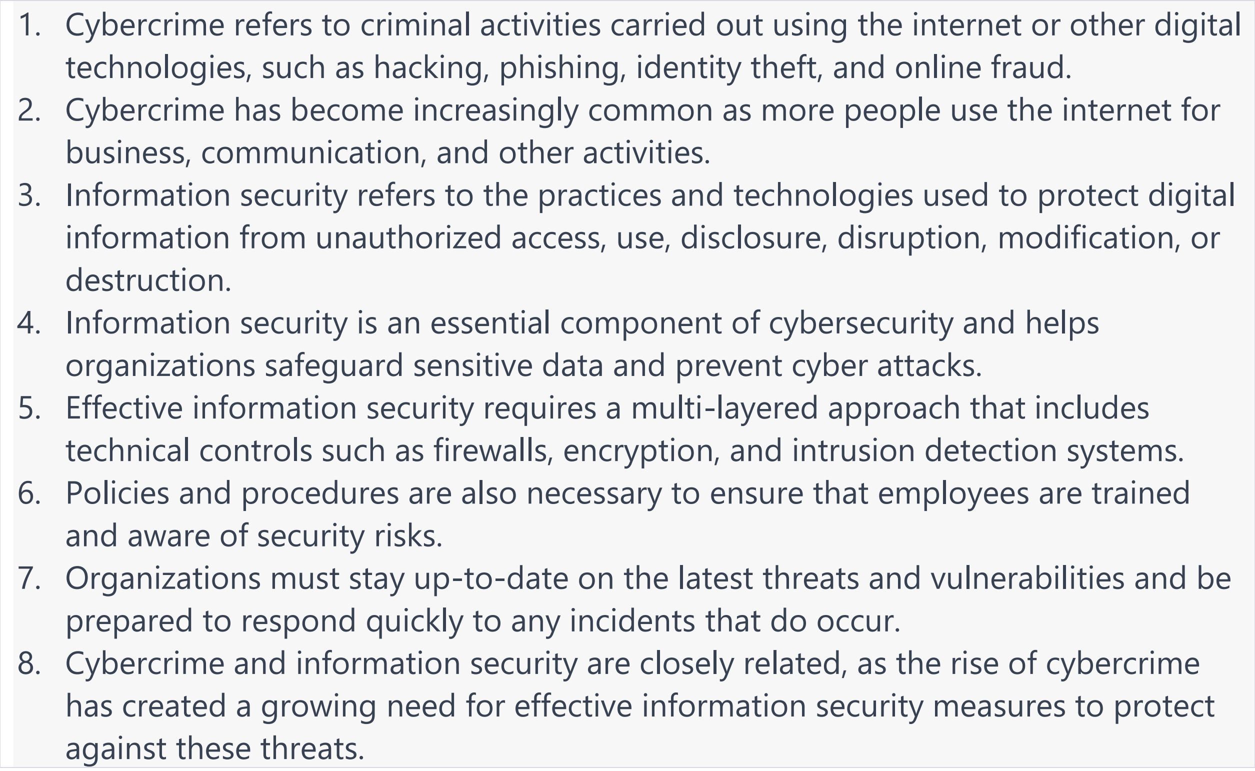
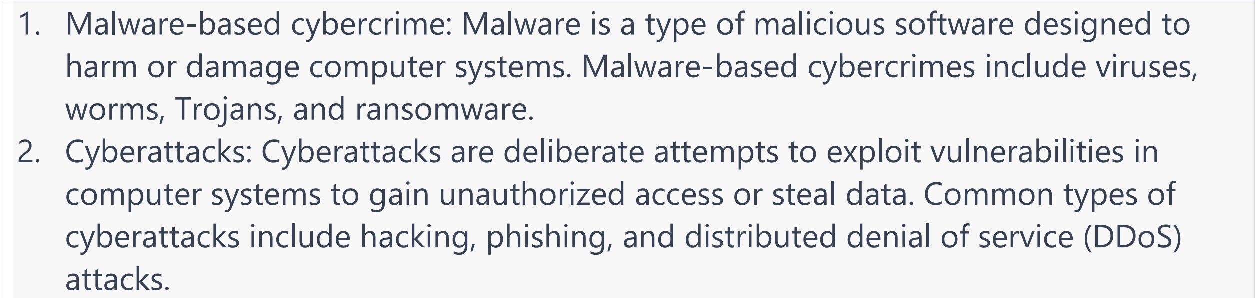
# UNIT-1: -

# # Explain Cybercrime and information security: -

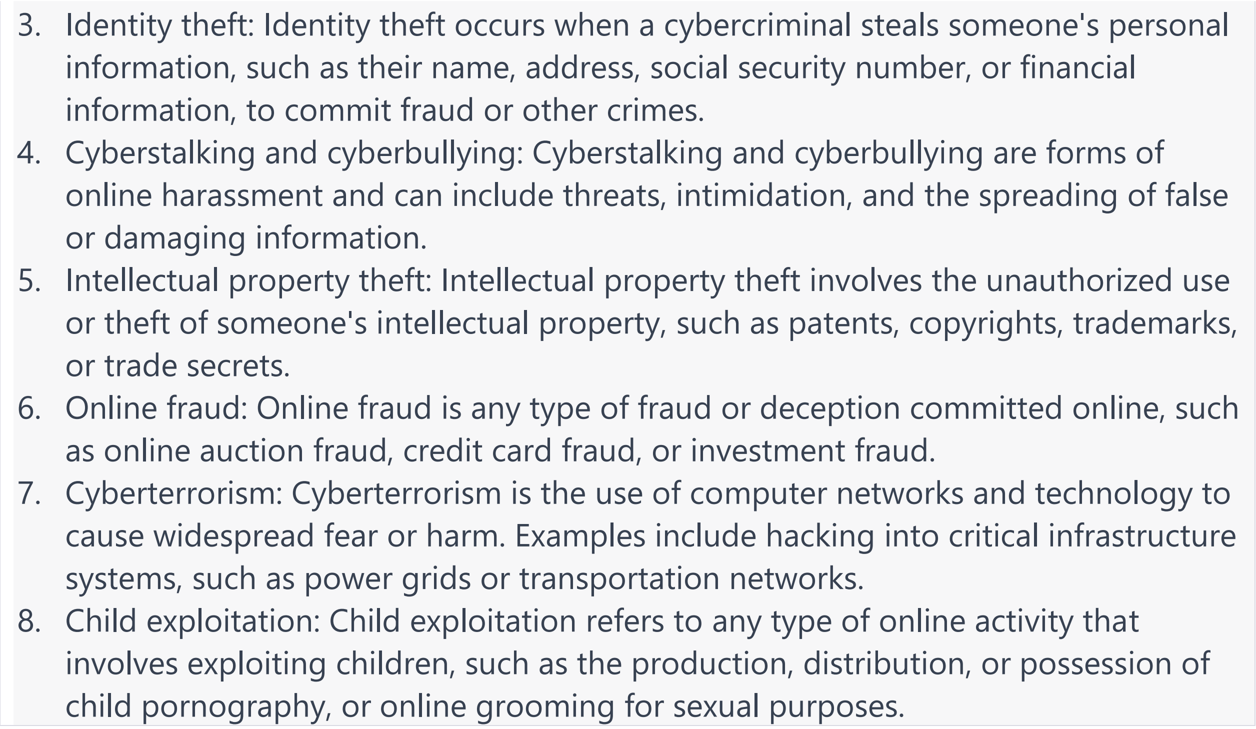


1. Cybercrime refers to criminal activities carried out using the internet or other digital technologies, such as hacking, phishing, identity theft, and online fraud.
2. Cybercrime has become increasingly common as more people use the internet for business, communication, and other activities.
3. Information security refers to the practices and technologies used to protect digital information from unauthorized access, use, disclosure, disruption, modification, or destruction.
4. Information security is an essential component of cybersecurity and helps organizations safeguard sensitive data and prevent cyber attacks.
5. Effective information security requires a multi-layered approach that includes technical controls such as firewalls, encryption, and intrusion detection systems.
6. Policies and procedures are also necessary to ensure that employees are trained and aware of security risks.
7. Organizations must stay up-to-date on the latest threats and vulnerabilities and be prepared to respond quickly to any incidents that do occur.
8. Cybercrime and information security are closely related, as the rise of cybercrime has created a growing need for effective information security measures to protect against these threats.

# # Explain Classes of cybercrime and categories: -

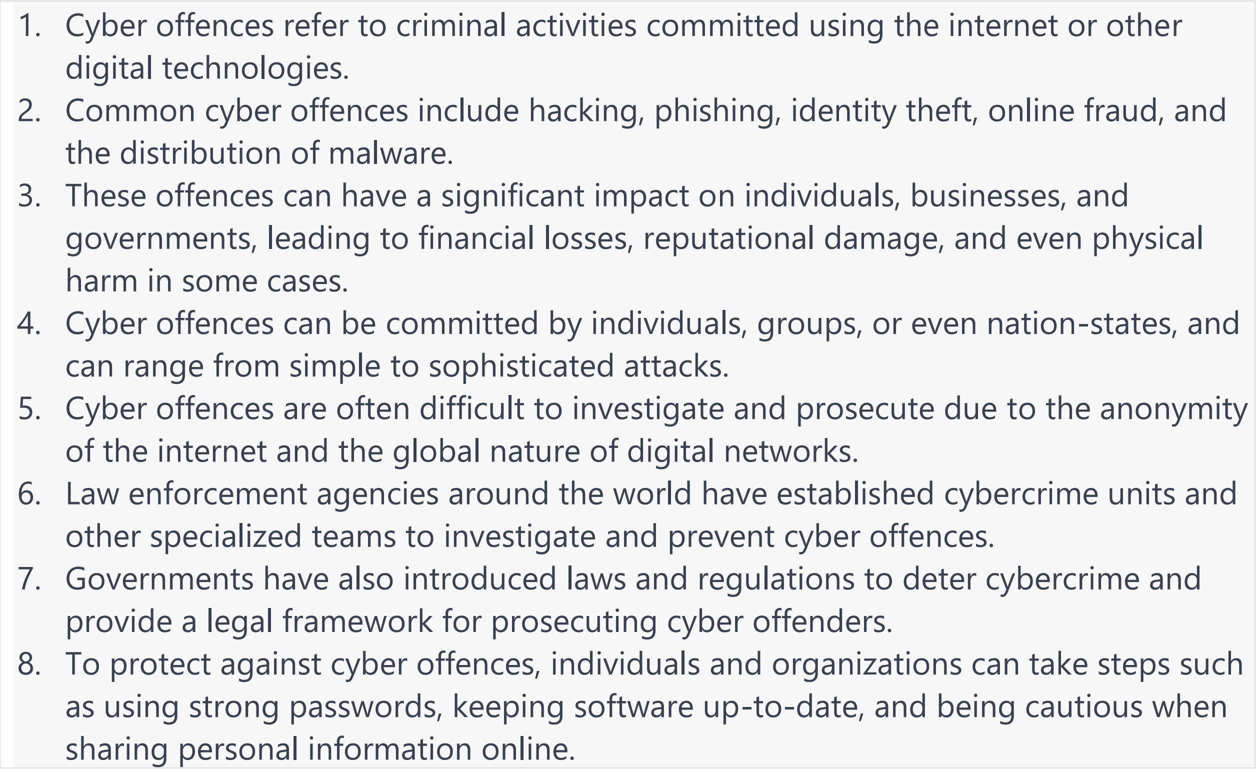


1. Malware-based cybercrime: Malware is a type of malicious software designed to harm or damage computer systems. Malware-based cybercrimes include viruses, worms, Trojans, and ransomware.
2. Cyberattacks: Cyberattacks are deliberate attempts to exploit vulnerabilities in computer systems to gain unauthorized access or steal data. Common types of cyberattacks include hacking, phishing, and distributed denial of service (DDoS) attacks.



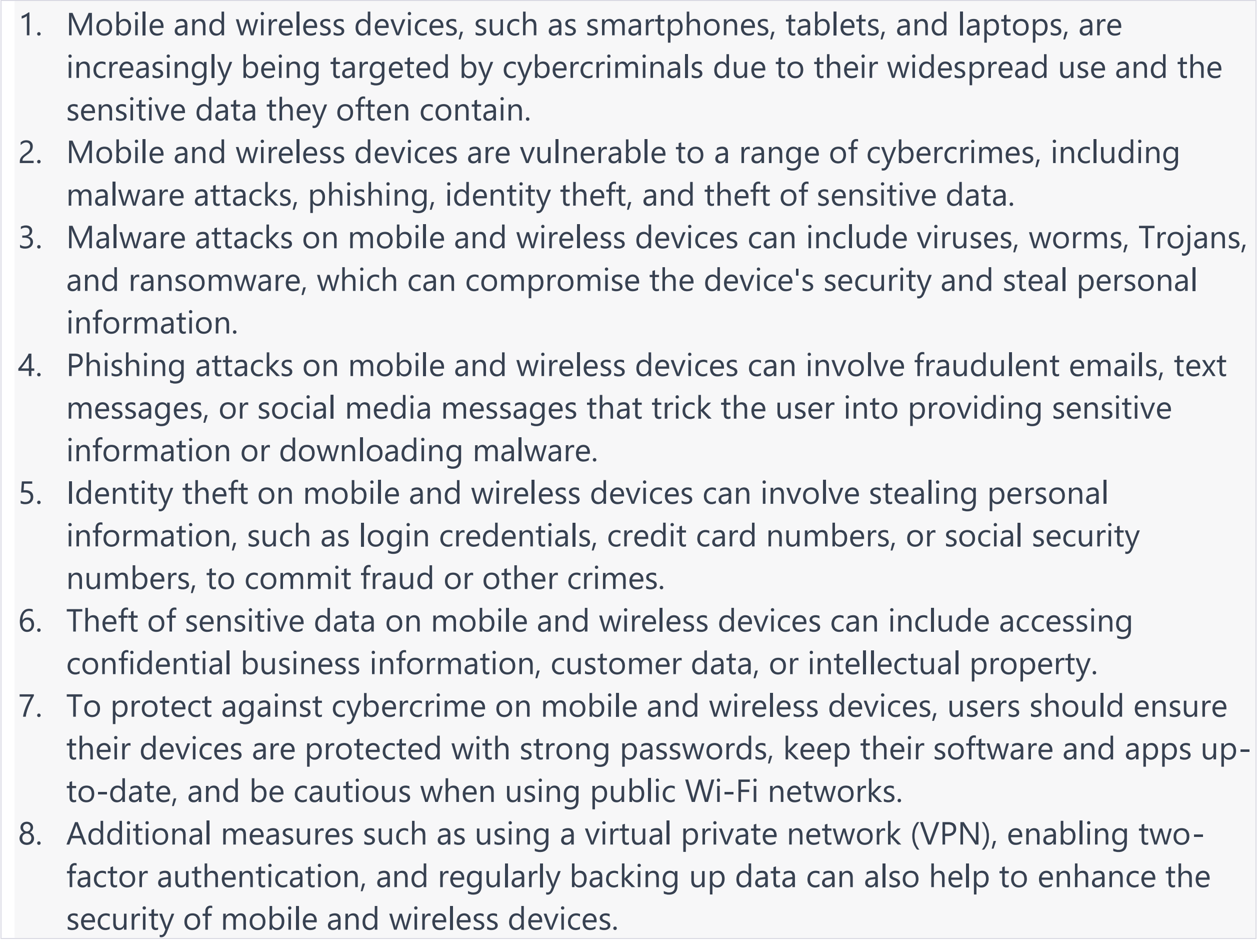
3. Identity theft: Identity theft occurs when a cybercriminal steals someone's personal information, such as their name, address, social security number, or financial information, to commit fraud or other crimes.
4. Cyberstalking and cyberbullying: Cyberstalking and cyberbullying are forms of online harassment and can include threats, intimidation, and the spreading of false or damaging information.
5. Intellectual property theft: Intellectual property theft involves the unauthorized use or theft of someone's intellectual property, such as patents, copyrights, trademarks, or trade secrets.
6. Online fraud: Online fraud is any type of fraud or deception committed online, such as online auction fraud, credit card fraud, or investment fraud.
7. Cyberterrorism: Cyberterrorism is the use of computer networks and technology to cause widespread fear or harm. Examples include hacking into critical infrastructure systems, such as power grids or transportation networks.
8. Child exploitation: Child exploitation refers to any type of online activity that involves exploiting children, such as the production, distribution, or possession of child pornography, or online grooming for sexual purposes.

# # Explain Cyber offences: -



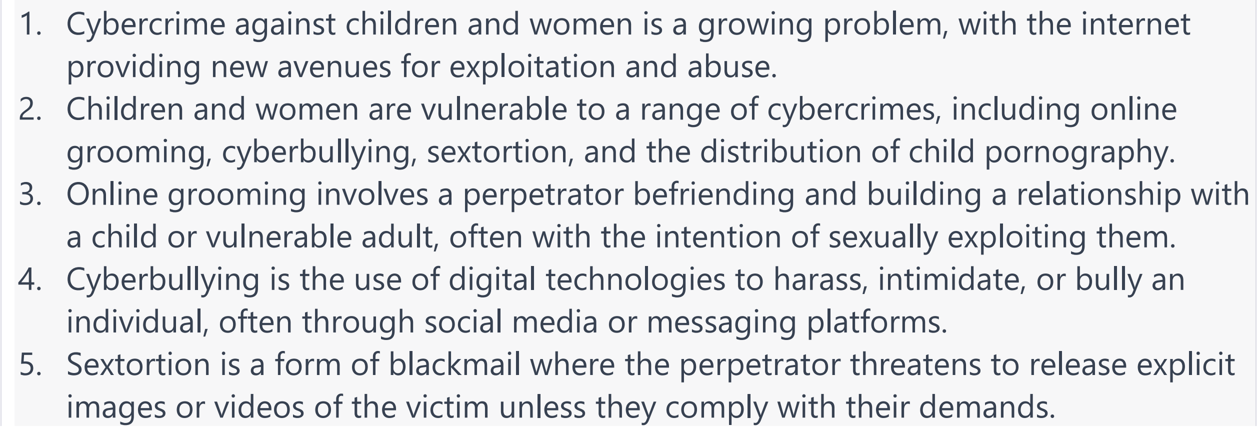
1. Cyber offences refer to criminal activities committed using the internet or other digital technologies.
2. Common cyber offences include hacking, phishing, identity theft, online fraud, and the distribution of malware.
3. These offences can have a significant impact on individuals, businesses, and governments, leading to financial losses, reputational damage, and even physical harm in some cases.
4. Cyber offences can be committed by individuals, groups, or even nation-states, and can range from simple to sophisticated attacks.
5. Cyber offences are often difficult to investigate and prosecute due to the anonymity of the internet and the global nature of digital networks.
6. Law enforcement agencies around the world have established cybercrime units and other specialized teams to investigate and prevent cyber offences.
7. Governments have also introduced laws and regulations to deter cybercrime and provide a legal framework for prosecuting cyber offenders.
8. To protect against cyber offences, individuals and organizations can take steps such as using strong passwords, keeping software up-to-date, and being cautious when sharing personal information online.

# # Cybercrimes with mobile and wireless devices: -

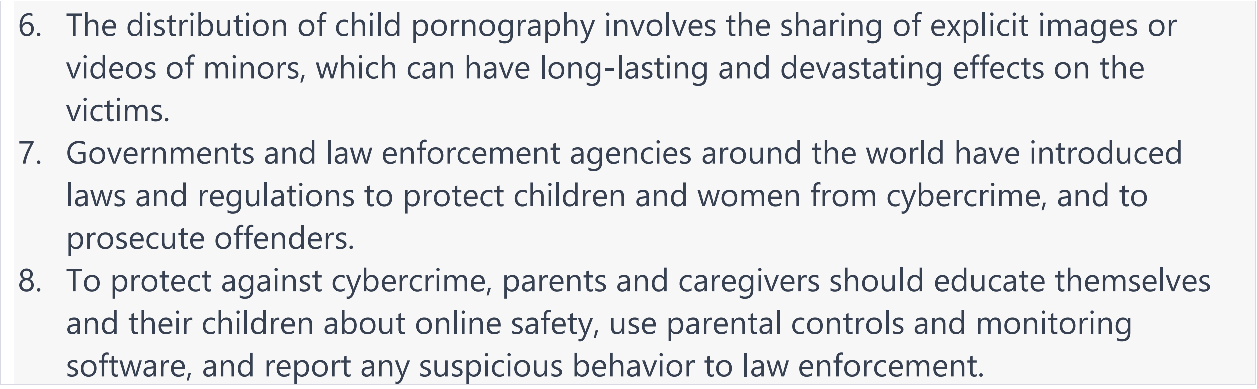


1. Mobile and wireless devices, such as smartphones, tablets, and laptops, are increasingly being targeted by cybercriminals due to their widespread use and the sensitive data they often contain.
2. Mobile and wireless devices are vulnerable to a range of cybercrimes, including malware attacks, phishing, identity theft, and theft of sensitive data.
3. Malware attacks on mobile and wireless devices can include viruses, worms, Trojans, and ransomware, which can compromise the device's security and steal personal information.
4. Phishing attacks on mobile and wireless devices can involve fraudulent emails, text messages, or social media messages that trick the user into providing sensitive information or downloading malware.
5. Identity theft on mobile and wireless devices can involve stealing personal information, such as login credentials, credit card numbers, or social security numbers, to commit fraud or other crimes.
6. Theft of sensitive data on mobile and wireless devices can include accessing confidential business information, customer data, or intellectual property.
7. To protect against cybercrime on mobile and wireless devices, users should ensure their devices are protected with strong passwords, keep their software and apps up-to-date, and be cautious when using public Wi-Fi networks.
8. Additional measures such as using a virtual private network (VPN), enabling two-factor authentication, and regularly backing up data can also help to enhance the security of mobile and wireless devices.

# # Cybercrime against women and children: -

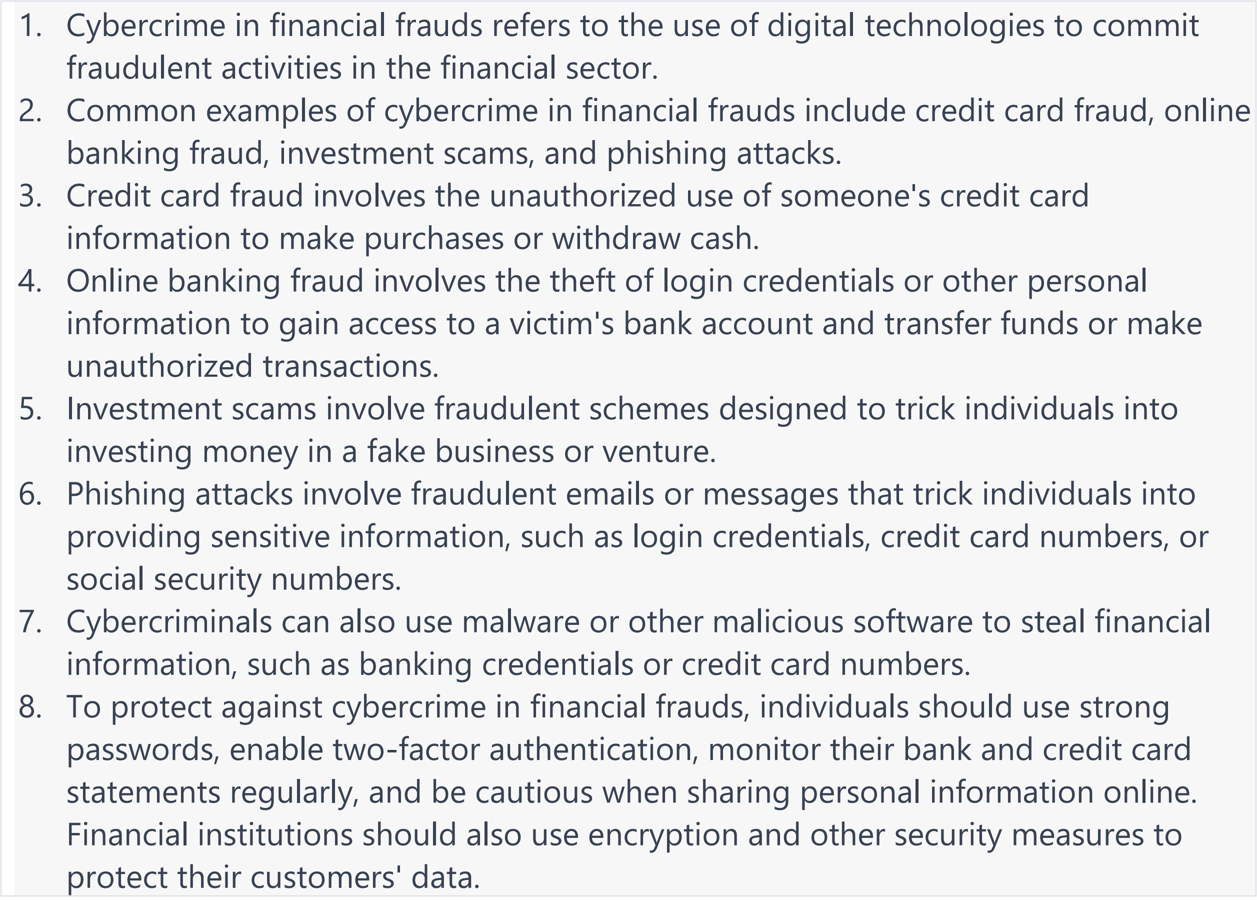


1. Cybercrime against children and women is a growing problem, with the internet providing new avenues for exploitation and abuse.
2. Children and women are vulnerable to a range of cybercrimes, including online grooming, cyberbullying, sextortion, and the distribution of child pornography.
3. Online grooming involves a perpetrator befriending and building a relationship with a child or vulnerable adult, often with the intention of sexually exploiting them.
4. Cyberbullying is the use of digital technologies to harass, intimidate, or bully an individual, often through social media or messaging platforms.
5. Sextortion is a form of blackmail where the perpetrator threatens to release explicit images or videos of the victim unless they comply with their demands.



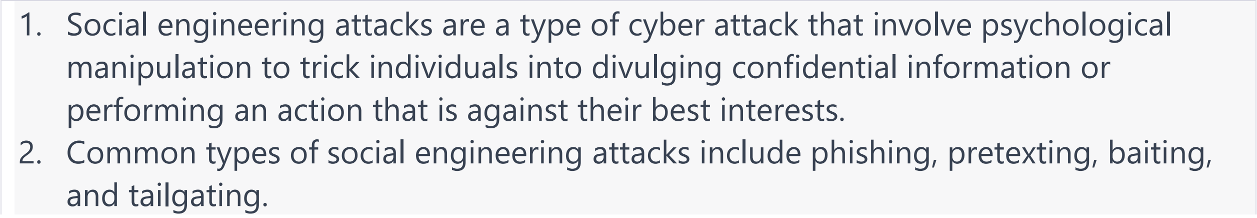
6. The distribution of child pornography involves the sharing of explicit images or videos of minors, which can have long-lasting and devastating effects on the victims.
7. Governments and law enforcement agencies around the world have introduced laws and regulations to protect children and women from cybercrime, and to prosecute offenders.
8. To protect against cybercrime, parents and caregivers should educate themselves and their children about online safety, use parental controls and monitoring software, and report any suspicious behavior to law enforcement.

# # Cybercrime in financial frauds: -



1. Cybercrime in financial frauds refers to the use of digital technologies to commit fraudulent activities in the financial sector.
2. Common examples of cybercrime in financial frauds include credit card fraud, online banking fraud, investment scams, and phishing attacks.
3. Credit card fraud involves the unauthorized use of someone's credit card information to make purchases or withdraw cash.
4. Online banking fraud involves the theft of login credentials or other personal information to gain access to a victim's bank account and transfer funds or make unauthorized transactions.
5. Investment scams involve fraudulent schemes designed to trick individuals into investing money in a fake business or venture.
6. Phishing attacks involve fraudulent emails or messages that trick individuals into providing sensitive information, such as login credentials, credit card numbers, or social security numbers.
7. Cybercriminals can also use malware or other malicious software to steal financial information, such as banking credentials or credit card numbers.
8. To protect against cybercrime in financial frauds, individuals should use strong passwords, enable two-factor authentication, monitor their bank and credit card statements regularly, and be cautious when sharing personal information online. Financial institutions should also use encryption and other security measures to protect their customers' data.

# # Cybercrime in social engineering attacks: -

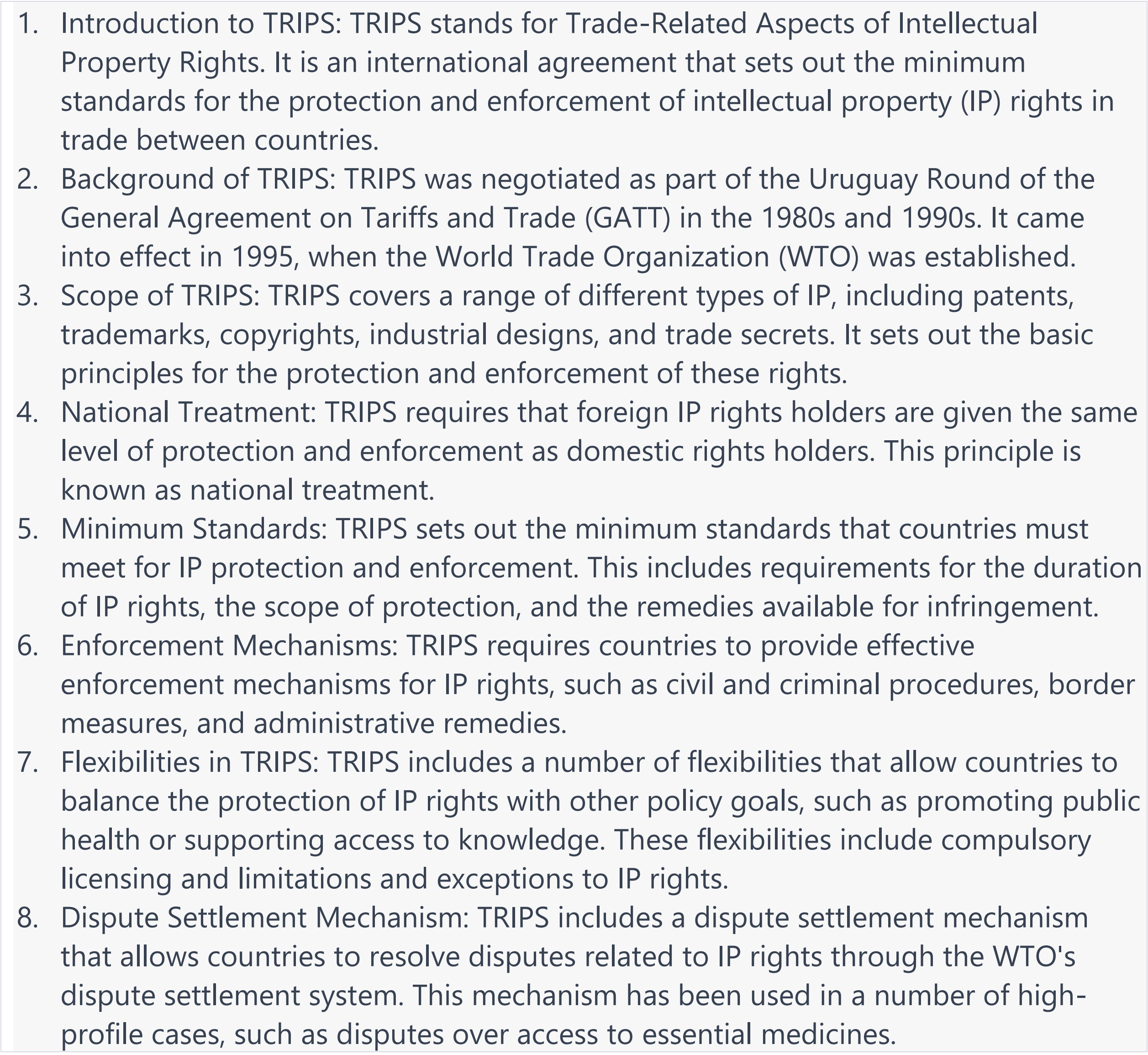


1. Social engineering attacks are a type of cyber attack that involve psychological manipulation to trick individuals into divulging confidential information or performing an action that is against their best interests.
2. Common types of social engineering attacks include phishing, pretexting, baiting, and tailgating.

3. Phishing attacks involve fraudulent emails, messages, or websites that appear to be legitimate but are designed to trick individuals into providing personal information, such as passwords, credit card numbers, or social security numbers.
4. Pretexting involves creating a false scenario to gain access to sensitive information, such as pretending to be an IT helpdesk representative to obtain login credentials.
5. Baiting involves enticing an individual with a tempting offer, such as a free gift, to click on a malicious link or download malware.
6. Tailgating involves following an individual into a restricted area without authorization, often by pretending to be an employee or delivery person.
7. Social engineering attacks can have serious consequences, including financial loss, identity theft, and reputational damage.
8. To protect against social engineering attacks, individuals should be aware of the common tactics used by cybercriminals, use strong passwords, keep software and systems up-to-date, and be cautious when sharing personal information. Organizations should also implement policies and training programs to raise awareness about social engineering attacks and reduce the risk of a successful attack.

# UNIT-4: -

## #TRIPS: -



1. Introduction to TRIPS: TRIPS stands for Trade-Related Aspects of Intellectual Property Rights. It is an international agreement that sets out the minimum standards for the protection and enforcement of intellectual property (IP) rights in trade between countries.
2. Background of TRIPS: TRIPS was negotiated as part of the Uruguay Round of the General Agreement on Tariffs and Trade (GATT) in the 1980s and 1990s. It came into effect in 1995, when the World Trade Organization (WTO) was established.
3. Scope of TRIPS: TRIPS covers a range of different types of IP, including patents, trademarks, copyrights, industrial designs, and trade secrets. It sets out the basic principles for the protection and enforcement of these rights.
4. National Treatment: TRIPS requires that foreign IP rights holders are given the same level of protection and enforcement as domestic rights holders. This principle is known as national treatment.
5. Minimum Standards: TRIPS sets out the minimum standards that countries must meet for IP protection and enforcement. This includes requirements for the duration of IP rights, the scope of protection, and the remedies available for infringement.
6. Enforcement Mechanisms: TRIPS requires countries to provide effective enforcement mechanisms for IP rights, such as civil and criminal procedures, border measures, and administrative remedies.
7. Flexibilities in TRIPS: TRIPS includes a number of flexibilities that allow countries to balance the protection of IP rights with other policy goals, such as promoting public health or supporting access to knowledge. These flexibilities include compulsory licensing and limitations and exceptions to IP rights.
8. Dispute Settlement Mechanism: TRIPS includes a dispute settlement mechanism that allows countries to resolve disputes related to IP rights through the WTO's dispute settlement system. This mechanism has been used in a number of high-profile cases, such as disputes over access to essential medicines.

# WTO: -

1. Introduction to the WTO: The World Trade Organization (WTO) is an international organization that promotes free trade and economic cooperation among its member countries. It was established on January 1, 1995, and is based in Geneva, Switzerland.
2. History of the WTO: The WTO was established as a result of the Uruguay Round of trade negotiations that began in 1986 under the General Agreement on Tariffs and Trade (GATT). The WTO replaced the GATT as the primary international organization for trade negotiations and dispute resolution.
3. Membership of the WTO: The WTO has 164 member countries, which account for more than 98% of world trade. Countries must apply for membership and meet certain criteria, including a commitment to trade liberalization and the adoption of WTO rules and agreements.
4. WTO Agreements: The WTO has a number of agreements that govern international trade in goods, services, and intellectual property. These agreements include the General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS), and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).
5. Principles of the WTO: The WTO is based on a number of principles, including non-discrimination, transparency, predictability, and fair competition. These principles help to promote free and open trade among member countries.
6. Functions of the WTO: The WTO has a number of functions, including negotiating new trade agreements, monitoring and enforcing existing agreements, providing technical assistance and training to member countries, and settling disputes related to international trade.
7. Decision-Making in the WTO: The WTO is run by its member countries, who make decisions through various committees and councils. The General Council, which meets regularly in Geneva, is the highest decision-making body of the WTO.
8. Criticisms of the WTO: The WTO has faced criticism from some quarters for being undemocratic, favoring the interests of developed countries over developing countries, and promoting a one-size-fits-all approach to trade liberalization. However, supporters of the WTO argue that it has been instrumental in promoting economic growth and reducing poverty around the world.

# Laws relating to IPR: -

1. Introduction to IPR: Intellectual property rights refer to the legal protections afforded to creators of original works, such as inventions, literary and artistic works, and symbols and designs. IPR laws aim to balance the interests of creators with those of society at large.

2. Types of IPR: There are several types of IPR, including patents, trademarks, copyrights, trade secrets, and industrial designs. Each type of IPR is protected under specific laws and regulations.
3. Patents: Patents provide inventors with exclusive rights to their inventions for a set period of time. In order to be granted a patent, an invention must be new, non-obvious, and useful.
4. Trademarks: Trademarks are distinctive signs, such as logos, symbols, and names, that are used to identify and distinguish the goods or services of one party from those of others. Trademark laws protect against the unauthorized use of such signs by competitors.
5. Copyrights: Copyrights protect original works of authorship, such as books, music, and software. Copyright owners have exclusive rights to their works, including the right to reproduce, distribute, and display them.
6. Trade Secrets: Trade secrets refer to confidential business information that provides a competitive advantage. Trade secret laws protect against the unauthorized use or disclosure of such information.
7. Industrial Designs: Industrial designs refer to the aesthetic aspects of a product, such as its shape, pattern, or color. Industrial design laws protect against the unauthorized copying or imitation of such designs.
8. Enforcement of IPR: IPR laws are enforced through civil and criminal remedies, such as injunctions, damages, and fines. In addition, border measures, such as customs seizures, can be used to prevent the importation of infringing goods.

# **#IPR Tool Kit: -**

The IPR Tool Kit is a collection of resources designed to help individuals and organizations better understand and manage intellectual property rights (IPR). It is a set of practical tools and guidelines that provide information on the different types of IPR and how to protect them.

The IPR Tool Kit typically includes the following resources:

1. Overview of IPR: This provides an introduction to the various types of IPR, including patents, trademarks, copyrights, trade secrets, and industrial designs.
2. IPR Policy and Strategy: This outlines how to develop an IPR policy and strategy that aligns with the organization's overall business goals and objectives.
3. Patent Search and Analysis: This covers how to conduct a patent search and analysis to determine whether an invention is patentable, and to assess the potential value of a patent.
4. Trademark Search and Analysis: This provides guidance on how to conduct a trademark search and analysis to determine whether a proposed trademark is available for use, and to assess the potential risks of using a particular mark.
5. Copyright and Licensing: This covers how to manage copyright ownership and licensing issues, including how to negotiate and draft license agreements.

6. IP Enforcement: This provides guidance on how to enforce IP rights, including how to identify and respond to instances of infringement, and how to initiate legal proceedings if necessary.
7. IP Valuation: This covers how to value intellectual property assets for various purposes, such as mergers and acquisitions, licensing, and financing.
8. IP Management: This provides guidance on how to manage intellectual property assets effectively, including how to develop an IP management plan and how to monitor and maintain IP rights.

Overall, the IPR Tool Kit is a valuable resource for individuals and organizations that want to better understand and manage their intellectual property rights. It provides practical guidance and tools that can help to maximize the value of intellectual property assets, while also minimizing the risks of infringement and other legal issues.

# **#Copyright and Neighbouring Rights: -**

Copyright and neighboring rights are two types of intellectual property rights that protect different aspects of creative works.

Copyright is a legal right that gives the creator of an original work, such as a book, film, or song, exclusive rights to use, reproduce, distribute, and display the work. Copyright protection is automatic and does not require registration, although registration may be required to enforce the rights in court. The duration of copyright protection varies depending on the type of work and the country in which it is protected, but typically lasts for the life of the creator plus a certain number of years after their death.

Neighboring rights, also known as related rights or neighboring rights in performances, are a type of intellectual property right that protect the rights of performers, producers of sound recordings, and broadcasters. Neighboring rights give these parties exclusive rights to control the use of their performances, sound recordings, or broadcasts. For example, a musician may have neighboring rights in a sound recording of their music, giving them the right to control how the recording is used and distributed. The duration of neighboring rights protection also varies depending on the type of work and the country in which it is protected.

Both copyright and neighboring rights are important for protecting the rights of creators and promoting innovation and creativity. By providing exclusive rights to control the use of their works, creators are incentivized to invest time and resources into creating new and original works. These rights also provide a way for creators to monetize their works and earn income from their creations.

However, copyright and neighboring rights can also be the subject of legal disputes and controversies, particularly in cases where there are questions around fair use or fair dealing, which allow for limited use of copyrighted works for certain purposes, such as criticism, commentary, news reporting, teaching, scholarship, or research. As such, it is important for creators and users of copyrighted and neighboring rights-protected works to understand the relevant laws and regulations in their jurisdiction to avoid potential legal issues.

## #Agencies of IPR Registration: -

Agencies of IPR registration are organizations that facilitate the registration and management of intellectual property rights (IPR). These agencies provide services related to the registration and protection of various types of IPR, such as patents, trademarks, copyrights, and industrial designs.

Here are some of the key agencies involved in IPR registration:

1. United States Patent and Trademark Office (USPTO): This agency is responsible for registering and administering patents and trademarks in the United States.
2. European Union Intellectual Property Office (EUIPO): This agency is responsible for registering and administering trademarks and designs in the European Union.
3. World Intellectual Property Organization (WIPO): This agency is a specialized agency of the United Nations that is responsible for promoting the protection of intellectual property rights worldwide. WIPO provides a wide range of services related to IPR, including patent and trademark registration, and dispute resolution.
4. Japanese Patent Office (JPO): This agency is responsible for registering and administering patents and trademarks in Japan.
5. Korean Intellectual Property Office (KIPO): This agency is responsible for registering and administering patents, trademarks, and designs in South Korea.
6. Intellectual Property Office of Singapore (IPOS): This agency is responsible for registering and administering patents, trademarks, and designs in Singapore.
7. Canadian Intellectual Property Office (CIPO): This agency is responsible for registering and administering patents, trademarks, and copyrights in Canada.

## Emerging Areas of IPR: -

Emerging areas of IPR refer to new or developing fields of intellectual property that are becoming increasingly important in today's economy. Here are some of the key emerging areas of IPR:

1. Artificial Intelligence (AI): With the increasing use of AI in various fields, there is a growing need to protect the intellectual property associated with AI, including the algorithms and models used to develop AI systems.
2. Blockchain Technology: Blockchain technology is being used in a variety of applications, from cryptocurrencies to supply chain management, and there is a

need to develop new intellectual property protection strategies for this emerging technology.

3. Internet of Things (IoT): The IoT refers to the growing network of interconnected devices and sensors that are being used in a wide range of applications. There is a need to protect the intellectual property associated with IoT devices and systems, including the software, hardware, and data generated by these devices.
4. 3D Printing: 3D printing is a rapidly growing field that is being used to create a wide range of products, from medical implants to aerospace components. There is a need to develop new intellectual property protection strategies for the designs and digital files used to create 3D printed objects.
5. Biotechnology: Biotechnology is an important field that is producing new treatments and therapies for a wide range of diseases. There is a need to protect the intellectual property associated with biotech research, including patents for new drugs and medical devices.
6. Green Technology: With the growing focus on sustainability and reducing carbon emissions, there is a need to protect the intellectual property associated with green technology, including patents for new renewable energy technologies and energy-efficient products.
7. Data Analytics: With the increasing importance of data in today's economy, there is a need to protect the intellectual property associated with data analytics, including the algorithms and models used to analyze and interpret data.

# **Use and Misuse of IPR: -**

Intellectual property rights (IPR) can be a powerful tool for fostering innovation, creativity, and economic growth. However, like any tool, IPR can also be misused, leading to negative consequences for society as a whole. Here are some examples of the use and misuse of IPR:

Use of IPR:

1. Encouraging innovation: IPR can encourage businesses and individuals to invest in new technologies, products, and services by providing legal protections for their intellectual property.
2. Promoting economic growth: IPR can stimulate economic growth by promoting innovation and encouraging investment in new technologies, which can create jobs and increase productivity.
3. Protecting consumers: IPR can protect consumers by ensuring that products are safe and of high quality, and by preventing counterfeit and pirated goods from entering the market.
4. Fostering creativity: IPR can encourage artists and creators to develop new works by providing legal protections for their intellectual property.

Misuse of IPR:

1. Monopolies: IPR can be misused to create monopolies that stifle competition and prevent others from entering the market. This can lead to higher prices for consumers and reduced innovation.
2. Abusive litigation: IPR can be used to engage in abusive litigation, where companies file frivolous lawsuits against their competitors to gain a competitive advantage.
3. Hindering access to essential medicines: IPR can be misused to prevent access to essential medicines in developing countries, where the high cost of drugs can be a barrier to treatment.
4. Inhibiting creativity: IPR can be used to stifle creativity by preventing artists and creators from using existing works to create new works or by restricting access to works that are in the public domain.

# UNIT 2: -

# # Malware and ransomware attacks: -

**Malware:** Malware, short for malicious software, refers to software or programs designed with malicious intent to harm, disrupt, or gain unauthorized access to computer systems, networks, or devices.

**Types of Malware:** Malware can take various forms, including viruses, worms, trojans, adware, spyware, and ransomware. Each type has its specific characteristics and functions.

**Delivery Methods:** Malware can be delivered through infected websites, email attachments, malicious links, compromised software downloads, or even through physical devices like USB drives. Phishing emails are a common method, tricking users into downloading or executing the malware.

**Ransomware:** Ransomware is a specific type of malware that encrypts the victim's files or locks their entire system, making the data inaccessible. Attackers demand a ransom payment in exchange for restoring access to the files or system.

**Encryption and Locking:** Ransomware encrypts the victim's files using strong encryption algorithms, rendering them inaccessible without the decryption key. Some variants also lock the victim's entire system, preventing access to any files or applications.

**Ransom Note and Payment**: After encrypting files or locking the system, attackers display a ransom note, informing the victim about the attack and providing instructions for making the ransom payment. Payment is usually demanded in cryptocurrencies for anonymity.

**Impact and Consequences:** Ransomware attacks can have severe consequences, including data loss, financial losses, disruption of business operations, reputational damage, and potential legal implications. Victims face the difficult decision of whether to pay the ransom or attempt data recovery independently.

**Prevention and Mitigation:** Protecting against malware and ransomware attacks involves implementing robust cybersecurity measures such as regularly updating software and operating systems, using strong and unique passwords, employing email and web filtering tools, educating users about phishing and safe browsing practices, and maintaining regular backups of critical data.

# # Legal Perspectives of Cybercrimes -

Legal perspectives of cybercrime encompass the laws and regulations established to address and combat criminal activities conducted in the digital realm. These legal frameworks are designed to define cybercrimes, establish penalties for offenders, and provide mechanisms for investigation, prosecution, and prevention. Here are key aspects of the legal perspectives of cybercrime:

**Legislation and Laws:** Governments around the world have enacted legislation specifically targeting cybercrimes. These laws vary across jurisdictions but commonly cover offenses such as hacking, identity theft, data breaches, phishing, cyberstalking, online fraud, and distribution of malicious software. Examples include the Computer Fraud and Abuse Act (CFAA) in the United States and the Computer Misuse Act in the United Kingdom.

**International Cooperation:** Given the borderless nature of cybercrimes, international cooperation is crucial for effective law enforcement. Countries work together through mutual legal assistance treaties, sharing information, evidence, and expertise to investigate and prosecute cybercriminals operating across national boundaries. Examples include the Budapest Convention on Cybercrime and INTERPOL's efforts in coordinating global cybercrime response.

**Jurisdictional Challenges**: Cybercrimes often present challenges regarding jurisdiction. Determining which laws apply and which law enforcement agency has authority can be complex, especially when crimes are committed remotely or involve actors from multiple jurisdictions. Legal frameworks are continuously evolving to address these challenges and establish principles of extraterritorial jurisdiction and cross-border cooperation.

**Digital Evidence and Forensics**: Cybercrime investigations heavily rely on digital evidence gathered from computer systems, networks, and online communications. Laws establish protocols and standards for the collection, preservation, and admissibility of digital evidence in court. Digital forensics plays a vital role in uncovering the identity of perpetrators, their methods, and the extent of damage caused.

# # IT Act 2000 and its amendments: -

**IT Act 2000:**

Legal Recognition of Electronic Transactions: Recognizes electronic records and digital signatures as legally valid and enforceable.

Security and Authentication: Establishes guidelines for digital signatures and electronic authentication methods to ensure secure electronic communications.

Offenses and Penalties: Defines various cybercrimes, including unauthorized access, hacking, identity theft, data theft, and cyber fraud, with corresponding penalties.

**Amendment Act 2008:**

Strengthening Cybersecurity: Addresses cybersecurity concerns, including unauthorized access, interception, and damage to computer systems. Establishes the National Critical Information Infrastructure Protection Center (NCIIPC).

Data Protection and Privacy: Introduces provisions for handling sensitive personal data and establishes guidelines for data collection, storage, and disclosure.

Enhanced Penalties: Increases penalties for offenses such as unauthorized access, hacking, and cyber terrorism.

**Amendment Act 2009:**

Cyber Terrorism: Introduces the offense of cyber terrorism, defined as any act with the intent to threaten India's unity, integrity, security, or sovereignty. Imposes stringent punishments for cyber terrorism.

**Amendment Act 2011:**

Intermediary Liability: Clarifies the liability of intermediaries, such as internet service providers, for content hosted or transmitted by them. Provides a safe harbor provision to protect intermediaries from liability for third-party content.

**Amendment Act 2013:**

Offensive Content: Adds provisions for the regulation of offensive and harmful content, including provisions for blocking websites and removing objectionable material.

Electronic Governance: Introduces provisions for electronic governance, including electronic filing of documents, authentication of electronic records, and establishment of cyber appellate tribunals.

**Amendment Act 2017:**

Digital Signatures: Expands the scope of digital signatures to include new technologies and mechanisms for secure electronic authentication.

Data Protection: Introduces provisions for the protection and processing of personal data, including the establishment of a Data Protection Authority and data breach reporting requirements.

# # Organizations dealing with cybercrime and cybersecurity in India: -

Organizations dealing with cybercrime and cybersecurity in India play a crucial role in addressing cyber threats, investigating cybercrimes, and implementing measures to enhance cybersecurity. Here are some key organizations in India working in this domain:

**Computer Emergency Response Team-India (CERT-In):**

- CERT-In is the national agency responsible for responding to and handling cybersecurity incidents in India.
- It operates under the Ministry of Electronics and Information Technology (MeitY) and serves as the nodal agency for coordination and collaboration among various sectors to strengthen cybersecurity.
- CERT-In provides incident response, threat intelligence, vulnerability assessment, and risk mitigation services to government departments, critical infrastructure, and other stakeholders.

**National Cyber Security Coordinator (NCSC):**

- NCSC is responsible for formulating and implementing policies and strategies to safeguard India's cyberspace.
- It operates under the Prime Minister's Office and works closely with other government agencies, law enforcement, and private sector entities to enhance cybersecurity preparedness.
- NCSC plays a key role in coordinating national-level cybersecurity initiatives and fostering collaboration among stakeholders.

**National Critical Information Infrastructure Protection Centre (NCIIPC):**

- NCIIPC focuses on protecting critical information infrastructure, which includes sectors such as power, finance, transportation, and defense.
- It is responsible for identifying critical information infrastructure, assessing risks, and implementing security measures to prevent cyber threats and attacks against these vital sectors.
- NCIIPC collaborates with sector-specific Computer Emergency Response Teams (CERTs) and other relevant organizations to ensure the security of critical infrastructure.

**Cyber Crime Investigation Cells**:

- Various state police departments in India have established specialized cybercrime investigation cells or units to handle and investigate cybercrimes.
- These units consist of trained personnel who specialize in cybercrime investigation techniques, digital forensics, and legal procedures related to cybercrime cases.
- They collaborate with other law enforcement agencies, CERT-In, and international organizations to combat cybercrimes and prosecute offenders.

# UNIT 3: -

**Introduction to social networks, Types of social media, social media** platforms just go through these once as everybody knows what is it.

# Social Media Monitoring: -

## Definition:-

- Social media monitoring is the process of identifying and determining what is being said about a planned individual or product through different social and online channels.
- Social media monitoring means tracking keywords and mentions related to your brand.

## APPLICATIONS OF SOCIAL MEDIA MONITORING IN DIFFERENT SOCIAL MEDIA PLATFORMS:-

- Brand Watch:- Spread and analyze data from many sources including blogs, forums, and reveal sites as well as social networks. Used by social media marketers who focus on brand monitoring. It is a paid tool.
- Google Analytics:- Track the traffics and leads to a website from social media channels. It is a free tool.
- Channel view insights:- Analyse the YouTube performance of multiple channels. It is a paid tool.
- Talk Walker:- Monitor conversation from more than 150 million sources to analyze comments, sentiments, and emotions. It is a paid tool.
- Mentionalities:- Track mentions, keywords, and sentiments across multiple languages on social channels and elsewhere on the web.

## NEED FOR SOCIAL MEDIA MONITORING:-

- To know the best time to share.
- To know what people say about the business.
- To better understand competitors.
- To create the best content(tutorial or video).

# **Hashtags: -**

Hashtags are widely used in social media platforms to categorize and organize content. In the context of social media cyber, here are four key points about hashtags:

- Content Categorization: Hashtags serve as a way to categorize content and make it discoverable within social media platforms. By adding a relevant hashtag to a post, users can ensure their content appears in searches related to that topic. This allows users to find and engage with specific content related to social media cyber.

- Trend Identification: Hashtags often represent ongoing trends or discussions within social media. Monitoring popular hashtags related to social media cyber can help users stay updated on the latest news, events, and conversations surrounding cybersecurity, privacy, online safety, and digital threats. It provides a quick way to identify and participate in relevant discussions.

- Community Building: Hashtags can help build communities of like-minded individuals interested in social media cyber. Users can follow specific hashtags to connect with others who share similar interests, exchange knowledge, and engage in conversations related to cybersecurity, best practices, or experiences. Hashtags facilitate the formation of communities and enable users to engage with others who have similar concerns or experiences in the digital realm.

- Campaigns and Awareness: Hashtags play a crucial role in social media campaigns and raising awareness about cyber-related issues. Organizations, advocacy groups, or individuals often create dedicated hashtags to promote specific campaigns, share educational content, or advocate for online safety practices. By utilizing hashtags, they can amplify their message, reach a broader audience, and encourage participation and engagement in spreading awareness about social media cyber threats and promoting responsible digital behavior.

# Social Media Privacy: -

Social media privacy is a critical aspect of online safety and involves protecting personal information, controlling access to one's data, and maintaining privacy boundaries on social media platforms. Here are four key points about social media privacy:

**Privacy Settings and Controls:**

- Social media platforms offer privacy settings and controls that allow users to customize the visibility of their posts, personal information, and interactions.
- Users should review and adjust their privacy settings to determine who can view their profile, posts, and personal details.
- Privacy controls also enable users to manage friend requests, block or unfriend individuals, and restrict access to their content.

**Data Collection and Sharing:**

- Social media platforms collect vast amounts of user data, including personal information, browsing habits, and preferences.
- Users should be aware of the data collected by these platforms and review privacy policies to understand how their data is used, shared, and stored.
- It is important to consider the potential implications of data sharing and be cautious about sharing sensitive or private information on social media.

**Online Reputation and Oversharing:**

- Maintaining social media privacy involves being mindful of the information shared and the impact it may have on one's online reputation.
- Oversharing personal information, location, or details about daily routines can increase the risk of identity theft, stalking, or other cybercrimes.
- Users should be cautious about sharing personal details and consider the potential consequences before posting or disclosing sensitive information publicly.

**Third-Party Applications and Privacy Risks:**

- Many social media platforms allow third-party applications to access user data, which can pose privacy risks.
- Users should carefully review the permissions requested by third-party apps and assess the trustworthiness and credibility of the developers before granting access to their social media accounts.

- Regularly reviewing and revoking permissions granted to third-party apps is crucial to maintain control over personal data and minimize privacy risks.

# Security Related Issues to Social Media: -

Security-related issues in social media encompass various threats and vulnerabilities that can compromise the privacy, safety, and integrity of users' accounts and information. Here are four key points about security-related issues in social media:

**Account Breaches and Unauthorized Access:**

- Social media accounts are vulnerable to breaches, where attackers gain unauthorized access to user accounts.
- Weak passwords, password reuse, and phishing attacks can lead to compromised accounts, allowing attackers to misuse personal information, post malicious content, or engage in identity theft.
- Users should employ strong, unique passwords, enable two-factor authentication (2FA), and be cautious of suspicious links or requests to protect their accounts from unauthorized access.

**Malware and Scams:**

- Social media platforms can be a breeding ground for malware distribution and scams.
- Users may encounter malicious links, fake profiles, or deceptive content that leads to malware infections or financial fraud.
- It is important to exercise caution when clicking on links, avoid downloading files from untrusted sources, and be skeptical of requests for personal or financial information.

**Privacy and Data Collection:**

- Social media platforms collect extensive user data, which raises concerns about privacy and potential misuse of personal information.
- Data breaches, unauthorized data sharing, and targeted advertising based on user information are prevalent issues.
- Users should review privacy settings, limit the amount of personal information shared publicly, and be mindful of the data they provide to social media platforms.

**Social Engineering and Impersonation:**

- Social media platforms can be exploited for social engineering attacks, where malicious actors manipulate users to divulge sensitive information or perform certain actions.
- Impersonation is also a common security issue, with attackers creating fake accounts to deceive and exploit others.
- Users should be cautious of suspicious messages, friend requests from unknown individuals, and requests for personal or financial information, especially when they seem out of character or too good to be true.

# Flagging and reporting inappropriate content on social media: -

Flagging and reporting inappropriate content on social media platforms is an essential mechanism for users to report violations of community guidelines, terms of service, or any content that is deemed offensive, abusive, or harmful. Here's an explanation of the flagging and reporting process:

**Identifying Inappropriate Content:**

- Users should familiarize themselves with the community guidelines and terms of service of the social media platform they are using. These guidelines outline the types of content that are considered inappropriate or violate platform rules.
- Inappropriate content can include hate speech, harassment, nudity, violence, spam, fake news, or any content that promotes illegal activities or violates the platform's policies.

**Flagging or Reporting the Content:**

- Most social media platforms provide a flagging or reporting feature that allows users to bring attention to inappropriate content.
- Users can typically find this option within the platform's interface, often represented by a flag icon or a report button.
- When encountering inappropriate content, users can select the flag/report option and provide details about the specific violation. Some platforms allow users to include additional comments or descriptions to provide more context.

**Platform Review and Investigation:**

- Once a user flags or reports content, the social media platform's moderation team reviews the reported content.

- The platform evaluates the reported content against its community guidelines and terms of service to determine if it violates any policies.
- The moderation team may consider factors such as the severity of the violation, the context in which the content was posted, and the user's history on the platform.

**Actions Taken:**

- If the reported content is found to be in violation of the platform's policies, appropriate actions are taken by the platform.
- Actions can range from content removal, warning or temporary suspension of the account, to permanent suspension or termination of the account, depending on the severity and frequency of the violations.
- In some cases, platforms may also escalate severe violations to law enforcement authorities if the content involves illegal activities or poses a threat to individuals' safety.

# Laws regarding posting inappropriate content on social media: -

The laws regarding posting inappropriate content on social media can vary depending on the jurisdiction. Here are some general principles and legal considerations to keep in mind:

**Defamation:**

- Posting defamatory statements about individuals or entities on social media can lead to legal consequences.
- Defamation involves making false statements that harm someone's reputation, and it can be categorized as libel (written defamation) or slander (spoken defamation).
- Laws regarding defamation vary across countries, but generally, individuals can pursue legal action if they can prove that the statements are false, have caused harm to their reputation, and were published negligently or with malicious intent.

**Harassment and Cyberbullying:**

- Posting inappropriate content that constitutes harassment or cyberbullying can also be subject to legal consequences.
- Harassment involves persistent unwanted behavior that causes distress or fear, while cyberbullying specifically refers to such behavior occurring online.

- Many jurisdictions have laws that address harassment and cyberbullying, and individuals who are victims of such behavior can seek legal remedies and protection orders.

**Hate Speech and Incitement to Violence:**

- Posting hate speech or content that incites violence against individuals or specific groups based on characteristics such as race, religion, ethnicity, gender, or sexual orientation may be subject to legal action.
- Laws regarding hate speech and incitement to violence vary across jurisdictions, with some countries having specific legislation in place to address these issues.
- It's important to be aware of the local laws and regulations that govern hate speech and incitement to violence when posting content on social media.

**Intellectual Property Infringement:**

- Posting content on social media that infringes upon someone's intellectual property rights, such as copyrighted material or trademarks, can lead to legal consequences.
- Intellectual property laws protect original works, inventions, and branding, and unauthorized use or distribution of such content can result in legal action.
- It's important to respect intellectual property rights and seek proper permissions or licenses when sharing or using copyrighted material on social media.

# UNIT 5: -

## #Introduction to patent: -

A patent is a legal right granted by a government to an inventor or assignee that gives exclusive rights to prevent others from making, using, selling, or importing an invention for a limited period of time.

Patents are a form of intellectual property protection, designed to encourage innovation by providing inventors with a temporary monopoly over their invention. In exchange for this exclusive right, the inventor must disclose the details of their invention to the public, which can then be used by others to further scientific and technological progress.

Patents are granted for a limited period of time, usually 20 years from the date of filing, and they vary in their scope and content depending on the jurisdiction and the type of invention. In order to obtain a patent, an invention must meet certain criteria, including novelty, usefulness, and non-obviousness.

Patents can be valuable assets, as they give the patent holder the right to exclude others from making, using, or selling the patented invention. However, obtaining a patent can be a lengthy and costly process, and not all inventions are eligible for patent protection.

## #Patent Requirements: -

The following are four key requirements for obtaining a patent:

1. Novelty: The invention must be new and not already in the public domain, which means that it has not been disclosed or made available to the public in any way.
2. Utility: The invention must have some practical use and must be capable of being used or made.
3. Non-obviousness: The invention must not be obvious to a person having ordinary skill in the relevant field of technology. This means that it must not be something that would be considered an obvious improvement to an existing invention.

4. Enablement: The invention must be described in a way that enables someone skilled in the relevant field to make or use the invention based on the information provided in the patent application.

# Difference between Product patent and process patent: -

| Product Patent | Process Patent |
|---|---|
| Provides protection for a new and useful product or device | Provides protection for a new and useful process or method of making a product |
| The patent holder has the exclusive right to prevent others from making, using, selling, or importing the product | The patent holder has the exclusive right to prevent others from using the patented process to make the product |
| Protects the end result | Protects the method used to achieve the end result |
| Examples include a new type of medication or an electronic device | Examples include a method of synthesizing a medication or a manufacturing process for a device |
| Patent application must include a description of the product and its features | Patent application must include a description of the process and its steps |
| Duration is 20 years from the date of filing | Duration is 20 years from the date of filing |

| Product Patent | Process Patent |
|---|---|
| Infringement occurs when someone makes, uses, sells, or imports the patented product without permission | Infringement occurs when someone uses the patented process to make the product without permission |
| Licensing allows others to make, use, sell, or import the patented product | Licensing allows others to use the patented process to make the product |

Overall, product patents and process patents protect different aspects of an invention, and the requirements for obtaining and enforcing them are slightly different.