hard disk drive,” that stores and provides relatively quick access to large amounts of data on an electromagnetically charged surface or set of surfaces.

2. *ROM (Read Only Memory):* ROM is a permanent form of storage. ROM stays active regardless of whether the power supply to it is turned on or off. ROM devices do not allow data stored on them to be modified.

3. *Optical Disk (ODD):* is a disk drive that uses laser light as part of the process of reading or writing data to or from optical discs. Some drives can only read from discs, but recent drives are commonly both readers and recorders, also called burners or writers. Compact discs, DVDs, and Bluray discs are common types of optical media that can be read and recorded by such drives. An optical drive is the generic name; drives are usually described as “CD”, “DVD”, or “Bluray”, followed by “drive”, “writer”, etc. There are three main types of optical media: CD, DVD, and Blu-ray discs. CDs can store up to 700 megabytes (MB) of data and DVDs can store up to 8.4 GB of data. Blu-ray discs, which are the newest type of optical media, can store up to 50 GB of data. This storage capacity is a clear advantage over the floppy disk storage media (magnetic media), which only has a capacity of 1.44 MB.

4. *Flash Disk:* A storage module made of flash memory chips. Flash disks have no mechanical platters or access arms, but the term “disk” is used because the data are accessed as if they were on a hard drive. The disk storage structure is emulated.



Comparison between Main Memory (RAM) and Secondary Memory (Hard Disk)

RAM	Hard Disk (Hard Drive)
Memory	Storage
Smaller amount (typically 500 MB to 6 GB)	Much larger amount (typically 80 GB to 1000 GB)
Temporary storage of files and programs	Permanent storage of files and programs
A little like your real desktop – has only your current work on it	Like a file cabinet – has long term storage of work
Contents disappear when you turn off power to the computer and when the computer crashes	Contents remain when you turn off the power to the computer (they don't disappear unless you purposely delete them), and when the computer crashes.
Consists of chips (Microprocessors)	Consists of hard disks (platters)
When you want to use a program, a temporary copy is put into RAM and that's the copy you use	Hold the original copy of the program permanently

Software

Software is a generic term for organized collections of computer data and instructions, often broken into two major categories: system software which provides the basic non-task-specific functions of the computer, and application software which is used by users to accomplish specific tasks.

Software Types:

A. *System software* is responsible for controlling, integrating, and managing the individual hardware components of a computer system so that other software and the users of the system see it as a functional unit without having to be concerned with the low-level details such as transferring data from memory to disk or rendering text onto a display. Generally, system software consists of an operating system and some fundamental utilities such as disk formatters, file managers, display managers, text editors, user authentication (login) and management tools, and networking and device control software.

B. *Application software* is used to accomplish specific tasks other than just running the computer system. Application software may consist of a single program, such as an image viewer; a small collection of programs (often called a software package) that work closely together to accomplish a task, such as a spreadsheet or text processing system; a larger collection (often called a software suite) of related but independent programs and packages that have a common user interface or shared data format, such as Microsoft Office, which consists of a closely integrated word processor, spreadsheet, database, etc.; or a software system, such as a database management system, which is a collection of fundamental programs that may provide some service to a variety of other independent applications.

Comparison between Application Software and System Software

Basis	System Software	Application Software
Definition	Computer software, or just software is a general term primarily used for digitally stored data such as computer programs and other kinds of information read and written by computers. App comes under computer software though it has a wide scope now.	Application software, also known as an application or an “app”, is computer software designed to help the user to perform specific tasks.
Example	1) Microsoft Windows 2) Linux 3) Unix 4) Mac OSX 5) DOS	1) Opera (Web Browser) 2) Microsoft Word (Word Processing) 3) Microsoft Excel (Spreadsheet software) 4) MySQL (Database Software) 5) Microsoft PowerPoint (Presentation Software) 6) Adobe Photoshop (Graphics Software)
Interaction	Generally, users do not interact with system software as it works in the background	Users always interact with application software while doing different activities
Dependency	System software can run independently of the application software	System software can run independently of the application software

Unit of Measurements

I) Storage measurements: The basic unit used in computer data storage is called a bit (binary digit). Computers use these little bits, which are composed of ones and zeros, to do things and talk to other computers. All your files, for instance, are kept in the computer as binary files and translated into words and pictures by the software (which is also ones and zeros). This two-number system is called a "binary number system" since it has only two numbers in it. The decimal number system in contrast has ten unique digits, zero through nine.

Size example:

- **1 bit -** answer to a yes/no question
- **1 byte** - a number from 0 to 255.
- **90 bytes -** enough to store a typical line of text from a book.
- **4 KB** - about one page of text.
- **120 KB -** the text of a typical pocketbook.
- **3 MB -** a three-minute song (128k bitrate)
- **650-900 MB -** a CD-ROM
- **1 GB** -114 minutes of uncompressed CD-quality audio at 1.4 Mbit/s
- **8-16 GB –** the size of a normal flash drive

Computer Storage units

Bit	BIT	0 or 1
Kilobyte	KB	1024 bytes
Megabyte	MB	1024 kilobytes
Gigabyte	GB	1024 megabytes
Terabyte	TB	1024 gigabytes

Unit of Measurements

II) Speed measurement: The speed of the Central Processing Unit (CPU) is measured by Hertz (Hz), Which represents a CPU cycle. The speed of the CPU is known as Computer Speed.

CPU SPEED MEASURES	
1 hertz or Hz	1 cycle per second
1 MHz	1 million cycles per second or 1000 Hz
1 GHz	1 billion cycles per second or 1000 MHz

GENERATIONS OF COMPUTER

Generation in computer terminology is a technology change a computer is/was being used. Initially, the generation term was used to distinguish between varying hardware technologies. Nowadays, generation includes both hardware and software, which together make up an entire computer system.

There are five computer generations known to date. Each generation has been discussed in detail along with their time period and characteristics. In the following table, approximate dates against each generation have been mentioned, which are normally accepted.

Following are the main five generations of computers.

Sl. No.	Generation & Description
1	**First Generation** The period of first generation: 1946-1959. Vacuum tube based.
2	**Second Generation** The period of second generation: 1959-1965. Transistor based.
3	**Third Generation** The period of third generation: 1965-1971. Integrated Circuit based.
4	**Fourth Generation** The period of fourth generation: 1971-1980. VLSI microprocessor based.
5	**Fifth Generation** The period of fifth generation: 1980-onwards. ULSI microprocessor based

First Generation Computers

- The period of the first generation was from **1946-1959.**
- The computers of the first generation used **vacuum tubes** as the basic components for memory and circuitry for the CPU (Central Processing Unit).
- These tubes, like electric bulbs, produced a lot of heat and the installations used to fuse frequently. Therefore, they were very expensive and only large organizations were able to afford them.
- In this generation, mainly **batch processing operating system** was used.
- **Punch cards, paper tape, and magnetic tape** were used as input and output devices.
- The computers in this generation used **machine code** as the programming language.
- The main features of the first generation are:
  - Vacuum tube technology
  - Unreliable
  - Supported machine language only
  - Very costly
  - Generates a lot of heat
  - Slow input and output devices
  - Huge size
  - Need of AC
  - Non-portable
  - Consumes lot of electricity
- Some computers of this generation were:
  - ENIAC
  - EDVAC
  - UNIVAC
  - IBM-701
  - IBM-750

Second Generation Computers

- The period of second generation was from **1959-1965**.
- In this generation, **transistors** were used that were cheaper, consumed less power, more compact in size, more reliable and faster than the first-generation machines made of vacuum tubes.
- In this generation, **magnetic cores** were used as the primary memory and **magnetic tape and magnetic disks** as secondary storage devices.
- In this generation, assembly language and high-level programming languages like **FORTRAN, and COBOL** were used.
- The computers used **batch processing and multiprogramming operating systems**.
- The main features of the second generation are:
  - Use of transistors
  - Reliable in comparison to first-generation computers
  - Smaller size as compared to first-generation computers
  - Generates less heat as compared to first-generation computers
  - Consumed less electricity as compared to first-generation computers
  - Faster than first-generation computers
  - Still very costly
  - AC required
  - Supported machine and assembly languages
- Some computers of this generation were:
  - IBM 1620
  - IBM 7094
  - CDC 1604
  - CDC 3600
  - UNIVAC 1108

Third Generation Computers

- The period of third generation was from **1965-1971**.
- The computers of the third generation used **Integrated Circuits (ICs)** in place of transistors. A single IC has many transistors, resistors, and capacitors along with the associated circuitry. The **IC was invented by Jack Kilby**. This development made computers smaller in size, more reliable, and efficient.
- In this generation **remote processing, time-sharing, and multi-programming operating system were used**.
- High-level languages (**FORTRAN-II TO IV, COBOL, PASCAL PL/1, BASIC, ALGOL-68 etc.**) were used during this generation.
- The main features of the third generation are:
  - IC used
  - More reliable in comparison to the previous two generations
  - Smaller size
  - Generated less heat
  - Faster
  - Lesser maintenance
  - Costly
  - AC required
  - Consumed lesser electricity
  - Supported high-level language
- Some computers of this generation were:
  - IBM-360 series
  - Honeywell-6000 series
  - PDP (Personal Data Processor)
  - IBM-370/168
  - TDC-316

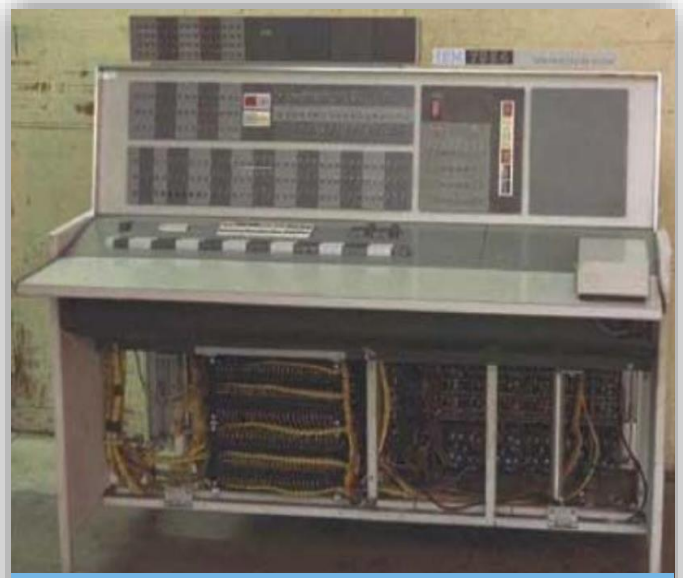
Fourth Generation Computers

- The period of fourth generation was from **1971-1980**.
- Computers of fourth generation used **Very Large Scale Integrated (VLSI) circuits**. VLSI circuits have about 5000 transistors and other circuit elements with their associated circuits on a single chip making it possible to have microcomputers of the fourth generation.
- Fourth-generation computers became more powerful, compact, reliable, and affordable. As a result, it gave rise to the Personal Computer (PC) revolution.
- In this generation, **time-sharing, real-time networks, and distributed operating systems** were used.
- All the high-level languages like **C, C++, DBASE etc.,** were used in this generation.
- The main features of the fourth generation are:
  - VLSI technology used
  - Very cheap
  - Portable and reliable
  - Use of PCs
  - Very small size
  - Pipeline processing
  - No AC required
  - Concept of internet was introduced
  - Great developments in the fields of networks
  - Computers became easily available
- Some computers of this generation were:
  - DEC 10
  - STAR 1000
  - PDP 11
  - CRAY-1(Super Computer)
  - CRAY-X-MP(Super Computer)

Fifth Generation Computers

- The period of fifth generation is **1980-till date**.
- In the fifth generation, VLSI technology became **ULSI (Ultra Large Scale Integration) technology**, resulting in the production of **microprocessor chips** having ten million electronic components.
- This generation is based on **parallel processing hardware and AI (Artificial Intelligence) software**. AI is an emerging branch in computer science, which interprets the means and method of making computers think like human beings.
- All the high-level languages like **C and C++, Java, .Net** etc., are used in this generation.
- The main features of the fifth generation are:
  - ULSI technology
  - Development of true artificial intelligence
  - Development of Natural language processing
  - Advancement in Parallel Processing
  - Advancement in Superconductor technology
  - More user-friendly interfaces with multimedia features
  - Availability of very powerful and compact computers at cheaper rates
- Some computer types of this generation are:
  - Desktop
  - Laptop
  - Notebook
  - Ultrabook
  - Chromebook

FIRST GENERATION COMPUTERS



SECOND GENERATION COMPUTERS

THIRD GENERATION COMPUTERS

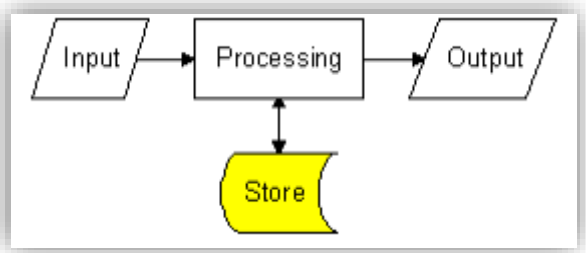
FOURTH GENERATION COMPUTERS

FIFTH GENERATION COMPUTERS

DIFFERENT TYPES OF STORAGE MEDIA

(REFER TO THE PDF FOR MORE INFORMATION)

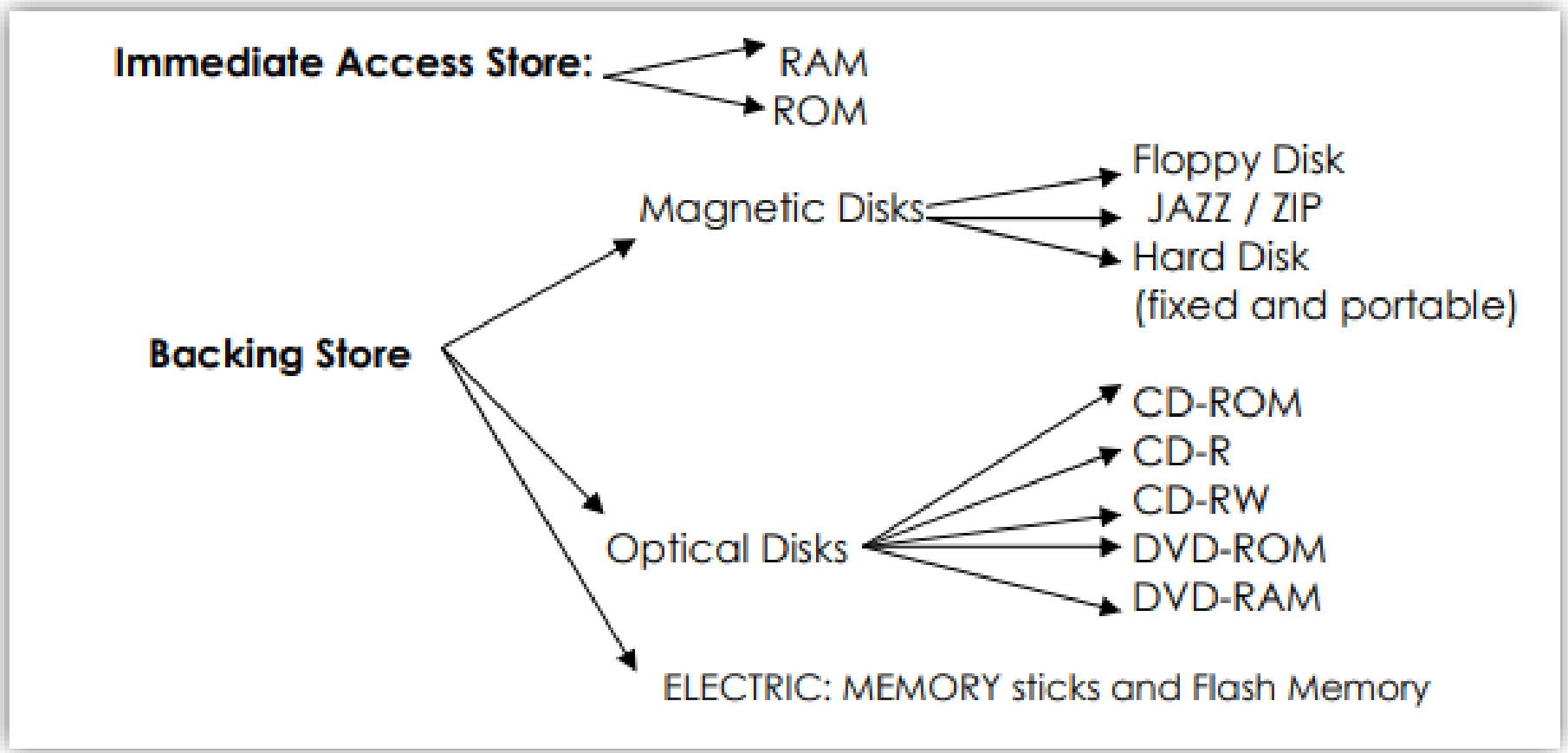
All information systems need to store data. This may be done temporarily whilst inputs are processed to produce outputs or for much longer periods of time.



A storage device stores programs and data either temporarily or permanently. All information systems contain two different types of storage :

- **Immediate Access Store (IAS):** Immediate access store holds programs and data that the user is currently working with. Immediate access store is also known as main store or primary store(RAM).
- **Backing Store:** Backing store keeps data and programs when the computer is turned off. Backing store is also known as secondary store.

DIFFERENT TYPES OF STORAGE MEDIA



CYBER CRIME

- ***Cyber Crime can be defined as unlawful acts committed by using the computer as a tool or as a target or as both.***
- Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery (copy), defamation (insult) and mischief, all of which are subject to the Indian Penal Code.
- The abuse of computers has also given birth to a gamut (range) of new age crimes that are addressed by the Information Technology Act, 2000 (introduced on 17th Oct 2000).
- *Cyber crime* refers to criminal activities carried out using computers and digital networks, targeting individuals, organizations, or governments to steal data, disrupt operations, or compromise security. This type of crime includes activities such as hacking, phishing, identity theft, online fraud, ransomware attacks, and the distribution of malicious software. With the rapid growth of technology and increased reliance on digital platforms, cyber crimes have become more sophisticated and widespread, posing significant challenges for law enforcement and cybersecurity professionals. The rise in cybercrime cases highlights the urgent need for stronger cybersecurity measures, public awareness, and robust legal frameworks to protect against evolving digital threats.
- Cyber crime cases in India have increased from 50,035 in 2020 to 65,893 in 2022. Telangana reported the highest number (15,297 cases) with a rate of 40.3 per lakh but a low charge sheeting rate (17.1%). Karnataka (12,556 cases) and Uttar Pradesh (10,117 cases) also had significant case counts but moderate charge sheeting rates. Delhi stood out among Union Territories with 685 cases and a high charge sheeting rate of 89.3%. States like Mizoram and Nagaland had minimal cases but struggled with low charge sheeting rates. The national average crime rate for cybercrimes was 4.8 per lakh. The data shows rising incidents, with disparities in charge sheeting, indicating a need for better resources and processes to manage cybercrime.

Continued….

CATEGORY TO CYBER CRIME

- Cyber Crime can be categorized mainly in two ways:

1. *Using the Computer as a Target*: Using a computer to attack other computers. E.g. Hacking, Virus/Worm attacks, DOS attacks etc.

2. *Using the computer as a Weapon*: Using a computer to commit real-world crimes. E.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

- Cyber Crimes and types of cyber crimes: Cybercrime involves unlawful human actions conducted through computers, networks and/or the internet. These illegal activities can be aimed at individuals, businesses or governmental bodies to cause system disruptions obtaining data or engaging in schemes. There are numerous crimes associated with the cyber world, like:

1. *Breach of Cybersecurity*: A breach incident in cybersecurity occurs when an individual or organisation obtains unauthorized access, to computer systems or networks and such unauthorised access leads to data theft or operational disruptions. These incidents encompass a variety of forms such, as data breaches, ransomware attacks, cyber terrorism and supply chain infiltrations.

2. *Cyber Threats*: Cyber threats refer to the illegal acts of hackers whose primary goals are to disrupt the computer network, harm the computer systems and/ or engage in malpractices on those devices. Examples include, but are not limited to Trojan attacks, Advanced Persistent threats (ATPs), phishing activities like fraudulent emails and messaging to trick individuals.

3. *Digital Content Offenses and Cyberbullying & Harassment*: This category encompasses the creation or distribution of hateful content online. Digital content offenses include a wide range of activities, including, but not limited to identity theft, cyberbullying, phishing, child pornography, cyberstalking, morphing, hate speech and others. The Information Technology Act (IT Act) and the Indian Penal Code have specified punishment for each of such types of terrible acts.

4. *Fraudulent Activities in the Cyberspace*: Credit card, and OTP scams have taken over the world. These involve deceiving individuals or organizations, with the intention of obtaining electronic signatures, money or personal information. This also includes identity theft, investment fraud and Aadhar card fraud are on the rise in India.

Moreover, cyber crimes are further categorized as follows:

Continued….

1. Unauthorized Access
2. Hacking & Cracking
3. Cyber Theft (Identity Theft, Theft of Internet Hours, Theft of Computer System (Hardware)
4. Cyber Pornography
5. Cyber Fraud/Online Fraud (Spoof Websites and Email Security Alerts, Virus Hoax Emails, Lottery Frauds, Spoofing, Credit Card Fraud)
6. Cyber Terrorism
7. Defamation
8. Cyber Stalking
9. Email & IRC Related Crimes (Email Spoofing, Email Spamming, Email Bombing, Sending Threatening Emails, Defamatory Emails, Email Frauds, Internet Relay Chat (IRC) Related)
10. Spamming
11. Denial of Service Attacks
12. Forgery
13. IPR Violations
14. E-Commerce/Investment Frauds
15. Sale of illegal articles
16. Online Gambling
17. Data diddling
18. Physically Damaging a Computer System
19. Breach of Privacy and Confidentiality

1. **Unauthorized Access:** Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any kind of access without the rightful owner's permission or the person in charge of a computer, computer system or computer network.

2. **Hacking & Cracking:** Every act committed to breaking into a computer and/or network is hacking. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destroy and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their accounts, and withdrawing money. Crackers may steal or modify data or insert viruses or worms which damage the system. Hacking a web server and taking control of another person's website is called as web hijacking.

3. **Cyber Theft:** Stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use.
   - ***Identity Theft:*** Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.
   - ***Theft of Internet Hours:*** Unauthorized use of Internet hours paid for by another person.
   - ***Theft of computer system (Hardware):*** This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

4. **Cyber Pornography:** Pornography' is "describing or showing sexual acts to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and the use of the internet to download and transmit pornographic videos, pictures, photos, writings etc. There are more than 420 million individual pornographic web pages today. Child pornography is a very unfortunate reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. *Paedophiles use a false identity to trap children/teenagers.*

5. **Cyber Fraud/Online Fraud:** The net is a boon for people to conduct business effectively, and very quickly. Net is also an open invitation to fraudsters and online frauds are becoming increasingly out of control.
   - ***Spoof Websites and Email Security Alerts:*** Fraudsters create authentic-looking websites that are nothing but a spoof. The purpose of these websites is to make the user enter personal information. This information is then used to access business and bank accounts. If you ever get an email containing an embedded link, and a request for you to enter secret details, treat it as suspicious. Do not input any sensitive information that might help provide access to your accounts, even if the page appears legitimate. No reputable company ever sends emails of this type.
   - ***Virus Hoax Emails:*** It is a sad fact of life that some enjoy exploiting the concerns of others. Many emailed warnings about viruses are hoaxes, designed purely to cause concern and disrupt businesses. These warnings may be genuine, so don't take them lightly, but always check the story out by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, including forwarding them to friends and colleagues.
   - ***Lottery Frauds:*** These are letters or emails, which inform the recipient that he/ she has won a prize in a lottery. To get the money, the recipient has to reply. After which another mail is received asking for bank details so that the money can be directly transferred. The email also asks for a processing fee/ handling fee. Of course, the money is never transferred in this case, the processing fee is swindled and the banking details are used for other frauds and scams.
   - ***Spoofing:*** Spoofing means illegal intrusion, posing as a genuine user. A hacker logs in to a computer illegally, using a different identity than his own. He can do this by having previously obtained an actual password. He creates a new identity by fooling the computer into thinking he is the genuine system operator. The hacker then takes control of the system. He can commit an innumerable number of frauds using this false identity. In short, spoofing refers to a thing that appears to have originated from one source when it was sent from another source.
   - ***Credit Card Fraud:*** Online Transactions have become a normal thing in day to day life. Knowingly or unknowingly passing credit card information over the internet can land you in trouble. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

6. **Cyber Terrorism:** Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, and telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyberterrorism is an attractive option for modern terrorists for several reasons:

- It is **cheaper** than traditional terrorist methods.
- Cyberterrorism is **more anonymous** than traditional terrorist methods.
- The **variety and number of targets** are enormous.
- Cyberterrorism can be **conducted remotely**, a feature that is especially appealing to terrorists.
- Cyberterrorism has the potential to **affect directly** a larger number of people.
- Flowing of **Viruses, Trojan horses, Worm & Logical Bombs:**
  - The program acts like something useful but does things that are quite damp. The programs of this kind are called as ***Trojans***. Trojans come in two parts, **a Client part and a Server part**. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.
  - A program that can infect other programs by making copies of itself and spread into other programs is called a ***Virus***. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (*for example*, triggered after a specific number of executions), time-driven effects (triggered on a specific date, such as Friday the 13th) or can occur at random. The action of a virus can display a message to prompt an action which may set off the virus, Erase files, Scramble data on a hard disk, Cause erratic screen behaviour, Halt the PC, etc.
  - Programs that multiply like viruses but spread from computer to computer are called as ***Worms***. *For example*, the Anna Kournikova worm (Feb-2001), The first computer virus ever to be seen was called BRAIN and it appeared in 1986. Some famous viruses are: Jerusalem (1987), Dark Avenger (1989), Michelangelo (1991), Concept (1995), Melissa, CIH (1999), The Love Letter (2000), CodeRed, Nimda (2001), Sir Cam-Nimda, etc.
  - ***Logical Bombs*** are event-dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. *For example*, even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

7. **Defamation:** Defamation can be understood as the intentional infringement of another person's right to his good name. Defamation can be understood as tarnishing the image, respect or dignity of any person in front of right-thinking members of the society.

   Cyber Defamation occurs when defamation takes place with the help of computers and/or the Internet. *For example*, someone publishes a defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends A matter defaming a person is sent to the said person directly is not defamation however if the said mail is sent through CC or BCC to third parties and if the contents tarnish (blemish/dull) the image of the recipient it is defamation. Publication of defamatory articles and matters on a website is defamation. Cyber defamation is also called as **Cyber Smearing**.

8. **Cyber Stalking:** Cyber Stalking can be defined as the repeated acts of harassment or threatening behaviour of the cyber criminal towards the victim by using Internet services. (or Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat rooms frequented by the victim, constantly bombarding the victim with emails etc.) Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as:

   - Following the victim.
   - Making harassing phone calls.
   - Killing the victim's pet.
   - Vandalizing the victim's property.
   - Leaving written messages or objects.
   - Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Both kinds of stalkers – online and offline – have a desire to control the victim's life.

   Cyber-stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. It is a relatively new form of harassment, unfortunately, rising to alarming levels especially in big cities like Mumbai.

9. **E-mail & IRC related crimes:**

- ***Email Spoofing:*** Email spoofing refers to an email that appears to have originated from one source when it was sent from another source.
- ***Email Spamming:*** Email "spamming" refers to sending emails to thousands and thousands of users - similar to a chain letter called Email Spamming. Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam.
- ***Email Bombing*****:** E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.
- ***Sending Threatening Emails:*** Email is a useful tool for technology-savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.
- ***Defamatory Emails:*** Cyber-defamation or even cyber-slander as it is called can prove to be very harmful and even fatal to the people who have been made its victims. **OR** Defamation is defined as communication to third parties of false statements about a person that injure the reputation of or deter others from associating with that person. A communication is not defamatory unless it is published to someone other than the target.
- ***Email Frauds:*** Email Fraud is the intentional deception made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game" or scam.
- ***IRC related:*** Internet Relay Chat (IRC) is a protocol for real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message as well as chat and data transfer, including file sharing. "Chat room" is another name for an Internet Relay Chat (IRC) channel Internet Relay Chat (IRC) Crime:
    - ✓Criminals use it for meeting coconspirators.
    - ✓Hackers use it for discussing their exploits/sharing techniques.
    - ✓Pedophiles use chat rooms to allure small children.

Three main ways to attack IRC are **Spam (Flood) Attacks, Clone Attacks and DoS (Denial of Service) Attacks**.

10. **Spamming:** Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising. *For example*, get-rich-quick schemes. There are two main types of spam, and they have different effects on Internet users: **Cancellable Usenet/Usenet Spam and Email-Spam**.
    - **Cancellable Usenet Spam** is a single message sent to 20 or more Usenet newsgroups.
    - **Email "spamming"** refers to sending emails to thousands and thousands of users - similar to a chain letter. Email spam, also known as **Junk Email** or **Unsolicited Bulk Email (UBE)**, is a subset of electronic spam. One subset of UBE is **UCE (Unsolicited Commercial Email)**. Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. They also use a practice known as "email appending" or "pending" in which they use known information about their target (such as a postal address) to search for the target's email address.

11. **Denial of Service Attacks:** Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access to service to authorized users. *Examples include* attempts to "flood" a network, thereby preventing legitimate network traffic attempts to disrupt connections between two machines, thereby preventing access to a service attempts to prevent a particular individual from accessing a service attempts to disrupt service to a specific system or person.

12. **Forgery:** Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. Also, impersonating another person is considered forgery.

13. **IPR Violations:** These include software piracy, copyright infringement, trademark violations, theft of computer source code, and patent violations. etc. **Cyber Squatting:** Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber Squatters registers domain names identical to popular service providers' domains to attract their users and benefit from it.

14. **E-commerce/Investment Frauds:** Sales and Investment Frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud is attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

15. **Sale of Illegal Articles:** This would include trade of narcotics, weapons, wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows the number of people employed in this criminal area. Daily people receive so many emails with offers of banned or illegal products for sale.

16. **Online gambling:** There are millions of websites hosted on servers abroad, that offer online gambling. It is believed that many of these websites are fronts for money laundering.

17. **Data Diddling:** Data diddling involves changing data before or during input into a computer. In other words, information is changed from the way it should be entered by a person typing. in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatically changing the financial information for some time before processing and then restoring the original information.

18. **Physically Damaging a Computer System:** Physically damaging a computer or its peripherals either by shock, fire or excess electric Supply etc.

19. **Breach of Privacy and Confidentiality:**
    - ***Privacy:*** Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.
    - ***Confidentiality:*** It means non-disclosure of information to unauthorized or unwanted persons. In addition to personal information, some other types of information which are useful for business and leakage of such information to other persons may cause damage to the business or person, such information should be protected. Generally, to protect the secrecy of such information, parties while sharing information form an agreement about the procedure of handling information and do not disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monetary gains and cause a breach of contract of confidentiality. Special techniques such as *Social Engineering* are commonly used to obtain confidential information.

CYBER LAW

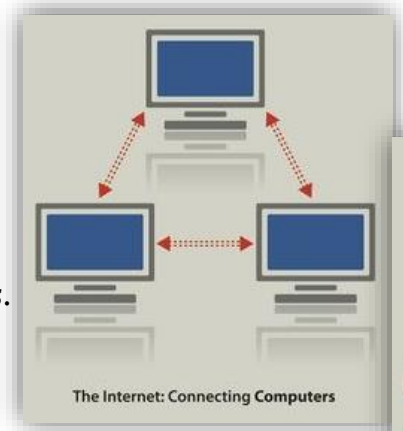
- ***"Cyber"*** is a prefix that describes a person, thing, or idea as part of the computer and information age.
- Taken from *kybernetes*, a Greek word for *"steersman" or "governor,"* it was first used in cybernetics, a word coined by **Norbert Wiener** and his colleagues.
- The virtual world of the internet is known as ***Cyberspace*** and the laws governing this area are known as ***Cyber Laws*** and all the netizens of this space come under the ambit of these laws as they carry a kind of universal jurisdiction.
- *Cyber Law* can also be described as that branch of law that *deals with legal issues related to using inter-networked information technology*. In short, cyber law is the *law governing computers and the internet*.
- The growth of Electronic Commerce (e-commerce) has propelled the need for vibrant and effective regulatory mechanisms that would further strengthen the legal infrastructure, which is crucial to its success. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law.
- Cyber law is important because it touches almost all aspects of transactions and activities on and involving the Internet, World Wide Web (WWW) and cyberspace. Every action and re-action in cyberspace has some legal and cyber legal perspectives.
- Cyber law encompasses laws relating to:

- Cyber crimes ***- Electronic and digital signatures*** ***- Intellectual property*** ***- Data protection and privacy***

HISTORY OF THE INTERNET AND WORLD WIDE WEB (WWW):

Continued….

- ***Definition of Internet:*** A global system of interconnected computer networks using the *Internet Protocol Suite (TCP/IP)*.
- ***Network Composition:*** Includes millions of *private, public, academic, business, and government networks* connected by technologies such as *copper wires, fibre-optic cables, and wireless connections*.
- ***Functions and Services: (a)*** Supports hypertext documents (WWW); ***(b)*** Provide infrastructure for email, online chat, file transfer, file sharing, online gaming, and VoIP (voice/video communication).
- ***Origins:***
  - *1960s:* U.S. military agencies funded research to create fault-tolerant and distributed networks.
  - *1990s:* Civilian funding by the National Science Foundation led to global commercialization and rapid development.
- ***Distinction Between Internet and WWW:***
  - *Internet:* The global data communication system providing connectivity between computers.
  - *WWW:* A service on the Internet that includes interconnected documents and resources linked by *URLs and hyperlinks*.
- ***Creation of the WWW:***
  - *Invented in **1989**:* By **Tim Berners-Lee**, assisted by **Robert Cailliau** at **CERN, Geneva**.
  - *Release: **December 1990***; introduced *"web of nodes" with "hypertext pages" accessible by "browsers".*
- ***Growth of Internet Usage:***
  - *2000-2009:* Global users grew from 394 million to 1.858 billion.
  - *2010:* 22% of the world had computer access, with 1 billion daily Google searches, 300 million blog readers, and 2 billion daily YouTube views.
- ***Popular Languages on the WWW:*** English (27%), Chinese (23%), Spanish (8%), Japanese (5%), Portuguese and German (4% each), Arabic, French, and Russian (3% each), Korean (2%).
- ***Regional Distribution of Users:*** Asia: 42% of users; Europe: 24%; North America: 14%; Latin America/Caribbean: 10%; Africa: 6%; Middle East: 3%; Australia/Oceania: 1%.



How to protect yourself on the Internet?

Continued….

1. *Use Anti-virus software:* Antivirus programs are designed *to identify and eliminate suspicious software* that can pose a threat, to your device and compromise its security. It's important to scan your devices for viruses and malware to ensure that they remain safeguarded.

2. *Use strong passwords and 2-factor authentications:* It's very necessary to prioritize passwords and multi-factor authentication *to protect your accounts from unauthorized access*. *Avoid using information such, as birthdays, names or common words, in your passwords*. *Instead opt for a combination of upper- and lower-case letters, numbers and symbols to create strong unbreakable passwords*.

3. *Be cautious of sharing information and the content you post:* Phishing scams are frequently utilized by cybercriminals to deceive people into exposing information or clicking on links. It's important to be cautious of emails that contain attachments or links. *Limit the amount of information you share online on social media platforms. Refrain, from disclosing details such, as your home address or phone number*.

NEED FOR CYBER LAW:

What is Cyber Law? – *Cyber Law or Information Technology Law* involves studying matters related to using the internet electronic devices, for communication and computer networks. This field addresses topics such as *agreements, digital crimes, data protection, privacy rights, jurisdiction in cyberspace and legal principles in the digital realm*. Its significance lies in safeguarding the rights of people and businesses to maintain a trustworthy online space.

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. The Internet was initially developed as a research and information-sharing tool and was in an unregulated manner. As time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all *transactions* in shares are in demat form.
- Almost all companies extensively depend upon their *computer networks* and keep their *valuable data in electronic form*.
- *Government forms* including income tax returns, company law forms etc. are now filled in *electronic form*.
- Consumers are increasingly using *credit cards for shopping*.
- Most people are using *email, cell phones and SMS messages for communication*.
- Even in *"non-cyber crime" cases, important evidence is found in computers/cell phones* e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency, smuggling, etc.
- Cyber crime cases such as *online banking fraud, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common*.
- *Digital signatures and e-contracts* are fast replacing conventional methods of *transacting business*.

Technology per se is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickle-down effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic matrix.

CYBER LAW IN INDIA:

Continued….

In the age of India's rapid development, cyber law has become an essential aspect of the legal framework. It covers a range of legal matters in the digital realm related to the use of electronic devices, computer networks and the increased use of social media. It plays an important role in protecting the rights of individuals and organizations in the world ensuring a safe and reliable online environment.

1. ***Information Technology Act, 2000 (IT Act):*** The IT Act in India serves as the foundation of cyber law and covers types of cybercrimes, imposes punishments for crimes involving unauthorized accessing into computer systems stealing data, hacking, cyberterrorism and spreading inappropriate or offensive material on the internet.

2. ***The Digital Personal Data Protection Act, 2023 (DPDPA):*** DPDPA focuses on regulating data collection, processing, storage and usage while bolstering privacy safeguards with an emphasis on securing minor consent through the permission of guardians.

3. ***Measures Pertaining Cybersecurity:*** India has made huge strides in cybersecurity by establishing the National Cyber Coordination Centre (NCSC) and the Indian Computer Emergency Response Team (CERT-In) to combat cyber threats, and data breaches and to improve cybersecurity resilience. The IT Act mandates companies and organisations to report data breaches within a 6-hour window of noticing such data breaches to CERT-In for investigation and response to cyber-attacks.

4. ***Cybercrime Investigation:*** Specialized cyber cell units within the police force have been set up specifically for investigating and prosecuting cybercrimes efficiently. The Digital India Initiative by the Government needs to be applauded for the sound implementation of this initiative.

IMPORTANCE OF CYBER LAW:

The field of cyber law plays a very crucial role, in today's digital era. *Its significance arises from the increasing reliance on the internet and computer networks across various aspects of our everyday lives ranging from personal interactions to businesses*. The importance is highlighted below:

- *Preserving Individual Rights:* Cyberlaw serves to safeguard rights such as privacy, identity and property within the realm of the world. It helps to block entry to data, safeguards against cyberbullying and dangers online and secures intellectual assets from being violated.

- *Fighting Cybercrime:* Cyber Laws are preventive and protective regulations about cyberspace crimes. They set out punishments for crimes such as hacking, phishing, data and identity theft, cyberbullying and online fraud. These laws also outline procedures for catching and punishing criminals and hence are aimed at preventing unlawful activities and holding individuals accountable for their wrongful actions.

- *Strengthening Cybersecurity:* Within the domain of cyber law lie frameworks that aim to protect infrastructure encompassing computer networks, data storage systems and online services. It mandates cybersecurity measures, promotes secure practices and facilitates cooperation in combating cyber threats. Examples are Computer Emergency Response Team (CERT-In) Directions to protect data theft.

OBJECTIVES OF CYBER LAW:

Continued….

Cyberlaw has numerous objectives all to establish an environment that is safe secure and reliable, for individuals, organizations and nations. A few advantages of cyber law and its objectives have been enumerated below:

- *Preserving Privacy:* Cyberlaw ensures that individuals' privacy rights are protected in the world by ensuring the collection, storage and proper processing of personal data.
- *Shielding Identity:* Cyberlaw acts as a safeguard for Individuals' identities by preventing unlawful access, theft or misuse of identity. This protection helps prevent impersonation and identity fraud.
- *Preventing Cybercrime:* Cyber law defines boundaries and penalties, for cybercrimes. Doing it discourages individuals from participating in malicious and unlawful activities online.

Difference between Cybercrime and Cybersecurity:

BASIS	CYBERCRIME	CYBERSECURITY
Definition	Commission of illegal activities through use of computer networks and programs.	Protection of computer systems and networks from malicious digital activities.
Focus On	Exploitation, harms towards Individuals, property and government.	Security, prevention and protection of harmful activities.
Legal Framework	IT Act, Criminal laws, Contracts	IT Act, Data Protection Laws
Objectives	Deterring crimes, protection of individuals, and to impose punishments on offenders.	Protection of assets and information, incident response plans and to minimise data attacks.
Examples	IT Act, IPC that is Bharatiya Nyaya Sanhita (BNS).	IPC that is Bharatiya Nyaya Sanhita (BNS), CERT-IN Rules, The Digital Personal Data Protection Act.

IMPORTANT TERMS RELATED TO CYBER LAW:

Continued….

1. **"Access"** with its grammatical variations and cognate expressions means *gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network*. (Sec.2(1)(a) of IT Act, 2000)

2. **"Addressee"** means *a person who is intended by the originator to receive the electronic record but does not include any intermediary*. (Sec.2(1)(b) of IT Act, 2000)

3. **"Affixing Electronic Signature"** with its grammatical variations and cognate expressions means the *adoption of any methodology or procedure by a person to authenticate an electronic record using an Electronic Signature*. (Sec.2(1)(d) of IT Act, 2000)

4. **"Asymmetric Crypto System"** means *a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature*. (Sec.2(1)(f) of IT Act, 2000)

5. **"Certifying Authority"** means *a person who has been granted a license to issue an Electronic Signature Certificate* under section 24. (Sec.2(1)(g) of IT Act, 2000)

6. **"Communication Device"** means *Cell Phones, Personal Digital Assistance (Sic), or a combination of both or any other device used to communicate, send or transmit any text, video, audio, or image*. (Sec.2(1)(ha) of IT Act, 2000)

7. **"Computer"** means *any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network* (Sec.2(1)(i) of IT Act, 2000)

8. **"Computer Network"** means the *interconnection of one or more Computers or Computer systems or Communication devices through - (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained*. (Sec.2(1)(j) of IT Act, 2000)

9. **"Computer Resource"** means *a computer, communication device, computer system, computer network, data, computer database or software*. (Sec.2(1)(k) of IT Act, 2000)

10. **"Computer System"** means *a device or collection of devices, including input and output support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions*. (Sec.2(1)(l) of IT Act, 2000)

IMPORTANT TERMS RELATED TO CYBER LAW:

Continued….

11. **"Cyber Cafe"** means *any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public*. (Sec.2(1)(na) of IT Act, 2000)

12. **"Cyber Security"** means *protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction*. (Sec.2(1)(nb) of IT Act, 2000)

13. **"Data"** means *a representation of information, knowledge, facts, concepts or instructions that are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*. (Sec.2(1)(o) of IT Act, 2000)

14. **"Digital Signature"** means *authentication of any electronic record by a subscriber using an electronic method or procedure* by the provisions of section 3. (Sec.2(1)(p) of IT Act, 2000)

15. **"Electronic Form"** refers to *any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device*. (Sec.2(1)(r) of IT Act, 2000)

16. **"Electronic Record"** means *data, record or data generated, image or sound stored, received or sent in an electronic form, micro film or computer generated micro fiche*. (Sec.2(1)(t) of IT Act, 2000)

17. **"Electronic Signature"** means *authentication of any electronic record by a subscriber using the electronic technique specified in the second schedule, including a digital signature*. (Sec.2(1)(ta) of IT Act, 2000)

18. **"Function"**, in relation to a computer, includes *logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer*. (Sec.2(1)(u) of IT Act, 2000)

19. **"Information"** includes *data, messages, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche*. (Sec.2(1)(v) of IT Act, 2000)

20. **"Intermediary"** with respect to any particular electronic records, means *any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes*. (Sec.2(1)(w) of IT Act, 2000)

IMPORTANT TERMS RELATED TO CYBER LAW:

11. **"Key Pair"**, in an asymmetric crypto system, means *a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key*. (Sec.2(1)(x) of IT Act, 2000)

12. **"Originator"** means *a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary*. (Sec.2(1)(za) of IT Act, 2000)

13. **"Private Key"** means the *key of a key pair used to create a digital signature*. (Sec.2(1)(zc) of IT Act, 2000)

14. **"Public Key"** means the *key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate*. (Sec.2(1)(zd) of IT Act, 2000)

15. **"Secure System"** means *computer hardware, software, and procedure that*: (a) are reasonably secure from unauthorized access and misuse; (b) provide a reasonable level of reliability and correct operation; (c) are reasonably suited to performing the intended functions; and (d) adhere to generally accepted security procedures. (Sec.2(1)(ze) of IT Act, 2000)

16. **"Subscriber"** means *a person in whose name the Electronic Signature Certificate is issued*. (Sec.2(1)(zg) of IT Act, 2000)

CYBER LAW IN INDIA:

Continued….

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate the filing of electronic records with the Government.

The following Acts, Rules and Regulations are covered under cyber laws:

1. ***Information Technology Act, 2000***
2. ***Information Technology (Certifying Authorities) Rules, 2000***
3. ***Information Technology (Security Procedure) Rules, 2004***
4. ***Information Technology (Certifying Authority) Regulations, 2001***

NEED FOR CYBER LAW IN INDIA:

- **Firstly,** India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Book Evidence Act, of 1891 and the Reserve Bank of India Act, of 1934, the Companies Act, and so on. However, the arrival of the Internet signalled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could visualize the Internet. Despite the brilliant acumen of our master draftsmen, the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.

- **Secondly**, the existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace. The practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the a need for the enactment of relevant cyber laws.

- **Thirdly,** none of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, that gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyberlaw.

- **Fourthly,** the Internet requires an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of the Internet, can only be possible if necessary legal infrastructure complements the same to enable its vibrant growth.

All these and other varied considerations created a conducive atmosphere for the need to enact relevant cyber laws in India.

HISTORY OF IT ACT IN INDIA:

- **Origin:** The Information Technology Act, of 2000, was *influenced by the UN General Assembly's 1997 resolution adopting the Model Law on Electronic Commerce*, encouraging member states to align their laws for consistency in electronic commerce and communication.
- **Initial Drafting:** The ***Department of Electronics (DoE) drafted the initial bill in July 1998***. It was ***delayed*** and ***introduced to Parliament on December 16, 1999, after the formation of the new IT Ministry***.
- **Revisions:** The Commerce Ministry added *provisions related to e-commerce and World Trade Organization (WTO) obligations*. The *draft was vetted by the Ministry of Law and Company Affairs*.
- **Parliamentary Review:** The bill was *reviewed by a 42-member Parliamentary Standing Committee after its introduction*. Various suggestions were proposed; only those *approved by the Ministry of Information Technology were incorporated*.
- **Debated Provision:** One controversial suggestion was for *cyber cafe owners to maintain a register of visitors' details and websites accessed, aimed at curbing cybercrime*. This was *dropped due to concerns over privacy and feasibility*.
- **Final Approval:**
  - ❖The ***Union Cabinet*** approved the bill on ***May 13, 2000***.
  - ❖Passed by ***both houses of Parliament*** on **May 17, 2000**.
  - ❖Received ***presidential assent*** on ***June 9, 2000***.
  - ❖***Came into force on October 17, 2000***.
- **Need for Amendments:**
  - ❖*Technological advancements and new cybercrime methods* highlighted gaps in the original act.
  - ❖The Information Technology (Amendment) Act, 2008, was introduced *to address new cyber offences and enforcement issues*.
  - ❖The *amendments became effective on October 27, 2009*, bringing significant updates to the original act.

INFORMATION TECHNOLOGY ACT, 2000

Introduction:

- The Information Technology Act, 2000 provides legal recognition for transactions carried out using electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend The Indian Penal Code, The Indian Evidence Act, 1872, The Banker’s Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

- The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention thereunder committed outside India by any person.

Applications of The Information Technology Act, 2000:

Nothing in The Information Technology Act, 2000 shall apply to documents or transactions specified in the First Schedule: Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto. Every notification issued shall be laid before each House of Parliament. Following are the documents or transactions to which the Act shall not apply:

- *Negotiable Instrument* (Other than a cheque) as defined in The Negotiable Instruments Act, 1881;
- A *power-of-attorney* as defined in The Powers of Attorney Act, 1882;
- A *trust* as defined in The Indian Trusts Act, 1882;
- A *will* as defined in The Indian Succession Act, 1925 including any other testamentary disposition;
- Any *contract* for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be *notified by the Central Government*.

INFORMATION TECHNOLOGY ACT, 2000

Importance of IT Act 2000:

- The Act provides legal recognition to electronic records, resulting in the growth of e-commerce and digital transactions in India.
- It has established electronic signatures as the legal equivalent of physical signatures.
- The formulation of this act has come up with the establishment of the Controller of Certifying Authorities (CCA), a government body that is responsible for issuing and maintaining the security of digital signatures as well as certificates.
- The Act has made it mandatory for companies to obtain consent from consumers when it comes to collecting or using their personal information.
- With the Act becoming effective, individuals have the right to seek compensation in case of damage or misuse of their personal data by an unauthorised party.
- Through the Act, the Government of India can criminalise cybercrime, hacking and spreading of computer viruses.
- The Information Technology Act 2000 also authorised the establishment of the Cyber Appellate Tribunal, a specialised official body hired to address the appeals against orders passed by Adjudicating Officers under the Act.
- It contains provisions that safeguard the critical information infrastructure, including communication networks and power grids.

Amendments in the IT ACT, 2000:

1) IT Act – 2008 Amendments –

The IT Act 2000 was *amended in 2008*. This amendment introduced the *controversial Section 66A into the Act*.

Section 66A:

- Section 66A gave authorities the power to arrest anyone accused of posting content on social media that could be deemed ‘offensive’.
- This amendment was passed in the Parliament without any debate.
- As per the section, a person could be convicted if proven on the charges of sending any ‘information that is grossly offensive or has menacing character’.
- It also made it an offence to send any information that the sender knows to be false, but for the purpose of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, through a computer or electronic device.
- The penalty for the above was up to three years imprisonment with a fine.

Arguments against Section 66A:

- Experts stated that the terms ‘offensive’, ‘menacing’, ‘annoyance’, etc. were vague, ill-defined, or not defined at all.
- Anything could be construed as offensive by anybody.
- There was a lot of scope for abuse of power using this provision to intimidate people working in the media.
- This also curbed the freedom of speech and expression enshrined as a fundamental right in the Constitution.
- The section was used most notably to arrest persons who made uncharitable remarks or criticisms against politicians.

The government contended that the section did not violate any fundamental right and that only certain words were restricted. It stated that as the number of internet users mushroomed in the country, there was a need to regulate the content on the internet just like print and electronic media. The Supreme Court, however, in 2015, struck down this section of the IT Act saying it was unconstitutional as it violated Article 19(1)(a) of the Constitution. This was in the famous Shreya Singhal v Union of India case (2015).

Amendments in the IT ACT, 2000:

1) IT Act – 2008 Amendments –

Section 69A:

- Section 69A empowers the authorities to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defence of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.
- It also empowers the government to block internet sites in the interests of the nation. The law also contained procedural safeguards for blocking any site.
- When parties opposed to the section stated that this section violated the right to privacy, the Supreme Court contended that national security is above individual privacy. The apex court upheld the constitutional validity of the section.
- The recent banning of certain Chinese Apps was done citing provisions under Section 69A of the IT Act.

Note: The Indian Telegraph Act of 1885 allows the government to tap phones. However, a 1996 SC judgement allows tapping of phones only during a 'public emergency'. Section 69A does not impose any public emergency restriction on the government.

2) Information Technology Intermediary Guidelines (Amendment) Rules, 2018 –

The Rules have been framed under Section 79 of the Information Technology Act. This section covers intermediary liability.

- Section 79(2)(c) of the Act states that intermediaries must observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the Central Government.
- *Online Intermediaries:*
  - ❖ An intermediary is a service that facilitates people to use the Internet, such as Internet Service Providers (ISPs), search engines and social media platforms.
  - ❖ There are two categories of intermediaries:
    - ✓ *Conduits:* Technical providers of internet access or transmission services.
    - ✓ *Hosts:* Providers of content services (online platforms, storage services).
- Information Technology Intermediary Guidelines (Amendment) Rules were first released in 2011 and in 2018, the government made certain changes to those rules.
- In 2018, there was a rise in the number of mob lynchings spurred by fake news & rumours and messages circulated on social media platforms like WhatsApp.
- To curb this, the government proposed stringent changes to Section 79 of the IT Act.

Amendments in the IT ACT, 2000:

2) Information Technology Intermediary Guidelines (Amendment) Rules, 2018 –

What do the Rules say?

- According to the 2018 Rules, social media intermediaries should publish rules and privacy policies to curb users from engaging in online material that is pedophilic, pornographic, hateful, racially and ethnically objectionable, invasive of privacy, etc.
- The 2018 Rules further provide that whenever an order is issued by government agencies seeking information or assistance concerning cybersecurity, then the intermediaries must provide them the same within 72 hours.
- The Rules make it obligatory for online intermediaries to appoint a 'Nodal person of Contact' for 24/7 coordination with law enforcement agencies and officers to ensure compliance.
- The intermediaries are also required to deploy such technologies based on automated tools and appropriate mechanisms to identify or remove or disabling access to unlawful information.
- The changes will also require online platforms to break end-to-end encryption to ascertain the origin of messages.
- Online Intermediaries are required to remove or disable access to unlawful content within 24 hours. They should also preserve such records for a minimum period of 180 days for investigations.

The Rationale Behind the Rules:

- The government intends to make legal frameworks in order to make social media accountable under the law and protect people and intermediaries from misusing the same.
- The government wants to curb the spread of fake news and rumours, and also pre-empt mob violence/lynching.
- There is a need to check the presentation of incorrect facts as news by social media, that instigates people to commit crimes.

There has been **criticism of the Rules** from certain quarters, that say that the State is intruding into the privacy of the individual. Some also say that this law widens the scope of state surveillance of its citizens. These criticisms are even though the new Rules are in line with recent SC rulings.

- *Tehseen S. Poonawalla case (2018):* SC said that authorities have full freedom to curb the dissemination of explosive and irresponsible messages on social media, that could incite mob violence and lynchings.
- *Prajwala Letter case (2018):* SC ordered the government to frame the necessary guidelines to "eliminate child pornography, rape and gang rape imagery, videos, and sites in content hosting platforms and other applications".

Objectives of the Amendments in The Information Technology Act, 2000:

- With the proliferation of information technology-enabled services such as e-governance, e-commerce and e-transactions, the protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, the protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system to restrict its access.

- A rapid increase in the use of computers and the internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by an intermediary, e-commerce frauds like personating commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.

- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly Computer Education-II UNIT-IV of the United Nations by its resolution No. 56/80, dated 12th December 2001, recommended that all States accord favourable consideration to the said Model Law on Electronic Signatures. Since digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.

- The service providers may be authorized by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also collect, and retain appropriate service charges for providing such services at such scale as may be specified by the Central Government or the State Government.

Offences under The Information Technology Act, 2000:

The Information Technology Act, 2000 has specified that Tampering with computer source documents, Hacking computer systems, Publishing of information that is obscene in electronic form or failure of a CA or its employees to follow the directions/ Orders of the CCA, failure to comply with Directions of Controller to a subscriber to extend facilities to decrypt information, accessing a protected system without proper authorization, material misrepresentation, Penalty for publishing Electronic Signature Certificate false particulars, Publication for fraudulent purpose, sending of grossly offensive information, false information, etc. will be offences.

The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

Continued….

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person 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.	Imprisonment up to three years, or/and with fine up to ₹2,00,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹5,00,000
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person’s private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹2,00,000

The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

Continued….

Section	Offence	Description	Penalty
66F	Acts of cyber terrorism	If a person denies access to authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.
67	Publishing information Which is obscene in electronic form	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it	Imprisonment up to five years, or/and with fine up to ₹10,00,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexually explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹10,00,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child thus defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹10,00,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹10,00,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediately (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹2,00,000

The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

Continued….

Section	Offence	Description	Penalty
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹1,00,000

Legal Recognition of Electronic Records and Signature:

❖Recognition of electronic records:

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic Information Systems Control and Audit means. The Act states that unless otherwise agreed, an acceptance of the contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

❖Digital Signature (Amended Vide ITAA 2008):

Section 3 gives legal recognition to electronic records and digital signatures. The digital signature is created in two distinct steps. First, the electronic record is converted into a message digest by using a mathematical function known as the “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key that attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

❖Electronic Signature:

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. An Amendment to the IT Act in 2008, introduced the term electronic signatures. This Amendment implies that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

CYBER ETHICS

- **Cyber Ethics is** *a branch of computer technology behaviour that defines the best practices that must be adopted by a user when he uses the computer system*.
- In simple terms, **cyberethics** *refers to the basic ethics and etiquette that must be followed while using a computer system***.**
- **Ethics**, in general, refers *to propagating good behaviour*, similarly by **Cyber Ethics** we refer *to propagating good behaviour online that is not harsh or rude*.
- Cyberethics governs rules that *individuals must be polite and responsible when they use the internet*.
- Cyberethics *aim to protect the moral, financial, and social behaviour of individuals***.**
- Cyberethics *engages the users to use the internet safely* and *use technology responsibly and sensibly*.
- Cyberethics empathizes the behaviour that must be adopted while using cyber technology.

Some of the breaches of cyber ethics are listed below:

Continued….

- **Cyber Bullying:** Cyberbullying is a form of bullying carried out via internet technology such as social media where *individuals are mocked on their physical appearance, lifestyle, preferences, etc*. The *teenage generation or say youngsters are the major victims* of this form of cyber ethic breach. Cyberbullying *affects the emotional ethics* of individuals and can *cause mental disturbance* to individuals.

- **Hacking:** *Stealing a user's personal or organizational information without authorized permission* is not considered a good practice. It is one of the *riskiest cyber breaches to data leak*. Data leak includes passing of sensitive information such as *passwords, bank details of the user to a third-party user* who is not authorized to access the information.

- **Copywriting:** *Claiming of another individual as one's own* is another type of cyber ethic breach that must be eradicated. Never engage in copywriting another person's content or document and claim as it is your own. It leads to a serious problem called ***plagiarism***, which is *a punishable offense and considered a legal crime*. It is always advisable to follow general cyberethics, while using the internet or say any kind of technology. *A proper code of conduct must be followed* while using cyber technology. Cyberethics if not used wisely can lead to serious situations. Social and legal laws are defined to use cyber technology wisely. In extreme cases, legal action can be taken if there is a violation of cyber ethics.

Cyber Ethics focuses on the following:

1. Privacy:

- The content that is available on the internet should not hurt any moral, emotional, or personal ethics of individuals.
- *Users should have the right to protect any information which they don't want to share openly*.
- Private information *like user's contact details, address, security-related information like bank details, credit card/debit card details*, are all included in basic cyber ethics of user privacy and must not be breached in any case.
- Any breach of privacy is theft/fraud of user identity and user personal information, which is punishable as per the rules of law.

2. IPR:

- IPR stands for *Intellectual Property Rights*.
- IPR defines that the *owners have the complete right to the content that is posted on the internet*.
- The entire content is solely a belonging of the originator and *no individual is allowed to claim that content published by the original creator as its own*.
- Unauthorized distribution of someone else's work should never be adopted as it's ethically incorrect to not give creation and monetary benefits to the creator of the work.

Cyber Ethics focuses on the following:

Continued….

3. Security:

- Security on the internet is the *most basic ethical right* that every user must be accessible.
- Users of the internet should feel safe while they surf the net.
- Security, in general, means *only authorized users have access to the content on the computer*.
- *And confidential information is safe, without any risk of loss of information/content*.

Data Quality & Accuracy

4. Accuracy:

- The content available on the internet is accessed by billions of users.
- If there is no reliability of the information that is posted online, then it would mislead the masses.
- *Cyberethics assert the importance of posting content on the internet that is correct in all aspects*.
- *Users trust the content of the internet* and rely heavily on the internet for facts, therefore *it is highly needed that the asked information is correct and reliable*.

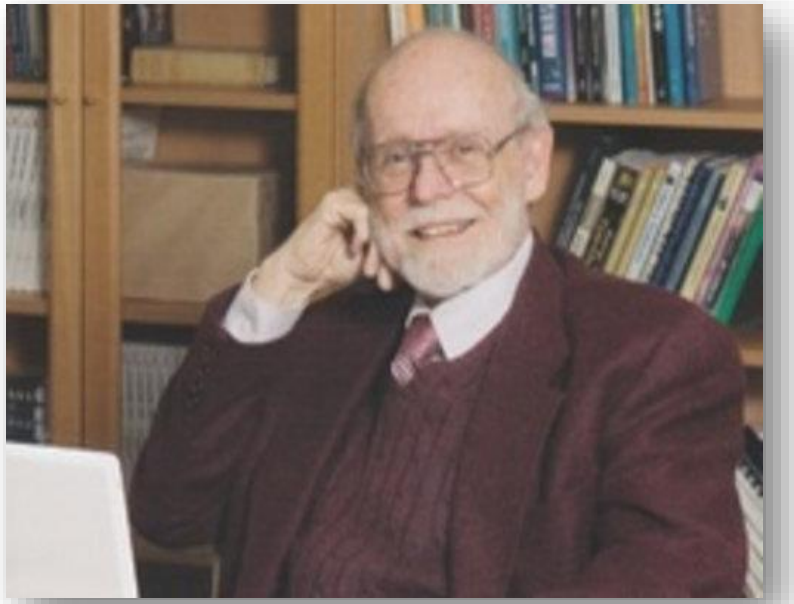
The best policies that individuals must adopt while using the internet or any kind of technology should include the following:

1. *Being Polite and not using harsh words.*
2. *Avoid clicking on unknown links.*
3. *Wisely opening Emails from known senders only.*
4. *Not mocking anyone on Social Media.*
5. *Not copying any individual's work and claiming it as their own. Always cite that you have used someone else's work.*
6. *Be careful and research before installing any free software.*
7. *Never intrude on another person's privacy.*
8. *Don't contribute to any malpractice that can lead to the leak of data of an individual or organization.*
9. *Never engage in Cyberbullying.*
10. *Never compromise the safety of your system. Always install an anti-virus on your system.*

INTRODUCTION TO CYBER ETHICS:

Continued….

Cyber ethics is the study of ethics pertaining to computers, *covering user behaviour* and *what computers are programmed to do*, and *how this affects individuals and society*. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics. *With the increase of young children using the internet, it is now more essential than ever to tell children about how to properly operate the internet and its dangers.*



Mr. Walter Maner

FOUNDATION OF CYBER ETHICS:

- Computer ethics was first coined by **Walter Maner**, a professor at Bowling Green State University.
- Maner noticed ethical concerns that were brought up during his Medical Ethics course at Old Dominion University became more complex and difficult when the use of technology and computers became involved.
- The conceptual foundations of computer ethics are investigated by information ethics, a branch of philosophical ethics promoted, among others, by **Luciano Floridi**.

HISTORY OF CYBER ETHICS:

- The concept of computer ethics originated in the **1940s** with MIT professor **Nobert Wiener**, the American mathematician and philosopher.
- While working on anti-aircraft artillery during World War II, Wiener and his fellow engineers developed a system of communication between the part of a cannon that tracked a warplane, the part that performed calculations to estimate a trajectory, and the part responsible for the firing.
- Wiener termed the science of such information feedback systems, ***"cybernetics"***, and he discussed this new field with its related ethical concerns in his 1948 book, Cybernetics.

IMPORTANCE OF CYBER ETHICS:

Continued….

- To *protect personal & commercial information* such as login & password info, credit card and account information and government and commercial databases. It also *controls unwanted internet mail and ads (Spam)*.
- To *control plagiarism, student identity fraud*, and the *use of copyrighted material*, etc.
- To *make ICT available and accessible to all people*, including the disabled and the deprived. Accessibility needs to be kept in mind during curriculum design (in educational contexts), to maximize the capabilities of the technology.
- To *suppress dishonest business practices* and to protect and encourage fair competition.
- To *promote moral and social values* in society.

RULES OF CYBER ETHICS:

(1) Do not break into someone else's computer or digital accounts.

(2) Do not plagiarize or copy other people's work without proper acknowledgement.

(3) Do not practice cyberbullying, harassment, or spread malicious content.

(4) Do not use rude, offensive, or discriminatory language online.

(5) Respect the privacy of others and do not share or expose their personal information without consent.

(6) Do not engage in hacking or unauthorized access to systems and data.

(7) Do not download or distribute illegal software, music, movies, or content.

(8) Avoid sharing false or misleading information (no spreading misinformation).

(9) Use strong and unique passwords to protect your digital identity.

RULES OF CYBER ETHICS:

Continued….

(10) Do not disrupt or harm network services or interfere with others' use of technology.

(11) Respect the digital property of others and adhere to intellectual property laws.

(12) Report suspicious or illegal activities to relevant authorities.

(13) Be cautious about the content you post or share, considering long-term impacts.

(14) Do not use technology to exploit or deceive others for personal gain.

(15) Follow rules and guidelines set by online communities and platforms.

(16) Protect your own data and devices with proper security measures.

(17) Always cite and give credit when using others' ideas, research, or media.

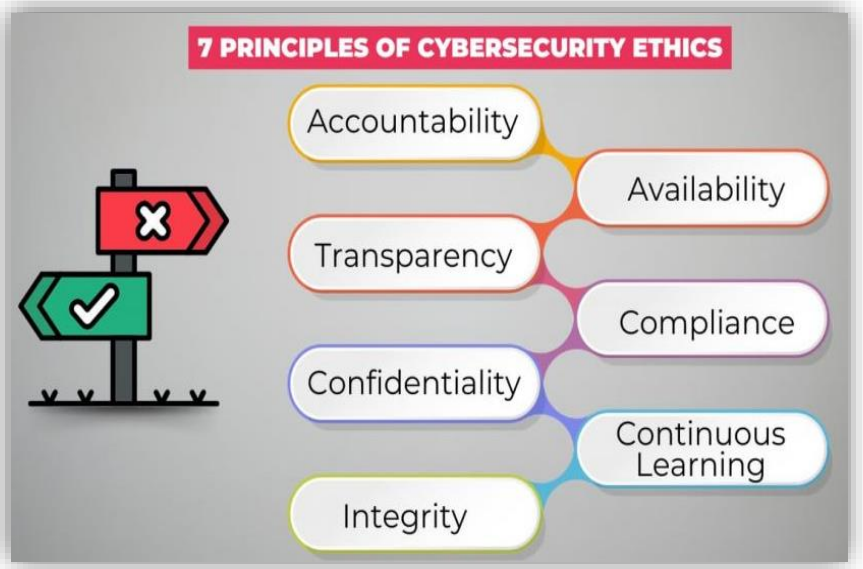
(18) Use the internet for constructive and positive interactions.

(19) Do not create or distribute harmful software (e.g., viruses, malware).

(20) Be mindful of your online presence and act responsibly in all digital interactions.

a) Responsible Behaviours On The Internet:

- Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life. The responsible behavior on the internet in many ways aligns with all the right behavior in everyday life, but the results can be significantly different.
- Some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep logs of their activities which can be used to spot illegal or inappropriate behavior.
- The Government has taken a positive role in making resources for parents and children to learn about cyber ethics. This is a growing problem and without parents and teachers using the resources available nothing can be done to prepare future generations of internet users from being safe online.



b) Crime And Punishment:

- Children do not believe that they will get into any real problem from neglecting the use of cyber ethics.
- It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust.
- The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

Lokmat Times

India is second in the world in terms of internet users, but it is far behind vis-a-vis cyber security

Cybercrime no less than terrorism

Vijay Darda

The news that the debit and credit cards of 1.3 million Indians are available for sale on a site on 'Dark Web' in itself is bizarre and worrisome. It is obvious that only cyber criminals will buy them and cheat or commit cyber robbery. This is not the first time this has happened. Only last year, it was reported that some 32 lakh debit/credit cards of Indians were hacked by criminals. How much loss has been caused to these card holders is not known exactly yet. Yes, it has been stated in the Norton Cyber Security Insight Report that in 2017, the Indians who were the victims of cybercrime lost $18.5 billion.

This report states that of all the people who use Internet in India, two of every five people invariably fall prey to some kind of cyber attack. They realise only after suffering the loss. The loss in India is usually not compensated. There are two reasons for this. One, there is no strong security system against cybercrime with no intensity in investigation and secondly, there is still not much awareness about insurance. There are only a few companies in the insurance sector which are offering this service. You will be surprised to know that the total cyber insurance business in India is only 1.6 per cent compared to the US. Most policies are taken by companies or institutions. Fewer people take the policy personally. This policy mainly compensates for losses due to recovery, phishing, email spoofing and unauthorised online transactions.

In America and the developed countries in Europe, the security situation seems much better. When my son Devendra was working after completing his studies in the US, the cyber criminals had withdrawn the entire amount from his bank account. After he complained to the bank, the matter was investigated promptly. You will be surprised to know that within eight days all the money was returned to the account. The situation is not so in our country even today. Although the Reserve Bank of India has issued several advisories, unfortunately there is no awareness among people.

Just as the world of internet is expanding, so are cyber criminals. From banks and big companies to the common man, everyone is under cyber threat. In fact, cybercrime is no less than terrorism by any measure. It is not only a financial robbery but also an attack on the right to privacy.

Recently, people received an SMS saying that an amount of ₹80,000 is being credited to their provident fund account. It also asked people to check their names in the list. When people opened the site, the PAN card number was being asked there. Obviously, those who did not exercise caution, must have fallen victim to it. Phishing messages in the name of banks and through phone calls keep coming but what is surprising is that people get trapped! In fact, with the world going digital at a faster pace, the threat of cyber attack is also increasing with the same speed. Your data is very important and it is being stolen. It is very difficult to understand when and how it will be misused.

A few days back, IT company Cisco released a report which clearly states that in the year 2018-19, there were a large number of cyber attacks on companies working in the field of banking, finance and infrastructure in India and on an average every company suffered a loss of about ₹35 crore. But I believe that if cyber security is given due attention, it can be dealt with. In September this year, the first National Conference on Cybercrime Investigation and Cyber Forensics was held at CBI headquarters in New Delhi. Let's hope a system will be put in place soon to enable India to crack down on cyber criminals.

There is an urgent need for India to be more vigilant because we are the second largest users of Internet in the world. Worldwide, 3.8 billion people use the Internet, of which 12 per cent are Indians. Even America, at eight per cent, is behind us. China is at number one with 21 per cent. We have many Apps to use for money transactions here. In such a situation, there is always a danger of cyber attack on banks. There have also been several incidents of Aadhaar data leakage. In fact, the companies to whom we give our data should also make strong security arrangements. Everyone knows the story of data leaks from Facebook. British Airways was even fined $229 million for this. Hackers are inventing new technology every day. We have to be on guard against them. I feel cybercrime is no less than terrorism by any measure. Terrorists kill people. Cyber criminals kill them financially.

And this news is worrying too that Indian politicians, businessmen, media houses, social activists, journalists and people associated with human rights are being spied through Israeli software. Congress on Sunday alleged that the party general secretary Priyanka Gandhi's phone was hacked too. NCP leader Praful Patel too fell victim to such an attack. The question that arises is who is spying. The answer to this question must be found. If this question is not answered, several doubts arise. Why was such a situation of doubts created should also be deliberated upon. The government should strictly tighten the screws on numbers of such cyber criminals so that no Indian is afraid that their personal information may get stolen. The government should assure that it is there to protect them!

The author is the chairman, Editorial Board of Lokmat Media and former member of Rajya Sabha. vijaydarda@lokmat.com

VIRUS | ATTACK

294 threat families were discovered on Android

Cyber criminals target city phones

DC CORRESPONDENT
HYDERABAD, SEPT. 3

Hyderabad is fast becoming a favourite destination for mobile malware after Chandigarh, Bengaluru, Chennai and New Delhi. With the numbers of smartphones skyrocketing and data usage expanding by the day, cyber criminals are attacking mobile phones.

Experts from the city said it is very important to update a computer or smartphone's software regularly. They claim that many email spam messages enable access to one's confidential information that is used by hackers without the owner's knowledge.

We have sometimes tried to test the strength of security, and trust me it is a cakewalk. People, whenever they get notifications for software update, must take it seriously and keep their devices updated

— A hacker

"We have sometimes tried to test the strength of security, and trust me it is a cakewalk. People, whenever they get notifications for software update, must take it seriously and keep their devices updated," said a hacker.

In the latest F Secure Lab's Threat Report H 1 2014, India is said to be the fourth most affected country across the world in mobile malware. Between April and June 2014, 295 new threat families were discovered, of which 294 were detected on Android and one on iOS.

Moreover, mobile ransomeware is going to be the next big threat to handsets. These ransomeware are also targeting enterprises. Ramsomware, a kind of malicious software, is designed to block access to a computer until a certain sum of money is paid.

Crime thrives online, little action on ground

LOW CONVICTIONS Experts blame lack of manpower, poor training

Vijay Kumar Yadav & Jayprakash S Naidu

MUMBAI: The state government in April this year, approved the setting up of four new police stations dedicated to tackling the rising cases of cyber crime in Mumbai. It also sanctioned creating 186 new posts, most of them to be filled by assistant police inspectors.

These units are yet to start work, but meanwhile, cases of cyber crime—which range from data theft to credit and debit card frauds and vishing—have steadily risen over the past three years. Convictions, however, have remained disproportionately low. According to the National Crime Records Bureau's (NCRB) 2016 report on crime, Mumbai ranked first in the country for cyber crime cases. From 2015, up until May 2018, 10,275 cyber crime cases were filed in Maharashtra. While 3,689 of these were solved by the police, just 93 of these cases went to trial. In all, since 2015, there have been convictions only in 28 cases.

"The detection (solving) rate depends on several factors," said Balsing Rajput, the superintendent of police (cyber).

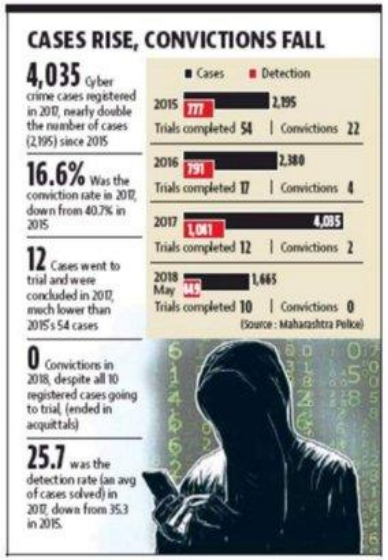
"It is difficult to extract information in cyber crime cases. There are many agencies involved, such as the internet service provider, the ones who provide media content on line, intermediaries like the banks and technology service providers. There is also the issue of international jurisdictions."

Rajput pointed out how in many cases, the fraudsters use SIM cards that they got after providing false information.

"The bank accounts of an illiterate person is used, after these fraudsters promise them a commission.".

Former Maharashtra director general of police and cyber crime expert, D Sivanandhan, said one of the main reasons for low detection and conviction rates was the lack of manpower and poorly trained police officers.

CONTINUED ON P10
RELATED REPORTS, P2



Crime thrives...

"Further, the law permits only officers from the rank of police inspectors and above to register and investigate the cyber crimes," he said, and added that the since cyber criminals operate online, many times from another state, it becomes difficult for the police to arrest them. "For this, we need a good inter-state and international network of officers, and improved coordination among investigative agencies."

At the trial stage, prosecutors and the judges also need to be updated about the growing incidents cyber crimes and the technology that is being used to cheat people. "This may help them better examine evidence, trials will be done faster, and conviction rates will improve. This is the missing link," Sivanandhan said. Special inspector general of police (cyber crime) Brijesh Singh also stressed on the need to better training and improved technology. "In the near future, we will have a centre for excellence where special training and information pertaining to cyber crimes and its investigations are provided to police, prosecutors and the judiciary. We will also have 44 cyber police units that have state-of-the-art technology."

Cops thwart attempt to siphon firm's ₹20-L payment

Jayprakash S Naidu

MUMBAI: The cyber cell at the BKC police station recently thwarted a man-in-the-middle (MITM) attack made on an agriculture trading firm and recovered ₹20 lakh that had been siphoned by the accused.

An MITM attack refers to a cybercrime wherein the attacker hacks into a company's email account, gathers information about transactions with other firms, and then poses as one of them in order to siphon the money being transacted between the two *(see box)*.

According to police, the complainant company, based in the city, had sold sprouts to a client company based in Madhya Pradesh (MP).

On January 17, the city firm emailed the GST invoice to the client and was to receive a payment of ₹20 lakh in return. On January 23, the client made the payment through a bank transfer.

Later that evening, the firm called the client to check on the status of payment. While the client claimed that the money had already been transferred, the company said it did not receive the payment.

Realising that it had been duped, the city firm approached the cyber police. "We immediately got in touch with the bank and froze the account to which the money had been transferred before it could be withdrawn by the accused," said an officer from the BKC cyber cell.

Explaining the modus operandi, the officer said, "The accused hacked the email id of the client company. After reading and copying the contents of the invoice sent by the Mumbai-based firm, the accused deleted it. The accused then created a new email id, identical to that of the Mumbai firm."

"Using the fake email id, the fraudster sent an email to the client company with the same contents, but a different bank account. The money was then transferred by the client into the accused's bank account," the officer said.

Officers from the BKC cyber cell have advised the client company to file a complaint with the local police in MP.

WHAT IS MAN-IN-THE-MIDDLE (MITM) FRAUD

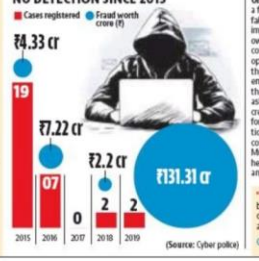
The man-in-the-middle (MITM) fraud/attack is a type of cybercrime, in which a fraudster secretly relays and alters communication between two parties through emails to make victims believe they are directly communicating with each other

The fraudster hacks into the official e-mail id of a company, which is in public domain, and gains information about the transactions that are to be made in future with another company

After getting the required information, for instance, invoices of previous transactions, the fraudster creates a fake e-mail id similar to the official e-mail id of beneficiary company and asks for money to be delivered to a new bank account

Insider could also leak information to hackers

NO DETECTION SINCE 2015



(Source: Cyber police)

COMPANIES UNDER ATTACK

European firm loses ₹130 crore

On November 13, 2018, a fraudster created a fake email account and impersonated the owner of a European company, which operates business in the city. He sent an email to the head of the Mumbai branch asking the latter to create a new email id for him for conversations related to a confidential deal. The Mumbai head did so, as he did not find anything amiss despite the email id below the header being a different one. As a part of business expansions in China, the fraudster asked the Mumbai head to deposit some money in a bank account. The city company transferred USD 18.6 million (₹130 crore) to accounts in China. The incident came to light on January 22 when the owner visited Mumbai from Europe and was informed about the incident.

"Fraudsters claim they are operating with new bank account because of government audits or that there is a problem with the current bank account."

Cyber police officer

Indian paint giant loses ₹28L

An Indian multinational paint company approached the cyber police on January 14 after it lost ₹28 lakh to man in the middle attack. The company had ordered raw materials from a Chinese company in December 2017. The fraudster made an email account similar to that of the Chinese company and asked the Indian company to send the money to a different bank account. The Indian company failed to notice the minor change in the email account. Between April and Dec 2018, the Indian company deposited ₹28 lakh in the accounts given by the fraudster.

'Fraudsters deposit money in Indian banks'

Jayprakash S Naidu

MUMBAI: The Mumbai cyber police said a new trend has been observed over the past few years in man-in-the-middle (MITM) attacks — the cheated money is being deposited in Indian bank accounts, unlike in the past when the money was deposited in bank accounts abroad.

A cyber police official said, "Prior to 2017, the money stolen by fraudsters in MITM attacks was getting deposited in foreign bank accounts. As per our records, prior to 2017, several crores of money in MITM attacks has been deposited in bank accounts in Poland, Hungary, Portugal, Dubai, China and Malaysia."

The official added that post 2016 after companies began to small foul play upon seeing bank accounts being opened in countries in which they did not operate, the attackers started teaming up with Indian nationals. A cyber police official said, "Most MITM cases in 2017 and 2018 have been registered at the police station level." Earlier, all cybercrime complaints used to be registered with the cyber police. However, now each police station in the city has its own cyber cell, which registers relatively minor complaints, in terms of the money involved. Officials said the police stations do not maintain statistics of MITM attacks.

Cyber advocate Vicky Shah said, "I have come across multiple cases where cyber criminals are operating from other countries and are teaming up with local fraudsters and vice-versa. This is a new trend. A lot of times during investigations the IP addresses are of other countries but one cannot say for sure if they are operating from the same country or not."

Cybercrime investigator Ritesh Bhatia said, "It's also important that all companies hold cybersecurity audits and awareness programmes at regular intervals."

Online markets are the new fraud hubs

Cons Pose As Armymen To Lure Buyers

POLICE VIGIL ON PORTALS

THE TIMES OF INDIA, KOLKATA
SATURDAY, FEBRUARY 22, 2020
TIMES

Man sent to jail for two years for harassing woman on social media

Convict To Also Pay ₹26k Fine

TIMES NEWS NETWORK

Kolkata: A Bidhannagar court on Friday sent a techie to jail for two years and fined him Rs 26,000 for allegedly threatening and extorting money from his former girlfriend, using social media. This is the first conviction in a case probed by the Bidhannagar Cyber Cell since its inception.

The accused, Jitender Singh Gerewal, had created five different fake profiles on Instagram and Facebook to carry out the crime. Both the convict and the complainant used to work in the same company for some time.

Bidit Mondal, OC, cyber cell, was the investigating officer. The charge sheet was filed in less than two months after the accused was nabbed after an 18-day probe.

According to Bivas Chatterjee, who represented the government in the trial for the past 15 months, on April 2, 2018, a complaint was lodged with the Bidhannagar cyber crime PS, stating that some objectionable photographs of the complainant had been uploaded onto some fake Facebook accounts.

During their relationship, the woman had been forced to appear in compromising positions over video calls. The accused used to record those videos and clicked screenshots. Later, when the complainant left the job, the accused started to threaten her with dire consequences as she refused to continue with the relationship.

TECHIE EX-COLLEAGUE OF COMPLAINANT

Convicted under	and a fine of ₹2,000	Instagram hack
IPC Sec 354 (molestation) | Jail for a year and a fine of ₹2,000	IPC Sec 507 (criminal intimidation) | jail for one year	In a case of professional rivalry, an MD of a private company complained to Bidhannagar cyber cell that her Instagram account was hacked, profile name and picture were changed, and her followers were deleted. TNN
IPC Sec 354D (stalking) | Jail for two years and a fine of ₹2,000	Sec 66C of IT Act | Jail for one year and a fine of ₹10,000	
IPC Sec 500 (defamation) | Jail for one year	67A IT Act | Jail for one year and fine of ₹10,000	
IPC Sec 509 (outraging modesty) Jail for one year	**All the terms of imprisonment will run concurrently**	

‘Public charging stations may put your data at risk’

Experts advise users to think twice before plugging to an unknown USB cord

Dhananjay Khatri
dhananjay.khatri@dnaindia.net

If your cell phone is out of battery and after desperately searching for a charging point, when you heave a sigh of relief after coming across a free USB port at the airport, shopping malls, mobile gallery or even a cafeteria, that's the moment you should think twice before plugging in the cord inside your phone as by doing so, you are allowing the access of malware in your device which can compromise your data. ‘Juice jacking’, as it is called by the cyber experts, occurs when the USB charging stations are modified by hackers so that whenever the phone is charged, the malicious element gets passed into the device.

“Charging your devices with any random USB wires is indeed equal to risk as after the charging is done, the device may function normally for a while but later, the malware starts performing its function which is indeed troublesome to get rid of. Through juice jacking, the phone gets vulnerable to allow incoming of all sorts of malware like adware, bots, spyware, etc. Plugging into a public USB cord is like picking any random stuff on the side of the road and meddling with it without even having the knowledge about the content it has. Juice jacking broadly performs three things which are the installation of malware, transmit other unwanted data and steal your personal information and other data,” cyber expert Ritesh Bhatia told DNA.

In order to escape from falling into the soup of such tedious cyberattacks, experts have prescribed some basic guidelines like charging the phone from a wall electric outlet using an adapter or always carrying a personal charger but the lack of awareness among the users is a result why such instances are reported. “The real issue apart from malware installation is the threat of ransomware which may emerge after critical data slips into the hands of miscreants. Speaking about Mumbai specifically, no such instance has come into the light but preparedness is required. People fail to discover about the presence of unknown devices behind the USB wires which cause unwanted trouble,” said Advocate and cybersecurity expert Prashant Mali.

Experts have suggested users to keep their personal chargers along with USB chord which prevents accidental data exchange.

‘JUICE JACKING’ POSES MAJOR THREAT

IS YOUR MOBILE PHONE DATA SAFE FROM SUCH A CYBER THREAT

- Keep the charger of your device with you and preferably the one which could be attached with electrical sockets.
- Carry your personal backup battery or a power bank so as to avoid finding charging stations and kiosk or wall outlet.
- A secured phone which is locked and protected by a password or a pin ensures there is invasion of malware.
- While charging the phone at public charging stations, switch off the phone as it averts possibility of malware attack.
- If possible, use a USB cable which enables only charging purposes to control the pairing behaviour of device.
- Disable data transfer feature on your mobile phones while charging.

WHAT IS JUICE JACKING

Juice jacking is an underrated serious security threat in which the setup of data or power supply through the same cable paves the way for malicious malware to gain access to your phones during the charging process. The attack could be as simple as an invasion of privacy wherein your phone, which is getting charged from a USB cable, pairs with the unknown source concealed with the charging kiosk and sensitive data like photos and contact information gets transferred to the malicious device. The term which was coined in 2011 simply refers to a hack attempt that uses public charging stations to inject the malware.

SUNDAY TIMES OF INDIA, INDORE
APRIL 8, 2018
TIMES

Rising ‘sextortion’ cases put cyber users on the edge

Video Calls, Chats Used To Blackmail Net Users

Karishma.Kotwal
@timesgroup.com

Indore: Small chat on messenger followed by a video call with exchange of compromising messages two months ago, changed the life of a 25-year-old IT professional Shikhar Singh (name changed) who became a victim when scammers from the other end started blackmailing him.

Shikhar had been in a relationship with a woman for past six years but the recorded video call and subsequent harassment that followed broke his ties with her.

He is one of the thousands of people in India caught by a growing internet scam the investigators call ‘sextortion’. Here the scamsters usually monitor activities of their targets online for days and weeks. After sifting through all the profile details, relationship links, profile pictures, activities and victim's habits based on the updates, a friend request is sent and conversation is initiated.

The woman on the other end sends objectionable pictures to the victim and asks him to do the same. In most of the cases, the video that victim sees is either a pre-recorded video or a completely fake one. While the victim imagines that he is chatting with a woman, there is a man who is texting him. They work in groups together.

Such scams wherein a victim is duped into performing a sexual act by unknown, attractive women, is rising in India. While women continue to be at the receiving end of revenge porn, online abuse and harassment, most of the victims are men, claim experts.

“In the past three months, ten people have come to me with such cases as they do not want to approach police. Six of them were men,” said Ritesh Bhatia, cyber expert.

Bhatia said that the crime ‘sextortion’ can be divided into three types – one which is done for physical relations, second is asking for more such videos and third is extorting money using the videos or images available. According to Bhatia, many cases similar to that of Shikhar have been recorded in the recent past.

The scammers also threaten to share the video of the sexual act with relatives or friends if the ransom is delayed.

Experts helping victims deal with such cases claim that such accused are part of sophisticated and organised gangs. While no police records are available on the increase in such cases in cyber space, cyber experts claimed that more than 50% women online have reported some or the other form of cyber abuse. “It can be anything starting from stalking, harassment, sharing obscene content etc,” said Shaik Javeed Ahmed, cyber expert.

Meanwhile, for Singh, the story is far from over. Weeks after the incident, he continues to live in fear. “He has deleted his Facebook account and is completely broken,” said the psychologist dealing with him.

TAKE PRECAUTIONS WHILE SHARING INFO ONLINE

- Use least amount of information necessary to register for and using the site. Opt for nickname or handle
- Use highest level privacy setting that a site allows & don't accept default settings
- Make sure you cover web cameras of laptops, mobile phone when not in use
- Verify emails, links in emails you get from social networking sites. They are often designed to gain access to your personal information

- Be certain of both the source and content of each file you download. When in doubt, don't open or download any content shared with you
- Never post publicly your address, phone number, driver's licence number, Aadhaar number, PAN card or student ID number
- Only connect with people you know and trust
- Read privacy and security policies closely - know what you are getting into. Some major social networking sites actually say they will use or sell information about you in order to display advertising or other information they believe might be useful to you

Cyber bullying makes the victims feel extremely guilty

Q&A
Nirali Bhatia
psychologist

How many cases of cyber bullying and sextortion do you come across every month and how you deal with the victims?
I deal with a number of cases on a day to day basis through social media, over mails or calls. Most of the victims, who approach me, come with extreme suicidal thoughts. I first make sure that they are safe and then speak about the issue. We provide whatever technical help we can but once a video or a picture is uploaded, it is very difficult to take it back. So it's important that the victim is counselled in a proper way to deal with the situation.

How does cyber bullying affect the victims?
The impact of cyber bullying and sextortion on the victims is so severe that they feel extremely guilty. We have to put them on medications as the trauma is deep and painful. In one of the cases, the victim was so paranoid after the incident that he stopped using social media and used to think that people are staring at him.

What should people do to avoid being dragged into such crimes?
One should always stick to basic instinct and common sense to avoid such things. If you feel that someone seems suspicious, do not talk to that person. Even if you fall prey to sextortion or cyber bullying, remember that it's not the end of the world and you can be saved by right kind of technical and psychological help.

SOME RUSES USED BY FRAUDSTERS

- Say they are calling from the bank to reactivate a credit card or debit and obtaining vital information
- ‘Selling’ insurance policies in the name of various private companies
- Use the offer of a loan to obtain vital data to hack account and misuse credit or debit cards

HOW THE MONEY IS REDEEMED

- The victim's card or information is used to make purchases on fake shopping websites, which deposits the money into an account or e-wallet linked to the site. The money is then transferred to the account of someone who needs to show income in business in return for cash
- Money is sometimes directly transferred into the accounts of people who have been hired on commission basis and is then withdrawn

CARD-SWIPING DEVICES ALSO USED: “Most of the financial cybercrimes executed without getting the victim to divulge their OTP are done using the chip in the card using a card swiping machine. Once the victim's card is swiped, the vital information on the chip is obtained and fake cards are made using this information. The involvement of some bank employees in providing customer data to scamsters cannot be ruled out,” said Bijoy Patel, a cyber crime expert.

80% OF CASES FOR FINANCIAL CHEATING, 20% FOR FAKE PROFILES: Senior cyber cell officers said 80% of cyber crime cases are financial crimes. “About 20% of them involve money being siphoning off without even obtaining OTPs. Some 20% relate to fake profiles being put up on social media with vindictive intentions,” said a senior cyber cell official.

JHARKHAND, DELHI TURNING INTO CYBERCRIME HUBS: Cyber cell officials said Jharkhand and Delhi have become hubs for such gangs. We are hunting for one kingpin, Tiku Mandal, who runs such rackets from Jharkhand and Samir Khan of Delhi, said a cyber cell officer.

HOW TO STAY SAFE

- Don't provide bank, credit or debit card details over the phone to people who may say they are bank officials
- Be caution about using debit or credit cards at shady places
- Never divulge the three digit CVV number of a card or the OTP sent to your phone or email

Many B’lureans lose cash to sim card swap fraud

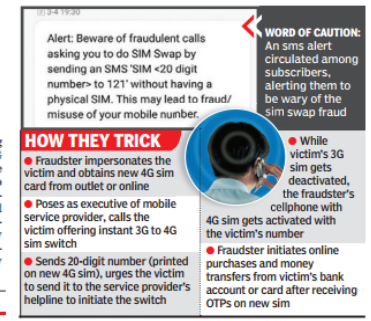
Bank Insiders Part Of Ploy: Investigators

Petlee.Peter@timesgroup.com

Bengaluru: If you are using a cellphone number with a 3G sim card and your online banking account is linked to it, you could be the next victim of a thriving ‘sim card swap fraud’. At least 30 Bengalureans have reportedly fallen prey to scamsters, losing huge sums of money since mid-2016.

BEWARE THE TRAP

For insurance executive Aroop Ghosh (39) from Domlur, the ordeal began when he attended a phone call at his lunch table in mid-February. “The male caller claimed he was calling from a mobile service provider and confirmed with me if I was still using a 3G sim. He told me that there is an offer for easy swapping to 4G for better internet speed and sent me a 20-digit number by SMS after disconnecting the call,” he said.



An ignorant Ghosh took the bait by texting the 20-digit number to the mobile service provider's helpline and selected option 1 to confirm the 4G swap as advised by the conman. “Within a few seconds my sim card got deactivated and it remained so,” rued Ghosh. The following day, electronics good worth over Rs 2 lakh were purchased online using his HDFC bank account.

According to an investigating officer with the CID's cybercrime unit, the modus operandi is thus: The culprits obtain a new 4G sim for the victim's cellphone number by either impersonating him at an outlet of the service provider or online, using the 4G sim swap page on the service provider's website. The new sim is then delivered to the given address within a day.

“The culprits then call the victim claiming to be executives from the service provider and send the 20-digit number printed on the new 4G sim card via SMS and convince him or her to activate it. Once the 3G sim on the victim's cellphone becomes inactive, the 4G one on the fraudsters' cellphone becomes active. The fraudsters then use it to receive OTPs,” the officer added.

Investigators suspect the scamsters must be obtaining victims' confidential bank account or card details, including cellphone details, from bank insiders. “They try every number pertaining to the accounts and some 3G sim card users fall for it,” the officer added.

Over 30 victims of the sim swap fraud have approached cybercrime police stations of state CID and Bengaluru city police (BCP) since mid-2016.

Some like Manish Raj, a city-based BPO employee, who are tech aware have also fallen prey to the fraud. “I didn't receive a call but only an internet-generated SMS with the 20-digit number from the fraudster, which I carelessly activated and lost Rs 30,000 from my ICICI account,” recalled Raj.

(Names of victims have been changed on request).

Continued….

Following some issues are increasing daily due to children using the internet improperly and we have to take care of it:

EXAMPLES:

I. COPYRIGHTING OR DOWLOADING –

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search what they need from the web and download it for their purpose. Their thinking is like "if everybody is doing it therefore it's ok", but an understandable and an appropriate lesson on Cyber Ethics could help children *to learn the risks involved in Internet downloading*.

II. CRIME AND PUNISHMENT –

Children do not believe that they will get into any real problem from neglecting the use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

III. INTERNET HACKING –

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance.

IV. CYBERBULLYING –

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance. When a child encounters cyber bullying that they should:* Tell a trusted adult, and keep telling them until they take action.

NOTE: (a) Avoid to open, read or respond to messages from cyber bullies; **(b)** Always keep messages from bullies. They may be needed to take corrective action; **(c)** Use software to block bullies if they encounter them through chat or IM.

Five Provisions of Cyber Ethics:

- Your computer or system should not be used to harm others.
- Your cyber knowledge should not be used to steal other people's resources.
- One should not use or copy softwares for which you have not paid.
- You should not break into someone else's accounts.
- Never use other people's resources without their consent.

DO'S AND DON'T IN CYBER ETHICS:

	Do's	Don't
School Work	Use the internet to help you to do the homework. You can find many information inside the internet.	Don't copy other people works and call it your own. Give credits to the author or the website.
Music, Videos and Copyright	Use the internet to learn about music, video and games.	Don't use the internet to download or share copyrighted material.
E-mail and instant messaging (IM)	Use the internet to communicate with friends and family. But make sure you know to whom you exchange your email and IM.	Don't use the internet to communicate with strangers. Don't pretend to be someone else and don't be rude or use bad language.
For Parents	Encourage your children to use the Internet. The Internet has a lot good things to offer children.	Don't leave your children unsupervised. Make sure you know what sites your children visit when they're on the Internet, and with whom they're communicating.

CHILD SEXUAL ABUSE MATERIAL (CSAM) RELATED TO CYBER DOMAIN

- **Child Sexual Abuse Material (CSAM)** is a serious issue in the cyber domain that involves the **illegal creation, distribution, and possession of explicit content depicting children**. Addressing this issue involves understanding key points and best practices:

Important Facts:

- *Illegal Content:* CSAM refers to any content depicting sexual abuse or exploitation of children. It is illegal in all its forms globally.
- *Severe Consequences:* Engaging in or facilitating CSAM can lead to severe criminal charges, including long-term imprisonment.
- *Digital Platforms:* CSAM can be distributed through websites, social media, encrypted messaging services, and peer-to-peer networks, making it challenging to detect.
- *Anonymity and Dark Web:* Offenders often use tools to stay anonymous, such as VPNs or accessing content through the dark web, which adds to the complexity of combating it.
- *Technology and AI:* Law enforcement agencies utilize AI, machine learning, and other technologies to identify and track CSAM content and perpetrators.
- *Online Grooming:* Predators may use social media, chat rooms, and gaming platforms to groom children and solicit CSAM or arrange in-person abuse.

Guidelines and Best Practices:

- *Report Suspected Material:* Immediately report suspected CSAM to local authorities or national hotlines such as the National Center for Missing & Exploited Children (NCMEC) or other relevant organizations.
- *Educational Programs:* Promote digital literacy and safety education for children and parents to recognize and avoid potentially dangerous online interactions.
- *Security Measures:* Use robust filtering and security settings on devices and accounts to prevent unwanted contact and access to harmful content.
- *Tech Company Accountability:* Support legislation and compliance measures that require tech companies to proactively monitor, report, and remove CSAM from their platforms.
- *Victim Support:* Ensure support and resources are available for victims of CSAM, including counseling and rehabilitation services.
- *Data Privacy and Encryption:* Balance the need for user privacy with effective measures to identify and prevent CSAM. Encryption must not become a shield for such content.
- *International Cooperation:* Strengthen collaboration between countries to share information, strategies, and resources for combating CSAM across borders.
- *Training for Law Enforcement:* Ensure that law enforcement agencies receive adequate training on digital forensics and best practices for investigating CSAM-related crimes.
- *Parental Controls:* Use parental control tools and monitoring software to limit children’s exposure to inappropriate content online.
- *Awareness Campaigns:* Run campaigns to inform the public about the dangers of CSAM, how to report it, and the importance of protecting children online.

- Tackling CSAM in the cyber domain requires a multifaceted approach involving individuals, organizations, and governments to ensure children's safety and prosecute offenders effectively.

- United States federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (a person less than 18 years old). Outside of the legal system, National Center for Missing and Exploited Children (NCMEC) chooses to refer to these images as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted – the sexual abuse and exploitation of children. Not only do these images and videos document victims' exploitation and abuse, but when these files are shared across the internet, child victims suffer re-victimization each time the image of their sexual abuse is viewed. In a recent survey led by the Canadian Centre for Child Protection, 67% of CSAM survivors said the distribution of their images impacts them differently than the hands-on abuse they suffered because the distribution never ends and the images are permanent.

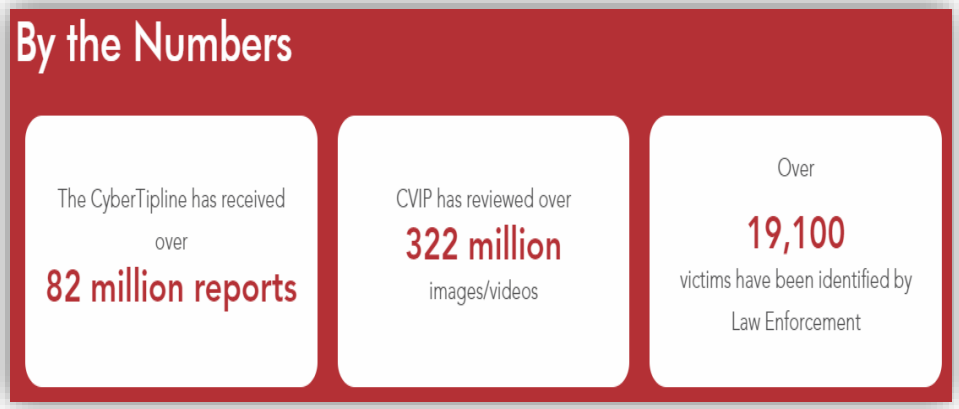
- It's important to remember CSAM consists of much more than just images and video files. While CSAM is seen and transmitted on computers and through other technology, these images and videos depict actual crimes being committed against children. The human element, children at risk, must always be considered when talking about this offense that is based in a high-tech world.

- The disturbing reality is that the internet platforms we use every day to connect with each other and share information, including social media, online gaming, and e-mail, are now being used to disseminate and collect CSAM. CSAM can be found in virtually any online realm.

Who are the Victims?

While there is limited research regarding victims of child sexual abuse material, it is a growing field of research and study to better understand the child victims and the offenders.

In March 2018, two studies on this topic were released. The first study is Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims, which is based on data collected by NCMEC's Child Victim Identification Program (CVIP) through 2014. The second study is Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material5, which is based on data in Interpol's global system.



Below are key findings from these two studies:

- Girls appear in the overwhelming majority of CSAM.
- Prepubescent children are at the greatest risk to be depicted in CSAM.
- When boys are victimized, they are much more likely than girls to be subjected to very explicit or egregious abuse.
- On average boys depicted in CSAM are younger than girls and more likely to have not yet reached puberty.
- 78% of reports regarding online enticement4 involved girls and 15% involved boys (in 8% of reports, the gender of the child could not be determined).

WHAT NCMEC IS DOING ABOUT IT?

Continued….

Operating the CyberTipline

In 1998, with the help of a private donation and after receiving an increase in reports relating to the online sexual exploitation of children, NCMEC created the CyberTipline. The CyberTipline provides an online mechanism for members of the public and electronic service providers (ESPs) to report incidents of suspected child sexual exploitation including:

For definitions and more information on these reporting categories and/or to make a CyberTipline Report, visit report.cybertip.org.

- online enticement of children for sexual acts
- extra-familial child sexual molestation
- child pornography
- child sex tourism
- child sex trafficking
- unsolicited obscene materials sent to children
- misleading domain names
- misleading words or digital images on the internet

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

Proud Partner of INHOPE

As part of our work to prevent the further victimization of children and to discover trends that can assist in preventing these crimes, NCMEC staff may review content reported to the CyberTipline and then the reports are made available to law enforcement for their independent review.

Electronic Service Provider (ESP) Reporting

U.S. federal law requires that U.S.-based ESPs report instances of apparent child pornography that they become aware of on their systems to NCMEC's CyberTipline. NCMEC works closely with ESPs on voluntary initiatives that many companies choose to engage in to deter and prevent the proliferation of online child sexual exploitation images. To date, over 1,400 companies are registered to make reports to NCMEC's CyberTipline and, in addition to making reports, these companies also receive notices from NCMEC about suspected CSAM on their servers.

Are you an ESP who would like to register with NCMEC? Click here.

Assisting in Victim Identification Efforts

CVIP
CHILD VICTIM IDENTIFICATION PROGRAM

VIDENTIFIER
Special thanks to Videntifier.

The Child Victim Identification Program began in 2002 after NCMEC analysts repeatedly saw images of the same child victims in their reviews and began tracking which victims had been previously identified by law enforcement. So far, more than 19,100 children have been identified.

Today CVIP operates with a dual mission: help provide information concerning previously identified child victims, and help locate unidentified child victims featured in sexually abusive images so that they may be identified and rescued.

Additionally, the Child Victim Identification Program provides training and educational assistance to law enforcement and attorneys on how child victims of sexual exploitation can be identified.

Empowering Survivors

More and more, survivors of CSAM speak to the long-lasting damage and impact of their images and videos being circulated on the internet. The lack of control of both the files' existence and circulation leaves the survivors struggling in their recovery.

Using new technology and working with like-minded partners, NCMEC is working with the ESP industry and with children and their families to identify these images and have them tagged for removal from ESP servers. This empowers and allows law enforcement and child advocates to tell the survivors that something CAN be done to limit these files online and remove them when they are flagged.

NCMEC also provides information for survivors who want to take quick action if they are made aware of their images or videos online. Learn how to contact the internet service providers to report files circulating online.

Supporting Victims & Families

NCMEC provides assistance and support to families impacted by child sexual exploitation. We offer crisis intervention to families as well as local referrals to appropriate professionals for longer-term support. Families of exploited children often feel alone in their struggle and overwhelmed by the issues impacting their lives. NCMEC's Team HOPE is a volunteer program that connects families to others who have experienced the crisis of a sexually exploited child. These trained volunteers offer peer support, coping skills, and compassion.

In addition, NCMEC is committed to addressing the long-term needs of survivors of CSAM by providing resources and avenues for the continuum of care after the abuse has stopped. NCMEC is creating a network of mental health therapists that specialize in CSAM cases, education for legal professionals on how to seek restitution and represent survivors in court, and increasing awareness of the unique and sensitive nature of this crime to law enforcement and other child advocates. Our hope is that this holistic approach will provide the continuing and ever-changing support survivors need in the years following the abuse.

Preventing Abuse Through Education

NCMEC utilizes the expertise it gains by operating the CyberTipline and CVIP to create and provide prevention and educational programs to parents and guardians, as well as technical assistance and educational programs to the public, law enforcement and other child-serving professionals regarding child sexual exploitation. Using data from actual CyberTipline reports enables NCMEC to craft outreach messaging that takes into account trends in the sexual exploitation of children and provides prevention and educational resources to help address these issues. NCMEC's central education programs include NetSmartz and KidSmartz.

VARIOUS LAWS RELATED TO SOCIAL MEDIA

What is Social Media?

- The term social in regards to media suggests that platforms are user oriented and becomes a place for communal activity.
- As such, **social media** can be viewed as *online facilitators or enhancers of human network webs of individuals who enhance social connectivity*.
- Social media largely consists of tools for sharing and exchanging information that is based on the internet and mobile devices. It combines *technology, communications, and social interaction* and offers a *platform for exchanging ideas* through written words, images, moving visuals, and musical compositions.
- People from all age groups are attracted to social media, especially the youth since it gives a medium for them to express their thoughts and discuss issues.
- There are different types of social media such as ***social networking sites*** like ***Facebook, Instagram, Twitter, etc. Blogs, Vlogs, Social news, etc.*** all these options just make it easily accessible to people.
- There are many benefits of using social media such as *it helps in staying updated in current times, helps people to stay connected with friends, family, and relatives, easy to obtain information, easy banking*, and other facilities which facilitates people to get any work done easily.
- Despite all of its advantages, social media has several possible dangers: *Social media is not a problem itself, but it is due to the manner that people replace it for face-to-face connection. Fear Of Missing Out (FOMO)* has emerged as a widespread issue and frequently encourages constant social media site checking. Your *mental health may be impacted* by the thought that you could lose out on something if you are not online. This can also lead up to *spending more time online* than staying present in the real world. This doesn't mean that social media is a problem, anything that is used in excess can cause issues.

Laws relating to Social Media

Continued….

We live in a technologically advanced world when knowledge is readily available. However, the media plays a primary part in it, hence in India, the media is governed by various regulations and codes. Since its purpose includes the *public and national interest, regulation is important* since it is one of the industries that is believed to be developing.

The Information Technology Act, 2000:

Section 69 (A): This section says that government has the right to ban or stop public access to any information that is not consistent with provisions of the government, and this section also provides the procedure of blocking access of the public to certain information. Who doesn't comply with this provision will be punished with *imprisonment for a term which may extend to seven years and shall also be liable to pay a fine*.

Constitution of India

The Indian constitution provides certain basic rights to citizens of India. These rights protect their basic life interest and if it is violated remedy is provided to them. **Article 19** of the Indian constitution talks about the **Right to Freedom**, there is no specific mention of freedom of press/media but it flows through **Article 19(a)** which is the **right to freedom of speech and expression**. Dr. Ambedkar quoted, "Freedom of press is essential for political liberty. When men cannot freely convey their thoughts to one another, no freedom is secured, where freedom of expression exists the beginning of free society and means for every retention of liberty are already present.

"Free-expression is, therefore, unique among liberties". There is no specific clause for freedom of the press but liberty of the press is included in freedom of speech and expression. The press has no special rights or liberty as an entity but it has the same liberty and right as provided to individuals of the country under freedom of speech and expression. For example, we can say journalists, editors can claim freedom of speech and expression as any other citizen claims it under article 19(a). The Indian Press Commission has rightly opined that the democracy of a country cannot be protected only through the help of legislature but the opinion of people also matters and what better medium other than media/press.

Laws relating to Social Media

Continued….

Indian Penal Code

The official criminal code of India is known as the Indian Penal Code (IPC). It is a thorough code that aims to cover all important areas of criminal law. Any person who violated the laws mentioned above will be dealt with under the provisions of IPC.

- **Section 295A:** Defaming religion or religious beliefs on purpose.
- **Section 153A:** encouraging hostility between groups based on race, religion, etc.
- **Section 499** deals with defamation, according to this, anybody who makes a defamatory comment in writing or verbally with the goal to destroy someone's reputation faces legal consequences. Section 499 and 500 of the law are the primary safeguards against social media abuse.
- **Section 505** deals with statements that incite public annoyance.
- **Section 509:** Disrespecting women's modesty.
- **Sections 124A:** deals with sedition, which means that a criminal act that encourages opposition that has the potential to bring down the government.

Why Laws regarding Social Media are required?

Continued….

In India, the media is regarded as the fourth pillar of democracy. Since the legislative, executive, and judicial branches of government are adopting the same framework as India's regulatory system. Although certain controls for the press are absolutely important, there are currently no specific regulations in place in India. Even though we can see in the constitution that there is no specific article relating to media, it is just under article 19(1)(a) freedom of speech and expression.

As we are living in a highly technology-driven world where information travels quickly and is unaffected by distance, thus the media must play a constructive role. One false or inaccurate report might have a negative impact on society, spark riots, or incite hatred among the populace. It is the responsibility of the media to provide the truth in India, where people of many cultures and religions coexist, but also abstain from spreading false information and politicizing stories to raise popularity. It is very necessary to have certain reasonable restriction, which stops any media personnel from creating hatred, and communal problems but also safeguards his/her freedom of speech and expression.

Problems in regulating Social Media Laws

In India, many legislation and rules govern the media. Since its purpose includes the public and national interest, regulation is important as it is one of the industries that is considered to be developing. Every time a law is formed, it takes into consideration three factors: the law, the economy, and psychology as laws are primarily designed for the benefit of people. And because the media is one of the fastest-growing industries, there are growing worries about the need to establish a single legal framework to govern all types of media.

However, due to a large number of media organizations in India, we are having trouble controlling the media. They are defending it by expressing their desire for themselves. Self-regulation is maintaining the freedom of expression without engaging in censorship or self-censorship and instead establishing basic standards of truth and morality. But there are talks of having a specific legal framework for regulating media in India.

PRIVACY AND SECURITY ON CYBER DOMAIN

What is Cyber Security?

Cyber Security refers to a set of methods, technologies, and procedures for defending computer systems, networks, and data from cyber-attacks or unauthorised access. The primary goal of cyber security is to secure all organisational assets from external and internal threats, as well as disruptions caused by natural disasters.

A good security posture against malicious attacks intended at obtaining access to, changing, deleting, destroying, or extorting important data from an organization's or user's systems can be achieved with a strong cyber security plan. Cyber security is also important in preventing attacks that try to disable or impair the operation of a system or device.

Simply put, cyber security refers to the safeguarding of internet-connected systems, including hardware, software, and data, from cyber threats. This method is used by individuals and corporations to prevent unauthorised access to data centres and other digital systems.

Domains of Cyber Security

A good cyber security posture demands coordinated efforts across all of an organization's systems because its assets are made up of a range of different platforms. As a result, cyber security has the following sub-domains:

- ***Application Security:*** The installation of various defences within all software and services used within an organisation to protect against a wide variety of threats is known as application security. To limit the likelihood of any unwanted access or alteration of application resources, it necessitates creating secure application architectures, writing secure code, implementing strong data input validation, threat modelling, and so on.

- ***Identity Management and Data Security:*** Identity management refers to the frameworks, processes, and activities that enable legitimate individuals to access information systems within an organisation. Implementing strong information storage techniques that assure data security at rest and in transit is part of data security.

- ***Network Security:*** The implementation of both hardware and software techniques to secure the network and infrastructure from unwanted access, disruptions, and misuse is known as network security. Network security is important for protecting an organization's assets from both external and internal attacks.

- ***Mobile Security:*** Mobile security refers to safeguarding both organisational and personal data held on mobile devices such as cell phones, laptops, tablets, and other similar devices from dangers such as unauthorised access, device loss or theft, malware, and so on.

- ***Cloud Security:*** Cloud Security refers to the creation of secure cloud architectures and applications for businesses that use AWS, Google, Azure, Rackspace, and other cloud service providers. Protection against diverse dangers is ensured by effective design and environment configuration.

- ***Disaster recovery and Business Continuity Planning (DR&BC):*** DR&BC deals with processes, monitoring, alerts, and plans that help organisations prepare for keeping business vital systems online during and after a disaster, as well as restarting lost operations and systems.

Types of Cyber Security Threats

The latest cyber security risks are taking use of work-from-home environments, remote access technologies, and new cloud services to put a new twist on "well-known" attacks. The following are some of the evolving threats:

- ***Phishing*** – Phishing is the act of sending fake emails that look like they came from a credible source. The intention is to steal sensitive data such as credit card numbers and login credentials. It's the most common kind of cybercrime. Education or a technical solution that filters dangerous emails can help you protect yourself.

- ***Ransomware*** – Ransomware is a sort of malicious software that encrypts files and holds them hostage. Its purpose is to extort money by preventing access to files or the computer system until a ransom is paid. Payment of the ransom does not ensure the recovery of the files or the restoration of the system.

- ***Malware*** – Malware refers to harmful software types such as worms, viruses, Trojans, and spyware that allow unauthorised access to a computer or cause damage to it. Malware attacks are becoming increasingly “fileless,” and are designed to avoid detection technologies that scan for harmful file attachments, such as antivirus software.

- ***Social Engineering*** – Adversaries employ social engineering to mislead you into divulging crucial information. They can demand a monetary payment or get access to your personal information. To make you more inclined to click on links, download malware, or believe a malicious source, social engineering can be used with any of the risks outlined above.

- ***Distributed denial-of-service (DDoS) Attacks*** – A DDoS attack overloads a server, website, or network with traffic, usually from numerous synchronised systems, in order to bring it down. DDoS attacks use the simple network management protocol (SNMP), which is used by modems, printers, switches, routers, and servers, to overwhelm enterprise networks.

- ***Man-in-the-middle Attacks*** – An eavesdropping attack in which a cybercriminal intercepts and relays messages between two parties in order to steal data is known as man-in-the-middle. An attacker, for example, can intercept data passing between a guest's device and the network on an insecure Wi-Fi network.

Challenges in Cyber Security

Hackers, data loss, privacy, risk management, and changing cyber security methods are all constant threats to cyber security. The number of cyberattacks is unlikely to reduce very soon. Furthermore, additional attack access points, such as the internet of things (IoT), raise the need to secure networks and devices.

The ever-changing nature of security vulnerabilities is one of the most difficult aspects of cyber security. New attack channels emerge as new technologies emerge and as technology is exploited in new or different ways. It can be difficult to keep up with the constant changes and advancements in attacks, as well as to update practises to protect against them. Among the issues is ensuring that all aspects of cyber security are kept up to date in order to protect against potential vulnerabilities. Smaller businesses without staff or in-house resources may find this particularly tough.

Furthermore, organisations can collect a wealth of information about individuals who utilise one or more of their services. The likelihood of a cybercriminal attempting to steal personally identifiable information (PII) increases as more data is collected. An organisation that saves PII on the cloud, for example, could be the target of a ransomware attack. Organizations should do all possible to avoid a cloud breach.

Employees may bring malware into the office on their laptops or mobile devices, thus cyber security strategies should include end-user education. Employees who receive regular security awareness training will be better able to contribute to keeping their company safe from cyberthreats.

Another challenge with cyber security is a scarcity of competent cyber security professionals. As businesses acquire and use more data, the demand for cyber security professionals to assess, manage, and respond to incidents grows. The workplace gap between needed cyber security jobs and security specialists, according to (ISC)2, is expected to be 3.1 million.

Why Cyber Security is Important?

Networks, computers, and other electronic devices, as well as software applications, are facilitating all parts of our life as human civilization becomes more digital. Since government, military, business, financial, and medical organisations acquire, process, and store massive amounts of data on computers and other devices, cyber security is critical.

Sensitive data, such as intellectual property, financial data, personal information, or other sorts of data, might make up a considerable amount of that data. Unauthorized access or exposure to that data can have serious implications. In the course of doing business, companies send sensitive data across networks and to other devices, and cyber security refers to the discipline committed to safeguarding that data and the systems that process or store it.

Companies and organisations, particularly those responsible with preserving information linked to national security, health, or financial records, must take efforts to protect their sensitive business and people information as the volume and sophistication of cyberattacks grows. Threat actors have more motivation than ever to breach those computer systems for monetary gain, extortion, political or social motives, or simply vandalism.

Cyberattacks have been undertaken against key infrastructure in all industrialised countries during the last two decades, resulting in devastating losses for many organisations.

THANK YOU

Best of Luck!