**Cyber-crime definition and origins of the world**

**Definition:** Cybercrime is any illegal activity that involves a computer, network or the internet. Basically, if someone uses technology to commit a crime, it’s called cybercrime.

**Origin of Cybercrime:**

1. **Early Days (1960s-1970):** It started with “Phone phreaking”, where people manipulated phone systems to make free calls

2. **1980s**: Hacking become popular as computer started connecting to each other. People like Kerin Mitnick became famous for breaking into

systems.

3. **1990s**: With rise of the internet, more people went online and cybercrime grow. Viruses and malware began to spread.

4. **2000s**: Organised crime groups formed online, using techniques like phishing (fake email/websites) and identify theft to steal information

5. **2010s-Present**: Cybercrime has become very advanced. Ransom ware (locking files and demanding money) and cyber espionage (spying) are common

**Purpose of Cybercrime :**

The purpose of cybercrime varies but generally includes:

1. Financial Gain: Stealing money or financial information.

2. Data Theft: Acquiring sensitive information.

3. Disruption: Causing service or network disruptions.

4. Espionage: Gathering confidential information for political, economic, or military purposes.

5. Identity Theft: Stealing personal information to commit fraud.

6. Political Motives: Promoting political agendas or social causes through activism.

**Cybercrime and information security**

Cyberspace means virtual environment created by computer networks and the Internet. It includes all the interconnected system such as websites, apps, social media platforms, emails and digital communication channels.

It also includes:

* Internet & Websites – Platforms where users browse, search, and access information.
* Online Communication – Emails, social media, and messaging apps that connect people.
* Digital Transactions – Online banking, shopping, and financial payments.
* Cloud Storage – Storing files and data on the internet instead of personal devices.
* Cyber Activities – Hacking, ethical hacking, digital marketing, and software development.
* Smart Devices – IoT devices, mobile phones, and smart gadgets connected via the internet.
* Gaming & Virtual Reality – Online multiplayer games and virtual worlds.

It is essentially a digital world where information is created, shared and stored.

Relation with cyber security:

Cyber security focuses on protecting cyberspace from harm such as hacking viruses or data theft. Since, cyberspace is used for storing personal information, financial information and business information it is at risk of being attacked by cyber criminals.

Cyber Security Works to:

1. Protect the data like sensitive information - Passwords, bank details and private messages.

2. Secure the devices like phones, computers, laptops, tablets and make secure them from harmful softwares or unauthorized access.

3. Defend the networks by securing the Internet connections and prevent cyber attacks on systems like Wi-Fi or corporate networks.

Example:

* We use antivirus to protect devices from harmful softwares in cyberspace.
* We use firewalls to block unwanted access to network.

**Classification of cybercrimes**

**I. Cybercrime Against Individuals**

These crimes directly target individuals, affecting their personal information, online security, and digital well-being.

* Email Spoofing – A technique where the sender’s email address is forged to appear as if it is coming from a trusted source, often used in scams.
* Phishing (Vishing, Smishing, Spear Phishing) – Fraudulent attempts to obtain sensitive information like passwords, credit card details, or personal data through emails (phishing), phone calls (vishing), or SMS (smishing).
* Spamming – Sending a large volume of unsolicited messages, often containing advertisements, malware, or phishing attempts.
* Cyber Defamation – Using online platforms to spread false information that damages a person’s reputation.
* Cyber stalking & Harassment – Persistent online threats, tracking, or intimidation of an individual, causing fear and distress.
* Computer Sabotage – The deliberate destruction or disruption of computer systems, often through malware or hacking.
* Password Sniffing – Intercepting and stealing login credentials using software or hardware tools.

**II. Cybercrime against Properties**

These crimes involve the unauthorized use or damage of digital assets, financial resources, and intellectual property.

* Credit Card Fraud – Stealing credit card details to make unauthorized transactions.
* Intellectual Property Crime – Violating copyrights, trademarks, or patents by distributing or using protected content without permission.
* Internet Time Theft – Unauthorized use of someone’s internet bandwidth or services without their knowledge.

**III. Cybercrime against Organizations**

These attacks are directed at businesses, government institutions, or corporate entities, aiming to disrupt operations or steal data.

* **Unauthorized Access of Computers (Hacking)** – Gaining illegal access to a computer system to steal or manipulate data.
* **Password Sniffing** – Capturing credentials to access restricted systems or steal sensitive information.
* **DoS Attack (Denial of Service)** – Flooding a network or server with traffic to make it unavailable to users.
* **Virus Attacks / Dissemination of Viruses** – Spreading malicious programs that harm systems and compromise data security.
* **Email Bombing / Mail Bombs** – Sending a large volume of emails to overload and crash an email server.
* **Salami Attacks / Salami Techniques** – Conducting small, undetectable financial frauds by taking minor amounts from many transactions.
* **Logic Bomb –** A hidden piece of malicious code that activates under specific conditions to cause damage.
* **Trojan horse** – A deceptive software program that appears useful but contains harmful malware.
* **Data Diddling** – Altering data before or during processing to commit fraud.
* **Crimes from Usenet Newsgroups** – Sharing illegal content, including pirated software, extremist propaganda, or malicious code.
* **Industrial Espionage** – Illegally spying on competitors to gain trade secrets or confidential data.
* **Software Piracy** – Unauthorized copying, distribution, or use of software without a license.

**IV. Cybercrime against Society**

These crimes have a broader impact, affecting the general public or national security.

* **Forgery** – Creating fake digital documents, such as passports, ID cards, or contracts, for fraudulent purposes.
* **Cyber terrorism** – Using digital means to carry out acts of terrorism, such as hacking critical infrastructure, spreading extremist propaganda, or causing public fear.
* **Web Jacking** – Taking control of a website by exploiting security vulnerabilities, often to spread misinformation or demand ransom.

**V. Crimes Emanating from Usenet Newsgroups**

These crimes arise from the misuse of online discussion forums (Usenet newsgroups), leading to illegal activities.

* **Illegal Content Sharing** – Posting or distributing pirated software, copyrighted materials, or confidential data.
* **Hate Speech & Extremist Propaganda** – Spreading hate speech, inciting violence, or radicalizing individuals online.
* **Fraudulent Activities** – Using newsgroups to promote scams, phishing schemes, or fake investment opportunities.
* **Malware Distribution** – Sharing virus-infected files or malicious software disguised as legitimate downloads.
* **Drug & Weapon Trade** – Facilitating illegal transactions involving drugs, firearms, or other illicit goods.

**Cyber defamation**

**Cyber defamation** is a cognizable offence. In section 499 of chapter XXI of IPC, regarding ‘defamation’ there is a mention that “Whoever by words either spoken or intended to be read, or by signs or by visible representation, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm the reputation of such person, is said, except in the case herein after expected, to defame that person.”

Cyber defamation happens when the above takes place in an electronic form. Defamation can take any form, including spoken or written words, gestures or images.

Defamation can be divided into two categories: Libel and Slander.

Libel is the written or published form of defamation, such as newspaper article, a blog post, or a social media post. Slander is the spoken form, such as false statements made in a conversation or a public speech.

Essentials to prove cyber defamation:

* The defamatory statement must be published, which means it must come to the attention of the 3rd party.
* The statement must refer to the plaintiff.
* The statement should be defamatory in nature.

**Web jacking, Forgery, Pornographic offences**

1. **Pornographic offenses**

· This offense involves the creation, distribution, publication, or access to absence and sexually explicit digital content.

· An Internet is being highly used by its abusers to teach and abuse children sexually worldwide.

· An Internet has become cheaper its exclusion has made the children a viable victim to the cybercrime.

· As the broadband connection get into reach of more and more homes, larger child population will be using the Internet and therefore large population get affected by such digital content.

· This results in the more children’s gate falling into the aggregation of pedophiles, “pedophiles” are people whose sexually or psychologically, force minors to engage in sexual activities which the minors could not cautiously consent to.

· Engaging in such activities can lead to severe legal consequences, including imprisonment, fines and a permanent criminal record.

· Cyber criminal may use hidden online platforms encrypted communication or the dark web to distribute such content making it harder for the law enforcement to track them.

Preventive Measures:

· Street container moderation, cybersecurity policies for online platforms.

· Awareness programs to educate users about the risk and consequences.

· Safe browsing to block user access to websites containing dangerous or offensive material.

1. **Forgery**

· Digital forgery refers to the act of falsifying or manipulating digital documents signatures images or identities to deceive others.

· Common example include fake digital certificate, forged back documents, manipulating emails and fraudulent digital transactions.

· Outside many colleges there is a sale of fake marksheets and degrees, It is one of the type of forgery.

· This becomes business involving large monetary amount given to student gangs in exchange for this bogus but authentic looking certificates.

· Such acts are considered cs cybercrimes as they can read to financial fraud and identity theft.

**Preventive measures:**

· Organization can implement security measures such as digital signatures, blockchain technology and encryption to prevent forgery and ensure document authenticity.

· Penalizing the people involves in the forgery activities and implementing stick laws.

1. **Web Jacking**

· Web Jacking is a form of Cybercrime wear hackers take control of website by exploiting vulnerabilities, hijacking domain names or allowing dns settings.

· Attackers may use fishing malware or brute force attacks to gain authorized access to websites administration.

· It occurs when someone forcefully takes control of a website.

· Web jacking is a serious threat to business as it can lead to financial losses, reputational damage and legal liabilities.

· The first step in web jacking is “password sniffing”, actual owner of the website does not have any more control over what appears on that website.

Preventive measures:

· Website owners should use strong authentication methods example two factor of authentication.

· Update softwares regularly.

· Monitor dns records and apply web security solutions like Firewalls and Intrusion detection systems.

· Penalties for web jacking activities.

**Software piracy**

Cybercrime is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them

There are five types of cyber crimes

* cyber-crime against individual
* crime against property
* crime against society
* crime against organizations
* crimes imaginating from Usenet Newsgroups

So in all this software piracy is a cyber-crime against organisation

Software Piracy is the illegal approach of unauthorized copying, distributing, modifying, selling, or using software that is legally protected.

In a simple term, we can say Software piracy is the act of stealing legal software.

**Software piracy** can be performed by **various types** such as

**1.** **Soft lifting**

In this piracy, the legal owner of the software is one, but others will illegally use that software by downloading the software to their computer. For example, many times we borrow software from our colleagues and install a copy of that on our computers just to save money which rises to soft lifting

**2. Hard-disk Loading**,

It is one type of Commercial software piracy which mainly happens in PC resell shops The shop owner buys a legal copy of the software and reproduces its copies on multiple computers by installing it. Most of the time customers/PC users are not aware of these things and get the pirated version of the software in the original S/W price or less than the original price

**3. Counterfeiting,**

Counterfeiting is a form of piracy that occurs when software is illegally copied and distributed under the guise of authenticity. Counterfeit software programs are usually sold at a cheaper price than the real thing, which may be attractive to certain buyers.

**4. Licenced overuse**

License overuse can be intentional or caused by a lack of asset management protocols.

Examples include:

• When too many people on the same network use a single, original copy of a piece of software simultaneously

• Or the software is used outside the location or company domain

• Or the license is based on named users, but multiple users access the software

**5.** **Online Piracy**

In online piracy, the illegal software is acquired from online auction sites and blogs which is mainly achieved through the P2P(Peer to Peer File Sharing)system. As it is acquired using the Internet, often it is called Internet Piracy.

Also software piracy can happen by

• **Downloading from unauthorized sites:** Downloading software from sites other than the official publisher's distribution stream

**• Using software beyond license agreement**: Using a software copy on more users or computers than the license agreement allows

• **Installing unauthorized software**: Installing unauthorized copies of software onto a computer's hard disk

• **Duplicating software**: Duplicating software programs that were purchased legitimately

**• Gaining illegal access to software**: Gaining illegal access to protected software, also known as "cracking"

People downloading pirated software for personal use

Companies installing unlicensed software on their computers to cut costs

Criminal networks that distribute pirated software on a large scale

**To prevent software piracy:**

• Purchasing licensed software: Always buy software from authorized retailers

• Using strong anti-virus software: Detect and block potential threats related to pirated software

• Educating users: Raising awareness about the consequences of software piracy

**Credit card frauds**

Credit card fraud is a financial crime where an unauthorized person misuses someone else's

credit card information to make purchases, withdraw money, or commit fraudulent activities. It can lead to financial losses for individuals, businesses, and banks. With the rise of online

transactions, fraudsters have developed more sophisticated techniques to steal card details and

exploit vulnerabilities.

**Common Types of Credit Card Frauds**

**1. Card-Not-Present (CNP) Fraud**

○ This occurs when a fraudster uses stolen credit card details for online, phone, or

mail transactions where the physical card is not required.

**2. Card Skimming**

○ Fraudsters install skimming devices on ATMs or point-of-sale (POS) machines to

secretly capture card information, allowing them to create a duplicate card.

**3. Lost and Stolen Card Fraud**

○ If a credit card is lost or stolen, it can be used by fraudsters for unauthorized

transactions before the owner reports it. This is commonly used for small

purchases that do not require PIN verification before the bank blocks the card.

**4. Phishing and Social Engineering**

○ Scammers trick victims into revealing their credit card details by sending fake

emails, messages, or phone calls pretending to be from a bank or a trusted

institution.

**5. Identity Theft**

○ Criminals use stolen personal details like Aadhar, PAN, and banking credentials

to apply for credit cards in someone else's name.

**6. Account Takeover**

○ In this type of fraud, criminals hack into a cardholder's account, change login

details, and use the account for fraudulent activities.

Example of Credit Card Fraud (Phishing Fraud)

Person X, an online shopper, receives an email from what appears to be his bank, stating that

his credit card has been temporarily suspended due to suspicious activity. The email contains a link directing him to a website that looks exactly like his bank's official page. Without suspecting

anything, X enters his credit card number, CVV, and OTP to "reactivate" his card. Moments

later, he notices unauthorized transactions on his account from international websites. By the

time he contacts his bank; significant damage has already been done.

This is an example of phishing fraud, where fraudsters trick victims into voluntarily providing

their sensitive details.

**Identity Theft**

Identity theft is a fraud involving another person’s identity for an illicit purpose. This occurs when a criminal uses someone else’s identity for his own illegal purposes. Such stolen identity is typically use to make unauthorized purchases, open new account, apply for loans, or file fraudulent tax returns. Identity thieves use sophisticated methods to steal information from unsuspecting victims. They use social engineering and phishing schemes, malware attacks, skimming devices and even old-fashioned tactics like dumpster diving to get their hands on sensitive data.

**Types:** There are various amounts of threats but some common ones are:

* **Criminal identity theft:** The thief uses the victim’s ID to commit crimes, making the victim responsible for the acts.
* **Tax identity theft:** Thieves uses Employee ID or SSN to fraudulent claim tax refunds.
* **Medical identity theft:** Thieves use the victim’s health info to create fraudulently medical services and bills.

Following are some methods by which you can enhance your security for identity theft:

* Use strong password and never share PINs.
* Enable two-factor authentication for emails.
* Don’t share sensitive info on social media.
* Always verify authenticity when entering password.
* Never share AADHAR/PAN with untrusted individuals.
* Don’t fill out suspicious forms or provide OTPs to strangers.

**Cyber defamation And Identity Theft Connection**

To understand how identity theft and cyber defamation are connected, we need to know

what this term means:

**Identity Theft:** This is a cybercrime where someone steals another person’s personal

information (like their name, Social Security number, bank details, or passwords) without

their permission. The thief then uses this information to commit fraud, such as making

purchases, opening accounts, or even pretending to be the victim online.

**Cyber Defamation**: This is when someone uses the internet to harm another person’s

reputation by spreading false or damaging information about them. This can happen on

social media, blogs, forums, or other online platforms. The goal is to embarrass, humiliate, or

ruin the victim’s image.

**Connection of Identity Theft and Cyber Defamation:**

Using Stolen Identities for Defamation: A cybercriminal might steal someone’s identity

(like their social media account or email) and use it to post false or harmful information about

another person. For example, they could log into your Facebook account and post offensive

messages or lies about someone else, making it look like you did it. This not only harms the

victim of defamation but also damages your reputation because it appears as if you were the

one responsible.

**Defaming the Victim of Identity Theft:** In some cases, the thief might use the stolen

identity to defame the original owner. For instance, they could post inappropriate or illegal

content using your name, making it seem like you are the one doing it. This can ruin your

reputation and cause emotional distress.

**Creating Fake Identities for Defamation:** Cybercriminals sometimes create fake online

profiles using stolen personal information. They might use these fake accounts to spread lies

or harmful content about someone else. Since the account is fake, it’s harder to trace the

real culprit, and the victim of defamation suffers without knowing who is behind it.

Blackmail and Extortion: In some cases, identity thieves might use the stolen information

to blackmail the victim. For example, they could threaten to spread false information or

private details unless the victim pays them money. This combines identity theft with cyber

defamation, as the thief uses the threat of damaging the victim’s reputation to extort them.

**Cybercrime and the IT Act 2000**

The Information Technology Act, 2000 (IT Act, 2000) is a comprehensive legislation in India that addresses legal aspects related to electronic transactions, electronic records, cybercrimes, and digital signatures. It was enacted to foster the growth of electronic commerce (e-commerce) and to bring the Indian legal framework in line with the growing dependence on information technology and the Internet. The Act was passed by the Indian Parliament on October 17, 2000, and came into force on October 17, 2000, with subsequent amendments, the most significant being the Information Technology (Amendment) Act, 2008.

**Key Objectives of the IT Act, 2000:**

Facilitate e-commerce and e-governance: The Act provides a framework that recognizes electronic documents, digital signatures, and online transactions, which are essential for conducting electronic business and facilitating online governance.

Legal recognition of digital documents and electronic records: The Act allows electronic records and documents to be considered valid evidence in courts, thereby enabling the legal use of digital platforms for business and governmental purposes.

Combating cybercrimes and related offenses: It introduces legal provisions to punish and prevent a wide array of cybercrimes, including hacking, identity theft, cyberstalking, and online fraud.

Key Provisions of the Information Technology Act, 2000:

**1. Legal Recognition of Electronic Documents**

The IT Act gives legal recognition to electronic records (e.g., e-mails, contracts, etc.) in place of paper-based documents.

Section 4 of the Act states that "a legal recognition is given to electronic records," thereby making them admissible in a court of law. This is a vital provision for businesses and individuals who rely on digital communication and documentation.

**2. Digital Signatures and Electronic Authentication**

The Act provides the legal recognition of digital signatures and electronic signatures. Digital signatures are used to authenticate the origin and integrity of electronic records and transactions.

Section 3 of the Act emphasizes the use of digital signatures, which rely on public-key cryptography to ensure that a document is both authentic and tamper-proof.

The Act specifies the role of Certifying Authorities (Cas) that issue digital certificates to individuals or organizations for performing secure transactions online.

**3. Cybercrimes and Offenses**

The IT Act defines a range of cybercrimes and prescribes penalties for the same. Some of the key offenses include:

Hacking (Section 66): Unauthorized access to computer systems or networks with the intent to cause damage or steal data.

Identity Theft (Section 66C): Fraudulent use of someone’s identity, particularly in online transactions.

Cyberstalking (Section 66A): Using electronic communication to harass or threaten an individual.

Cyber Fraud (Section 66D): Committing fraud using computer resources.

Publishing or transmitting obscene material (Section 67): This section penalizes the publication or transmission of obscene content through the internet or other electronic means.

These provisions aim to safeguard individuals and organizations from growing threats in cyberspace, including unauthorized access, data breaches, cyber terrorism, and harassment.

**4. E-Governance**

The IT Act facilitates electronic governance (e-Governance) in India by recognizing the legal validity of electronic records. This ensures that government documents and transactions can be carried out electronically, improving efficiency and reducing paper-based processes.

It allows the use of electronic filing in courts and facilitates the electronic delivery of services by the government to citizens. Various government departments and agencies are empowered to conduct business electronically.

**5. Regulation of Certifying Authorities**

The IT Act provides a framework for the regulation of Certifying Authorities (CAs) who are authorized to issue digital certificates to individuals or organizations.

These digital certificates are used to authenticate the identity of the parties involved in an electronic transaction, ensuring a secure environment for online communication and business.

The Controller of Certifying Authorities (CCA), a regulatory body under the Act, oversees the functioning of Certifying Authorities in India.

**6. Cyber Appellate Tribunal (CAT)**

The IT Act established the Cyber Appellate Tribunal (CAT), which is tasked with hearing appeals related to cybercrimes and violations of the IT Act. The Tribunal is empowered to adjudicate issues related to cyber disputes and impose penalties or fines.

The Tribunal's decisions can be appealed to higher courts, including the High Courts.

**7. Data Protection**

The IT Act contains some provisions concerning the protection of data and privacy. However, these provisions were quite limited before the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which laid down guidelines for businesses to follow when handling sensitive personal data.

The Personal Data Protection Bill, 2019, introduced a comprehensive framework for data privacy, which is seen as an extension of the IT Act.

**Amendments to the IT Act:**

**Information Technology (Amendment) Act, 2008:**

The IT (Amendment) Act, 2008 brought significant changes to the original Act, including:

**Expanded Definitions of Cybercrimes:** The Amendment added new provisions related to cyber terrorism, child pornography, and identity theft, making the legal framework more comprehensive to address emerging challenges.

**Introduction of Cyber Terrorism:** The Amendment introduced provisions to punish acts of cyber terrorism (Section 66F), which involves the use of computers or networks to create fear or disruption in society.

**Stricter Penalties for Cybercrimes**: The Amendment introduced enhanced penalties for crimes such as hacking, identity theft, and cyberstalking.

**Regulation of Intermediaries:** The Amendment brought in provisions that outlined the responsibilities of intermediaries (such as ISPs, social media platforms, and websites) to take down harmful content when directed by law enforcement.

**Privacy and Data Protection**: The Amendment also addressed issues of privacy, especially with regard to sensitive personal data, and introduced guidelines for the protection of such data in the digital space.

**Implementation Challenges and Criticism:**

While the IT Act has brought positive reforms to India’s digital landscape, it has faced some criticism and challenges, such as:

**Outdated Provisions**: Some provisions in the Act are seen as outdated and unable to address modern-day technological advancements, such as cloud computing, AI, and the rise of social media platforms.

**Lack of Clarity on Privacy**: There are concerns regarding privacy laws under the IT Act, as it doesn’t provide comprehensive guidelines for data protection, unlike the GDPR in Europe.

Limited Awareness and Enforcement: The enforcement of cyber laws and consumer awareness about the IT Act remains a challenge in India, as many citizens and businesses are still unaware of their rights and obligations.

**A global perspective on cybercrimes**

Cyber Crime: -

Any unlawful Act being performed by an individual against Indian legal system using an electronic device and which is liable for punishment under IT Act of India is called Cyber Crime.

Global Impact: -

· Cyber crimes casts global economy billions annually, disrupting business and government.

· They harm national security by attacking important systems like power grids or defense.

· People’s personal information get stolen and leading to misuse like identity theft or cyber defamation.

Challenges: -

· Cyber Crimes happen across countries, making it hard to catch the criminals.

· Different countries have different laws which slows down the investigation.

· Criminals use advanced tools and techniques to hide their identity.

For Stopping Cyber Crimes: -

· Countries should work together with agreements like the Budapest Convention.

· Agencies like interpole helps nation fight cyber crimes together.

We have to use better technologies to prevent the cyber crimes